

z/OS



Migration from z/OS V2R1 and z/OS V1R13 to z/OS V2R2

Version 2 Release 2

Note

Before using this information and the product it supports, read the information in "Notices" on page 515.

This edition applies to Version 2 Release 2 of z/OS (5650-ZOS) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 1996, 2017.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this document	vii
Who should read this document	vii
How this document is organized	vii
How to use this document	viii
Conventions and terminology used in this document.	viii
z/OS information.	x

How to send your comments to IBM	xiii
If you have a technical problem	xiii

Summary of changes	xv
Summary of changes for z/OS Version 2 Release 2 (V2R2) as updated June 2017	xv
Summary of changes for z/OS Version 2 Release 2 (V2R2) as updated March 2016	xv
Summary of changes for z/OS Version 2 Release 2 (V2R2) as updated December 2015	xv
Summary of changes for z/OS V2R2.	xvi
Summary of changes for z/OS Migration as updated June 2015	xix
Summary of changes for z/OS Migration as updated February 2015	xix
Information applicable to all releases	xx

Chapter 1. Migration: Introduction	1
Typical migration steps	1
Using IBM Health Checker for z/OS for migration checking.	2
Elements and features that do not have migration actions	3

Chapter 2. General migration actions for everyone migrating to z/OS V2R2.	5
Migration actions for everyone moving to z/OS V2R2	5
Migration actions for everyone before installing z/OS V2R2	5
Migration actions for everyone before the first IPL of z/OS V2R2	13
Migration actions for everyone after the first IPL of z/OS V2R2	43
Hardware migration actions	43
Migrate to an IBM z13 or IBM z13s server	43
Migrate to an IBM zEnterprise EC12 or IBM zEnterprise BC12 server	60
Migrate to an IBM zEnterprise z196 or z114 server	72
Ensure that you are running on supported servers and storage controllers	85
Replace unsupported devices	87
Provide for new device installations	88
Update your CFRM policy with coupling facility structure size changes	89

Chapter 3. Migration from z/OS V2R1	91
Sysplex migration actions.	91
Sysplex actions related to hardware upgrades	91
Sysplex actions to perform before installing z/OS V2R2	91
Sysplex actions to perform before the first IPL of z/OS V2R2	92
Sysplex actions to perform after the first IPL of z/OS V2R2	92
BCP migration actions.	92
BCP actions to perform before installing z/OS V2R2	92
BCP actions to perform before the first IPL of z/OS V2R2	99
BCP actions to perform after the first IPL of z/OS V2R2	127
BookManager BUILD migration actions	130
BookManager BUILD actions to perform before installing z/OS V2R2.	130
BookManager BUILD actions to perform before the first IPL of z/OS V2R2	131
BookManager BUILD actions to perform after the first IPL of z/OS V2R2	131
CIM migration actions	131
CIM actions to perform before installing z/OS V2R2	131
CIM actions to perform before the first IPL of z/OS V2R2	132
CIM actions to perform after the first IPL of z/OS V2R2	132
Communications Server migration actions.	133
Communications Server actions to perform before installing z/OS V2R2	133
Communications Server actions to perform before the first IPL of z/OS V2R2	140
Communications Server actions to perform after the first IPL of z/OS V2R2	151
Cryptographic Services migration actions	152
Cryptographic Services actions to perform before installing z/OS V2R2	152
Cryptographic Services actions to perform before the first IPL of z/OS V2R2	154
Cryptographic Services actions to perform after the first IPL of z/OS V2R2	163
DFSMS migration actions	168
DFSMS actions to perform before installing z/OS V2R2	168
DFSMS actions to perform before the first IPL of z/OS V2R2	173
DFSMS actions to perform after the first IPL of z/OS V2R2	183
DFSORT migration actions	185
DFSORT actions to perform before installing z/OS V2R2	185
DFSORT actions to perform before the first IPL of z/OS V2R2	185

DFSORT actions to perform after the first IPL of z/OS V2R2	186	JES2 actions to perform before the first IPL of z/OS V2R2	210
Distributed File Service migration actions	186	JES2 actions to perform after the first IPL of z/OS V2R2	211
Distributed File Service actions to perform before installing z/OS V2R2	186	JES3 migration actions	211
Distributed File Service actions to perform before the first IPL of z/OS V2R2	187	JES3 actions to perform before installing z/OS V2R2	211
Distributed File Service actions to perform after the first IPL of z/OS V2R2	187	JES3 actions to perform before the first IPL of z/OS V2R2	211
HCD migration actions	188	JES3 actions to perform after the first IPL of z/OS V2R2	213
HCD actions to perform before installing z/OS V2R2	188	Language Environment migration actions	214
HCD actions to perform before the first IPL of z/OS V2R2	188	Language Environment actions to perform before installing z/OS V2R2	214
HCD actions to perform after the first IPL of z/OS V2R2	188	Language Environment actions to perform before the first IPL of z/OS V2R2	216
HLASM migration actions	188	Language Environment actions to perform after the first IPL of z/OS V2R2	218
HLASM actions to perform before installing z/OS V2R2	188	Library Server migration actions	218
HLASM actions to perform before the first IPL of z/OS V2R2	190	Library Server actions to perform before installing z/OS V2R2	218
HLASM actions to perform after the first IPL of z/OS V2R2	191	Library Server actions to perform before the first IPL of z/OS V2R2	218
IBM HTTP Server migration actions	191	Library Server actions to perform after the first IPL of z/OS V2R2	221
IBM HTTP Server actions to perform before installing z/OS V2R2	191	RMF migration actions	221
IBM HTTP Server actions to perform before the first IPL of z/OS V2R2	193	RMF actions to perform before installing z/OS V2R2	221
IBM HTTP Server actions to perform after the first IPL of z/OS V2R2	193	RMF actions to perform before the first IPL of z/OS V2R2	222
IBM Tivoli Directory Server migration actions	193	RMF actions to perform after the first IPL of z/OS V2R2	222
IBM Tivoli Directory Server actions to perform before installing z/OS V2R2	193	SDSF migration actions	225
IBM Tivoli Directory Server actions to perform before the first IPL of z/OS V2R2	195	SDSF actions to perform before installing z/OS V2R2	225
IBM Tivoli Directory Server actions to perform after the first IPL of z/OS V2R2	195	SDSF actions to perform before the first IPL of z/OS V2R2	225
IBM z/OS Management Facility migration actions	195	SDSF actions to perform after the first IPL of z/OS V2R2	228
z/OSMF actions to perform before installing z/OS V2R2	195	Security Server migration actions	228
z/OSMF actions to perform before the first IPL of z/OS V2R2	195	Security Server actions to perform before installing z/OS V2R2	228
z/OSMF actions to perform after the first IPL of z/OS V2R2	195	Security Server actions to perform before the first IPL of z/OS V2R2	230
ICKDSF (Device Support Facility)	199	Security Server actions to perform after the first IPL of z/OS V2R2	232
ICKDSF actions to perform before installing z/OS V2R2	199	XL C/C++ migration actions	233
ICKDSF actions to perform before the first IPL of z/OS V2R2	199	XL C/C++ actions to perform before installing z/OS V2R2	233
ICKDSF actions to perform after the first IPL of z/OS V2R2	199	XL C/C++ actions to perform before the first IPL of z/OS V2R2	234
Infoprint Server migration actions	200	XL C/C++ actions to perform after the first IPL of z/OS V2R2	234
Infoprint Server actions to perform before installing z/OS V2R2	200	z/OS Font Collection migration actions	234
Infoprint Server actions to perform before the first IPL of z/OS V2R2	204	z/OS Font Collection actions to perform before installing z/OS V2R2	234
Infoprint Server actions to perform after the first IPL of z/OS V2R2	206	z/OS Font Collection actions to perform before the first IPL of z/OS V2R2	235
JES2 migration actions	208	z/OS Font Collection actions to perform after the first IPL of z/OS V2R2	236
JES2 actions to perform before installing z/OS V2R2	208	z/OS OpenSSH migration actions	236

z/OS OpenSSH actions to perform before installing z/OS V2R2	236
z/OS OpenSSH actions to perform before the first IPL of z/OS V2R2	236
z/OS OpenSSH actions to perform after the first IPL of z/OS V2R2	236
z/OS UNIX migration actions	241
z/OS UNIX actions to perform before installing z/OS V2R2	241
z/OS UNIX actions to perform before the first IPL of z/OS V2R2	246
z/OS UNIX actions to perform after the first IPL of z/OS V2R2	247

Chapter 4. Migration from z/OS V1R13 249

Sysplex migration actions	249
Sysplex actions related to hardware upgrades	249
Sysplex actions to perform before installing z/OS V2R2	249
Sysplex actions to perform before the first IPL of z/OS V2R2	250
Sysplex actions to perform after the first IPL of z/OS V2R2	250
BCP migration actions	250
BCP actions to perform before installing z/OS V2R2	250
BCP actions to perform before the first IPL of z/OS V2R2	261
BCP actions to perform after the first IPL of z/OS V2R2	300
BookManager BUILD migration actions	306
BookManager BUILD actions to perform before installing z/OS V2R2	306
BookManager BUILD actions to perform before the first IPL of z/OS V2R2	307
BookManager BUILD actions to perform after the first IPL of z/OS V2R2	307
CIM migration actions	307
CIM actions to perform before installing z/OS V2R2	307
CIM actions to perform before the first IPL of z/OS V2R2	308
CIM actions to perform after the first IPL of z/OS V2R2	308
Communications Server migration actions	309
Communications Server actions to perform before installing z/OS V2R2	309
Communications Server actions to perform before the first IPL of z/OS V2R2	323
Communications Server actions to perform after the first IPL of z/OS V2R2	340
Cryptographic Services migration actions	342
Cryptographic Services actions to perform before installing z/OS V2R2	342
Cryptographic Services actions to perform before the first IPL of z/OS V2R2	346
Cryptographic Services actions to perform after the first IPL of z/OS V2R2	360
DFSMS migration actions	365
DFSMS actions to perform before installing z/OS V2R2	365

DFSMS actions to perform before the first IPL of z/OS V2R2	374
DFSMS actions to perform after the first IPL of z/OS V2R2	390
DFSORT migration actions	396
DFSORT actions to perform before installing z/OS V2R2	396
DFSORT actions to perform before the first IPL of z/OS V2R2	396
DFSORT actions to perform after the first IPL of z/OS V2R2	399
Distributed File Service migration actions	399
Distributed File Service actions to perform before installing z/OS V2R2	399
Distributed File Service actions to perform before the first IPL of z/OS V2R2	403
Distributed File Service actions to perform after the first IPL of z/OS V2R2	404
HCD migration actions	405
HCD actions to perform before installing z/OS V2R2	405
HCD actions to perform before the first IPL of z/OS V2R2	406
HCD actions to perform after the first IPL of z/OS V2R2	406
HLASM migration actions	407
HLASM actions to perform before installing z/OS V2R2	407
HLASM actions to perform before the first IPL of z/OS V2R2	408
HLASM actions to perform after the first IPL of z/OS V2R2	409
IBM HTTP Server migration actions	409
IBM HTTP Server actions to perform before installing z/OS V2R2	409
IBM HTTP Server actions to perform before the first IPL of z/OS V2R2	411
IBM HTTP Server actions to perform after the first IPL of z/OS V2R2	411
IBM Tivoli Directory Server migration actions	411
IBM Tivoli Directory Server actions to perform before installing z/OS V2R2	411
IBM Tivoli Directory Server actions to perform before the first IPL of z/OS V2R2	413
IBM Tivoli Directory Server actions to perform after the first IPL of z/OS V2R2	413
IBM z/OS Management Facility migration actions	413
z/OSMF actions to perform before installing z/OS V2R2	413
z/OSMF actions to perform before the first IPL of z/OS V2R2	421
z/OSMF actions to perform after the first IPL of z/OS V2R2	426
ICKDSF (Device Support Facility)	430
ICKDSF actions to perform before installing z/OS V2R2	430
ICKDSF actions to perform before the first IPL of z/OS V2R2	430
ICKDSF actions to perform after the first IPL of z/OS V2R2	430
Infoprint Server migration actions	431

Infoprint Server actions to perform before installing z/OS V2R2	431	Security Server actions to perform before installing z/OS V2R2	475
Infoprint Server actions to perform before the first IPL of z/OS V2R2	435	Security Server actions to perform before the first IPL of z/OS V2R2	477
Infoprint Server actions to perform after the first IPL of z/OS V2R2	437	Security Server actions to perform after the first IPL of z/OS V2R2	481
Integrated Security Services migration actions	439	TSO/E migration actions	482
Integrated Security Services actions to perform before installing z/OS V2R2	439	TSO/E actions to perform before installing z/OS V2R2	482
Integrated Security Services actions to perform before the first IPL of z/OS V2R2	439	TSO/E actions to perform before the first IPL of z/OS V2R2	483
Integrated Security Services actions to perform after the first IPL of z/OS V2R2	441	TSO/E actions to perform after the first IPL of z/OS V2R2	484
JES2 migration actions	441	XL C/C++ migration actions	484
JES2 actions to perform before installing z/OS V2R2	441	XL C/C++ actions to perform before installing z/OS V2R2	484
JES2 actions to perform before the first IPL of z/OS V2R2	444	XL C/C++ actions to perform before the first IPL of z/OS V2R2	485
JES2 actions to perform after the first IPL of z/OS V2R2	447	XL C/C++ actions to perform after the first IPL of z/OS V2R2	485
JES3 migration actions	447	z/OS Font Collection migration actions	485
JES3 actions to perform before installing z/OS V2R2	447	z/OS Font Collection actions to perform before installing z/OS V2R2	485
JES3 actions to perform before the first IPL of z/OS V2R2	447	z/OS Font Collection actions to perform before the first IPL of z/OS V2R2	485
JES3 actions to perform after the first IPL of z/OS V2R2	451	z/OS Font Collection actions to perform after the first IPL of z/OS V2R2	488
Language Environment migration actions	453	z/OS OpenSSH migration actions	488
Language Environment actions to perform before installing z/OS V2R2	453	z/OS OpenSSH actions to perform before installing z/OS V2R2	488
Language Environment actions to perform before the first IPL of z/OS V2R2	455	z/OS OpenSSH actions to perform before the first IPL of z/OS V2R2	488
Language Environment actions to perform after the first IPL of z/OS V2R2	460	z/OS OpenSSH actions to perform after the first IPL of z/OS V2R2	488
Library Server migration actions	460	z/OS UNIX migration actions	493
Library Server actions to perform before installing z/OS V2R2	460	z/OS UNIX actions to perform before installing z/OS V2R2	493
Library Server actions to perform before the first IPL of z/OS V2R2	460	z/OS UNIX actions to perform before the first IPL of z/OS V2R2	502
Library Server actions to perform after the first IPL of z/OS V2R2	463	z/OS UNIX actions to perform after the first IPL of z/OS V2R2	507
RMF migration actions	464		
RMF actions to perform before installing z/OS V2R2	464		
RMF actions to perform before the first IPL of z/OS V2R2	464		
RMF actions to perform after the first IPL of z/OS V2R2	467		
SDSF migration actions	470		
SDSF actions to perform before installing z/OS V2R2	471		
SDSF actions to perform before the first IPL of z/OS V2R2	471		
SDSF actions to perform after the first IPL of z/OS V2R2	474		
Security Server migration actions	475		
		Appendix. Accessibility	511
		Accessibility features	511
		Consult assistive technologies	511
		Keyboard navigation of the user interface	511
		Dotted decimal syntax diagrams	511
		Notices	515
		Policy for unsupported hardware	516
		Minimum supported hardware	517
		Trademarks	517
		Index	519

About this document

This document describes how to migrate to z/OS® Version 2 Release 2 (V2R2) from the following releases:

- z/OS V2R1
- z/OS V1R13

The document is arranged in parts with chapters 1 and 2 as an introduction for everyone who performs z/OS migration actions regardless of the migration path and migration paths for hardware, chapter 3 for those customers migrating from z/OS V2R1, and chapter 4 for those customers migrating from z/OS V1R13. For chapters 3 and 4 only those actions for the specific migration path are documented. See “How this document is organized.”

This document does not explain how to exploit new functions in z/OS. For that information, see the many publications that pertain to the z/OS base elements and optional features.

Who should read this document

This document is intended for system analysts, system programmers, system administrators, security administrators, network administrators, database administrators, and other members of an information technology team who have experience installing and managing z/OS, and want to plan for and implement the installation of z/OS V2R2.

How this document is organized

This document is organized into the following parts:

- Chapter 1, “Migration: Introduction,” on page 1 is general in scope and for all users, that is, not devoted to a specific z/OS base element or optional feature, or specific migration path. It includes the following topics:
 - “Typical migration steps” on page 1
 - “Using IBM Health Checker for z/OS for migration checking” on page 2.
 - “Elements and features that do not have migration actions” on page 3.
- Chapter 2, “General migration actions for everyone migrating to z/OS V2R2,” on page 5 is general in scope and for all users, that is, not devoted to a specific z/OS base element or optional feature. It includes the following topics:
 - “Migration actions for everyone moving to z/OS V2R2” on page 5
 - “Migration actions for everyone before installing z/OS V2R2” on page 5
 - “Migration actions for everyone after the first IPL of z/OS V2R2” on page 43
 - “Hardware migration actions” on page 43.
- Chapter 3, “Migration from z/OS V2R1,” on page 91 is a customized path for migration from z/OS V2R1 to z/OS V2R2. It includes topics devoted to the specific elements and features that have migration actions, with one element or feature per chapter. These topics are in alphabetic order — from BCP (“BCP migration actions” on page 92) to z/OS UNIX (“z/OS UNIX migration actions” on page 241). Within each topic, the following organization is used:
 - Migration actions to perform *before installing z/OS V2R2*
 - Migration actions to perform *before the first IPL of z/OS V2R2*
 - Migration actions to perform *after the first IPL of z/OS V2R2*.
- Chapter 4, “Migration from z/OS V1R13,” on page 249 is a customized path for migration from z/OS V1R13 to z/OS V2R2. It includes topics devoted to the specific elements and features that have

migration actions, with one element or feature per chapter. These topics are in alphabetic order — from BCP (“BCP migration actions” on page 250) to z/OS UNIX (“z/OS UNIX migration actions” on page 493). Within each topic, the following organization is used:

Migration actions to perform *before installing z/OS V2R2*

Migration actions to perform *before the first IPL of z/OS V2R2*

Migration actions to perform *after the first IPL of z/OS V2R2*.

How to use this document

Use this document as your initial source for z/OS migration information. Where appropriate, this document refers you to other documents for additional information.

Within this document, read Chapter 1, “Migration: Introduction,” on page 1 and Chapter 2, “General migration actions for everyone migrating to z/OS V2R2,” on page 5 regardless of your particular migration path from an earlier release. When you have completed Chapter 1 and Chapter 2, read one of the subsequent chapters, based on the release from which you are migrating. You should choose either Chapter 3 or Chapter 4. You do not need to read both chapters, as the material in each chapter has been customized for that migration path.

If you are migrating from z/OS V2R1, go to Chapter 3, “Migration from z/OS V2R1,” on page 91 and proceed sequentially through the subsequent topics or in whatever order you prefer based on element or feature interest. The topics are in alphabetic order by name of element or feature, once you pass the topic on migration actions for everyone, the topic on hardware migration actions, and the topic on sysplex migration actions

If you are migrating from z/OS V1R13, go to Chapter 4, “Migration from z/OS V1R13,” on page 249 and proceed sequentially through the subsequent topics or in whatever order you prefer based on element or feature interest.

The topics in are in alphabetic order by name of element or feature, once you pass the topic on migration actions for everyone, the topic on hardware migration actions, and the topic on sysplex migration actions.

Another way to proceed is to concentrate first on preinstall migration actions within each topic for the appropriate migration path, then pre-IPL migration actions, and then post-IPL migration actions. These actions are clearly identified by major headings within each topic in the appropriate chapter.

Conventions and terminology used in this document

When this document refers to **IBM z Systems™** servers without stating a specific server, it refers to all of the following servers:

- IBM z Systems z13™ (z13)
- IBM z Systems z13s™ (z13s™)
- IBM® zEnterprise® BC12 (zBC12)
- IBM zEnterprise EC12 (zEC12)
- IBM zEnterprise™ 114 (z114)
- IBM zEnterprise™ 196 (z196)
- IBM System z10™ Enterprise Class (z10 EC)
- IBM System z10 Business Class (z10 BC)
- IBM System z9® Enterprise Class (z9 EC), formerly the IBM System z9 109 (z9-109)
- IBM System z9 Business Class (z9 BC)
- IBM eServer™ zSeries 990 (z990)
- IBM eServer zSeries 890 (z890)
- IBM eServer zSeries 900 (z900)
- IBM eServer zSeries 800 (z800)

Important terms you should understand are:

- **Migration.** Migration is the first of two stages in an upgrade to a new release of z/OS. (The second stage is exploitation.) During this stage you install your new system with the objective of making it functionally compatible with the previous system. After a successful migration, 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. Migration does not include exploitation of new functions except for new functions that are now required.
- **Exploitation.** Exploitation is the second of two stages in an upgrade to a new release of z/OS. (The first stage is migration.) During this stage you do whatever customizing and programming are necessary to take advantage of (exploit) the enhancements available in the new release.
- **Coexistence.** Coexistence is the situation in which two or more systems at different software levels share resources. The resources could be shared at the same time by different systems in a multisystem configuration, or they could be shared over a period of time by the same system in a single-system configuration.

Examples of coexistence are two different JES releases sharing a spool, two different service levels of DFSMSdfp sharing catalogs, multiple levels of SMP/E processing SYSMODS packaged to exploit the latest enhancements, or an older level of the system using the updated system control files of a newer level (even if new function has been exploited in the newer level).

The sharing of resources is inherent in multisystem configurations that involve Parallel Sysplex[®] implementations. But other types of configurations can have resource sharing too. Examples of configurations where resource sharing can occur are:

- A single processor that is time-sliced to run different levels of the system, such as during different times of the day
- A single processor running multiple images by means of logical partitions (LPARs)
- Multiple images running on several different processors in either Parallel Sysplex or non-Parallel Sysplex configurations

The way in which you make it possible for earlier-level systems to coexist with the most current level is to install coexistence and fallback PTFs on the earlier-level systems.

- **Fallback.** Fallback is a return to the prior level of a system. Fallback can be appropriate if you migrate to a new release and, during testing, encounter severe problems that can be resolved by backing out the new release. By installing coexistence and fallback PTFs on the “old” system before you migrate, the old system can tolerate changes that were made by the new system during testing.

To identify the timing of migration actions, this document uses three types of headings:

- **Actions to perform before installing z/OS V2R2.** These are migration 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 do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 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 V2R2.
- **Actions to perform before the first IPL of z/OS V2R2.** These are migration actions that you perform after you have installed z/OS V2R2 but before the first time you IPL. These actions require the z/OS V2R2 level of code to be installed but do not require it to be active. That is, you need the z/OS V2R2 programs, utilities, and samples in order to perform the migration actions, but the z/OS V2R2 system does not have to be IPLed in order for the programs to run. Examples are running sysplex utilities and updating the RACF[®] database template.

It is possible to perform some of the migration actions in this category even earlier. If you prepare a system on which you will install z/OS V2R2 by making a clone of your old system, you can perform migration actions that involve customization data on this newly prepared system before installing z/OS V2R2 on it. Examples of such migration actions are updating configuration files and updating automation scripts.

- **Actions to perform after the first IPL of z/OS V2R2.** These are migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 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 V2R2 to be active to perform the task. You might perform the task quite a while after the first IPL.

Each migration action within the headings described is presented using the following standard format:

- A title that identifies the migration action.
- **Description.** This is a brief description of the functional change that caused the migration action.
- **Element or feature.** This is the name of the base element or optional feature that changed.
- **When change was introduced.** This is the z/OS release in which the change was introduced.
- **Applies to migration from.** The migration action is relevant if you are migrating from this release.
- **Timing.** This is when you should perform the migration action. There are three categories: before installing z/OS, before first IPL, or after first IPL. (For SMP/E there are two categories: after installing SMP/E but before starting to use it, and after starting to use SMP/E.)
- **Is the migration action required?** This question refers to the migration action identified by the title. The answer can be one of the following:
 - *Yes.* The migration action is required in all cases.
 - *Yes, if...* The migration action is required only in a certain case. Most of the migration actions in this document are in this category.
 - *No, but recommended...* The migration 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.
- **Target system hardware requirements.** This is hardware required by the functional change. It could be processor and peripheral devices; drivers, engineering changes, or patches needed; or specific hardware functions that must be active.
- **Target system software requirements.** This is software required by the functional change. It could be z/OS optional features, software products, and PTFs that are needed on the target system, as well as specific software functions that must be active.
- **Other system (coexistence or fallback) requirements.** These are requirements placed on an earlier release by the functional change in the new release. The earlier release could be running on a system that shares resources (coexists) with the new system or it could be the release from which you are migrating (and to which you might want to fall back).
- **Restrictions.** These are any known limits on how the function can be used.
- **System impacts.** These are any known impacts of using the function, such as increased storage or more time required to run.
- **Related IBM Health Checker for z/OS check.** These are IBM Health Checker for z/OS checks available for the migration action.
- **Steps to take.** This is what you have to do to perform the migration action.
- **Reference information.** This is a pointer to additional information that helps you perform the migration action.

The order in which the migration actions are presented does not imply importance or chronology.

z/OS information

This information explains how z/OS references information in other documents and on the web.

When possible, this information uses cross document links that go directly to the topic in reference using shortened versions of the document title. For complete titles and order numbers of the documents for all products that are part of z/OS, see *z/OS V2R2 Information Roadmap*.

To find the complete z/OS library, go to IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SSLTBW/welcome) or e0zlib.

How to send your comments to IBM

We appreciate your input on this documentation. Please provide us with any feedback that you have, including comments on the clarity, accuracy, or completeness of the information.

Use one of the following methods to send your comments:

Important: If your comment regards a technical problem, see instead “If you have a technical problem.”

- Send an email to mhvrcfs@us.ibm.com.
- Send an email from the Contact z/OS web page (www.ibm.com/systems/z/os/zos/webqs.html).

Include the following information:

- Your name and address
- Your email address
- Your phone or fax number
- The publication title and order number:
 - z/OS V2R2 Migration
 - GA32-0889-08
- The topic and page number or URL of the specific information to which your comment relates
- The text of your comment.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute the comments in any way appropriate without incurring any obligation to you.

IBM or any other organizations use the personal information that you supply to contact you only about the issues that you submit.

If you have a technical problem

Do not use the feedback methods that are listed for sending comments. Instead, take one or more of the following actions:

- Visit the IBM Support Portal (support.ibm.com).
- Contact your IBM service representative.
- Call IBM technical support.

Summary of changes

This information includes terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations for the current edition are indicated by a vertical line to the left of the change.

Summary of changes for z/OS Version 2 Release 2 (V2R2) as updated June 2017

The following changes are made for z/OS V2R2 as updated June 2017.

Changed information

The topic “Ensure that the CustomPac Installation Dialog is updated” on page 11 is updated for service.

Summary of changes for z/OS Version 2 Release 2 (V2R2) as updated March 2016

The following changes are made for z/OS V2R2 as updated March 2016.

New information

The IBM z Systems z13s is the newest IBM mainframe. For information, see “Migrate to an IBM z13 or IBM z13s server” on page 43.

The following migration actions are new:

- “IP Services: Prepare for the removal of the TFTPDP function” on page 139
- “IP Services: Replace configuration of additional z/OS legacy device types” on page 138
- “DFSMSdftp: Accommodate new authorization requirements for users of the IDCAMS DEFINE command” on page 179

These actions are applicable for customers migrating from either z/OS V2R1 or z/OS V1R13, and are thus included in both Chapter 3, “Migration from z/OS V2R1,” on page 91 and Chapter 4, “Migration from z/OS V1R13,” on page 249.

Changed information

The following topics are updated:

- “Update your check customization for modified IBM Health Checker for z/OS checks” on page 25
- “Accommodate new address spaces” on page 41
- “IP Services: Update /etc configuration files” on page 142
- “Accommodate the removal of default passwords on RACF commands” on page 228.

Summary of changes for z/OS Version 2 Release 2 (V2R2) as updated December 2015

The following changes are made for z/OS V2R2 as updated December 2015.

New information

The following information is new. For migration actions, only actions that did not appear in the previous level of the document are listed.

- New BCP actions:
 - “AMBLIST uses the system-determined block size for SYSPRINT” on page 93
 - “Accommodate system symbol names that contain underscores” on page 103
 - “Examine your IEFUSI exit routine for possible changes” on page 107
 - “Evaluate the stand-alone dump default for large memory objects” on page 129
- New Common Information Model (CIM) action: “Prepare for the removal of the CIM Java Managed Provider Interface (JMPI)” on page 132
- New Communications Server action: “IP Services: Verify that the changed DHGroup default is acceptable” on page 137
- New Cryptographic Services action: “ICSF: Deprecated parameters in installation options data set” on page 156
- New DFSMSdftp actions:
 - “DFSMSdftp: Accommodate change for data set name prefix in IDCAMS ALLOCATE” on page 177
 - “DFSMSdftp: Review the DCB block size specified in IDCAMS REPRO JCL” on page 373
- New DFSMSrmm action: “DFSMSrmm: Prepare for the removal of the DFSMSrmm CIM provider” on page 172
- New Infoprint Server action: “Discontinue use of Infoprint Server aophinvd, aoplogd, and aopsdbd daemons” on page 204
- New Security Server actions:
 - “Accommodate the removal of default passwords on RACF commands” on page 228
 - “Evaluate your use of the ICHDEX01 exit routine” on page 231

The following health check is new: PFA_PRIVATE_STORAGE_EXHAUSTION. For the list of health checks, see “Update your check customization for modified IBM Health Checker for z/OS checks” on page 25.

Changed

The following information is changed:

- This topic is updated with more information: “Plan for the removal of IBM HTTP Server powered by Domino” on page 191

Summary of changes for z/OS V2R2

The summary of changes that are made to z/OS Version 2 Release 2 (V2R2) Migration, as updated September 2015, in support of z/OS Version 2 Release 2 (z/OS V2R2).

This document contains information that is previously presented in GA32-0889-04, which supports z/OS Version 2 Release 1 (V2R1).

New information

The following information is new. For migration actions, only actions that did not appear in the previous level of this document are listed.

New BCP actions:

- “Consider the new COUPLExx CFRMTAKEOVERCF(NO) default” on page 128
- “Update a Capacity Provisioning Manager parameter to avoid a defined capacity WTOR” on page 98
- “Format the ARM couple data set for long symbol table support” on page 105
- “Ensure that PARMDD or REGIONX are not used as job statement symbols” on page 106

- “Assess the use of the INCLUDE1MAFC keyword on the LFAREA parameter in IEASYSxx” on page 109
- “Plan for the use of freemained frames” on page 110
- “Relocate Cross System Extended Services (XES) component trace buffers” on page 113
- “MVS SLIP command change for MODE=HOME” on page 115
- “Plan for the increase of the maximum number of supported CPUs to 256” on page 269
- “Update Capacity Provisioning to use Java 7.1 or higher” on page 118
- “Modify the UPDATE statement for the PFA date change” on page 119
- “Review PFA check values” on page 120
- “Ensure that PFA finds the configuration file” on page 121
- “Update PFA to use Java 7.1 or higher” on page 122
- “Ensure that the IWM4HLTH service is used properly” on page 123
- “Identify unauthorized callers of the IWMSRDRS and IWMSRSRG services” on page 124
- “Ensure that authorizations are correct for callers of WLM services” on page 126
- “Plan for the new default format level of HBB7705 in the IXCL1DSU utility” on page 127

New Communications Server actions:

- “IP Services: Replace configuration of TCP/IP legacy device types” on page 134
- “IP Services: Modify GLOBALCONFIG SMCR PFID definitions” on page 140
- “IP Services: Make changes for Netstat enhancements” on page 141
- “IP Services: Verify z/OS UNIX file permission settings” on page 144
- “IP Services: Verify the new default for the QUEUEDRTT parameter” on page 147
- “IP Services: Use the new maximum segment size adjustments if required” on page 148
- “IP Services: Check code that automates on IKE daemon syslogd messages” on page 148
- “IP Services: Decide whether to accept the new FIXED CSM default” on page 150
- “SMTP: Prepare for the removal of SMTPD NJE Mail Gateway and Sendmail” on page 136
- “SNA Services: Update TIBUF pool size and T1BUF pool size” on page 150

New Cryptographic Services actions:

- “System SSL: Modify code or System SSL application configurations to enable SSLV2 or SSLV3” on page 158
- “System SSL: Modify code or System SSL application configurations to enable null encryption, RSA-Export, or RC4 ciphers” on page 160
- “PKI Services: Migrate to IBM HTTP Server - Powered by Apache” on page 165

New DFSMS actions:

- “DFSMSdss: Determine whether you need DISABLE(REFUCB) in parmlib member DEVSUPxx” on page 170
- “DFSMSdftp: Prepare for the removal of TSO copy services commands” on page 171
- “DFSMSdftp: Define a security profile for VSAM exception exits” on page 176
- “DFSMSHsm: Update applications that depend on LIST command output” on page 183
- “DFSMSdss: Lock or suspend user catalog data sets before performing a logical restore operation” on page 395

New DFSORT action:

- “Update automation for changed DFSORT messages” on page 186

New Distributed File Service action:

- “SMB: Add _BPXK_UNUSEDTASKS=KEEP to the DFSCNTL environment file” on page 187

New IBM HTTP Server action:

- “Plan for the removal of IBM HTTP Server powered by Domino” on page 191

New IBM z/OS Management Facility actions:

- “Migrate to the new release of z/OSMF” on page 195
- “Remove the most-generic profile for z/OSMF authorizations” on page 196

- “Recreate all table filters in the z/OSMF user interface” on page 197
- “Convert to SAF Authorization Mode” on page 413
- “Review the SAF profile prefix” on page 415
- “Check the security for ports 32207 and 32208” on page 416
- “Evaluate your usage of the zOSMFAD user ID from previous releases” on page 417
- “Remove WebSphere constructs from previous releases” on page 418
- “Remove the APF authorization for SYS1.MIGLIB(AMATERSE)” on page 419
- “Check the security profile for the Software Management task” on page 421
- “Authorize the z/OSMF server to create PassTickets” on page 422
- “Install the z/OSMF cataloged procedures” on page 423
- “Verify that the z/OSMF server has sufficient authorization” on page 424
- “Defining the z/OSMF started procedures to RACF” on page 425
- “Review the new z/OSMF service process” on page 427
- “Notify users of the correct URL to use for z/OSMF” on page 427

New ICKDSF action:

- “ICKDSF: Accommodate new default for INIT and REFORMAT commands” on page 199

New Infoprint Server actions:

- “Upgrade web browser support for Infoprint Central” on page 202
- “Upgrade Java support for IPP Server and Infoprint Central” on page 202
- “Remount the Printer Inventory and copy files that were customized” on page 205
- “Configure IBM HTTP Server - Powered by Apache” on page 207

New JES3 actions:

- “Be aware that JES3 honors the DSI setting in SCHEDxx” on page 211
- “Check code that references the JES3 Locate Response control block in IATYLRs” on page 213

New Integrated Security Services action:

- “NAS: Allow GSS-API application programs to access the CSFRNG resource of the CSFSERV class” on page 439

New Language Environment action:

- “Ensure that the name of the debug tool event handler is recognized by Language Environment” on page 214

New Library Server action:

- “Migrate the Library Server configuration to work with IBM HTTP Server - Powered by Apache” on page 220

New RMF actions:

- “Determine whether RMF should monitor zFS file system activity by default” on page 222
- “Update programs that use ERBZFST3 or ERBZFAT3” on page 223

New z/OS Font Collection action:

- “Use the font libraries that are shipped in z/OS V2R2” on page 235

New z/OS OpenSSH action:

- “Accommodate the OpenSSH ported level” on page 236

New z/OS UNIX actions:

- “Determine whether your system has z/OS UNIX program files with certain attributes” on page 245
- “Remove files and directories in /var/man” on page 246

Changed information

The following information is changed:

- Migration actions from earlier releases that apply to z/OS V2R2 are carried over from the previous level of this document.
- The naming convention for migration health checks is changed. See “Using IBM Health Checker for z/OS for migration checking” on page 2.
- “Update your check customization for modified IBM Health Checker for z/OS checks” on page 25.

Moved information

The migration actions for IBM z/OS Management Facility (z/OSMF) are moved to this document from *IBM z/OS Management Facility Configuration Guide*. These actions are described in the following topics:

- “IBM z/OS Management Facility migration actions” on page 195
- “IBM z/OS Management Facility migration actions” on page 413.

Deleted information

Migration actions that were introduced in z/OS V1R13 and do not apply to the z/OS V2R2 path have been removed.

Summary of changes for z/OS Migration as updated June 2015

This document contains information that was previously presented in *IBM z/OS Migration*, GA32-0889-03, which supported z/OS Version 2 Release 1. This document contains new or revised information for maintenance.

Summary of changes for z/OS Migration as updated February 2015

This document contains information previously presented in GA32-0889-02, which supports z/OS Version 2 Release 1 (V2R1).

New information

The following information is new. For migration actions, only actions that did not appear in the previous level of the document are listed.

- New section added in support of newest z Systems server: “Migrate to an IBM z13 or IBM z13s server” on page 43
- New BCP actions:
 - “Plan for HWIREXX helper program restriction for z/OS BCPii” on page 101
 - “Adjust parameters to start IOSHMCTL in TPC-R Basic Hyperswap environment” on page 102
- New Communication Server actions:
 - “Migrate environment variable settings” on page 340
 - “IP Services: Enable SSLv3 for z/OS components if required” on page 145
- New DFSMS actions:
 - “DFSMSdftp: Define a security product profile for IDCAMS DCOLLECT exit” on page 184
 - “DFSMSdftp: Adjust parameters to control whether offline device discovery is performed” on page 175
 - “DFSMSdss: Accommodate ADREID0 EIREC14 expansion” on page 182
- New HLASM action: “Adjust the block size on assembler SYSLIN when using the HEWLKED linkage editor program” on page 190

Changed information

Highlights include:

- “Use LOGR Couple Data Set at format level HBB7705” on page 95 is moved under BCP migration actions from general migration actions.
- “IP Services: Ensure that FTP is listed in AUTHCMD and AUTHPGM NAMES” on page 311
- “IP Services: Replace configuration of TCP/IP legacy device types” on page 134

Information applicable to all releases

This document contains terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations are indicated by a vertical line in the margin by the change.

The *Readers' Comments - We'd Like to Hear from You* section at the end of this publication has been replaced with a new section “How to send your comments to IBM” on page xiii. The hardcopy mail-in form has been replaced with a page that provides information appropriate for submitting comments to IBM.

Chapter 1. Migration: Introduction

This chapter is an introduction to z/OS migration for both z/OS V2R1 and z/OS V1R13 users who are migrating to z/OS V2R2.

Typical migration steps

It is possible to make migration changes at the same time you make the changes necessary to exploit new functions in the new release. However, the more prudent approach is to do your migration first and then exploit new functions. The typical steps to accomplish this are:

1. Learn about z/OS V2R2. Good sources of information include:

z/OS Introduction and Release Guide

z/OS Planning for Installation

The z/OS Library at z/OS Internet Library (www.ibm.com/systems/z/os/zos/library/bkserv).

2. Perform as many of the migration actions as you can on your existing (“old”) system so that you have fewer actions to perform after you install z/OS V2R2. In this information, the actions you can perform on your existing system are identified by headings that say **Actions to perform before installing z/OS V2R2**. (Note that not all of the actions are required. Some depend on your environment, configuration, and workload, and are identified accordingly.) These actions should be made to, or copied (cloned) to, all existing systems that will be migrated to z/OS V2R2.
Use IBM Health Checker for z/OS to assist with some migration actions. See “Using IBM Health Checker for z/OS for migration checking” on page 2.
3. Order and install coexistence and fallback service for any system that will share resources with a z/OS V2R2 system. (See “Install coexistence and fallback PTFs” on page 6.) This service needs to be installed on all systems that will coexist with z/OS V2R1 and all systems that will be migrated to z/OS V2R2 (and which you might fall back to).
4. Prepare the driving system. For driving system requirements, see the topic about preparing the driving system in *z/OS Planning for Installation*.
5. Order and install z/OS V2R2. If you use a ServerPac, refer to *ServerPac: Installing Your Order*. If you use a CBPDO, see the *z/OS Program Directory* at the z/OS installation related information website.
6. Prepare target system hardware and software. During this step, perform the migration actions identified by headings that say **actions to perform before the first IPL of z/OS V2R2**. (Again, not all of the actions are required. Some depend on your environment, configuration, and workload, and are identified accordingly.)
7. IPL the new z/OS V2R2 system with your updated customization and configuration files.
8. Perform any migration actions identified by headings that say **actions to perform after the first IPL of z/OS V2R2**. (Again, not all of the actions are required. Some depend on your environment, configuration, and workload, and are identified accordingly.)
Use IBM Health Checker for z/OS to assist with some migration actions. See “Using IBM Health Checker for z/OS for migration checking” on page 2.
9. Deploy z/OS V2R2 to other systems within a sysplex, data center, and enterprise.
The migration is now complete.
10. When you are confident that a system, or in some cases all systems in a sysplex, are not going to fall back to z/OS V2R1 or z/OS V1R13 exploit the functions introduced in z/OS V2R2.
11. Deploy this exploitation on other systems (again within a sysplex, data center, and eventually enterprise).

Using IBM Health Checker for z/OS for migration checking

Before you migrate to a new z/OS release, you can use IBM Health Checker for z/OS to assist with migration planning. Migration checks can help you determine the applicability of various migration actions to your current system. As with other checks provided by IBM Health Checker for z/OS, no updates are made to the system. Migration checks report only on the applicability of specific migration actions on a system, and only on the currently active system.

Note: As of z/OS V2R1, the IBM Health Checker for z/OS is started automatically at initialization. For more information, see “Accommodate new address spaces” on page 41 and “Convert your existing IBM Health Checker for z/OS setup for automatic start-up” on page 266.

Migration checks are similar to the other checks provided by IBM Health Checker for z/OS. The only differences are:

- Migration checks are inactive by default.
- The names of migration checks begin with the characters **ZOSMIG**. Following this prefix is a value to help you plan the timing of the migration action, as follows:

ZOSMIGVvRr_NEXT

Migration action is recommended, but will become a required migration action in the release after VvRr.

ZOSMIGVvRr_NEXT2

Migration action is recommended, but will become a required migration action two releases after VvRr.

ZOSMIGVvRr

Migration action is required in the release indicated by VvRr.

ZOSMIGREC

Migration action is recommended for the foreseeable future. The migration action might never be required.

ZOSMIGREQ

Migration action that is recommended now, but will be required in a future release.

Note: In previous releases, the names of migration checks followed a different set of naming conventions: one for ICSF, which used the convention **ICSMIG***nnnn_component_program_name*, and one for the rest of z/OS, which used the convention **ZOSMIG***VvRrr_component_program_name*.

On your current z/OS release, follow these steps:

1. Install the latest migration checks. Review all the latest health checks for both best practices and migration by using the SMP/E FIXCAT IBM.Function.HealthChecker.
You might want to install the PTFs during a regular service window, so that an IPL is scheduled afterward. Checks are often added by a function when it is started or restarted, so you might find that installing the PTFs before a scheduled IPL works best for you. More migration checks can be added at different times, so having all the latest checks installed before making your migration plans is recommended.
2. Activate the migration checks that are appropriate to your migration path. Because the naming convention for migration checks indicates which release introduced the corresponding migration actions, you can activate only the checks that are appropriate for your migration path. Using SDSF (or another method for viewing checks, such as filters), you can view ahead of time which migration checks you have available on your system. For example, if you are migrating from z/OS V1R13 to z/OS V2R2, you must activate the migration checks for changes that occurred in both z/OS V2R1 and z/OS V2R2. If you are migrating from z/OS V2R1 to z/OS V2R2, you need to activate only the migration checks for changes that occurred in z/OS V2R2. There are many ways to make a check active, and many ways to use wildcards to include specific checks.

Here are some examples of using the MODIFY command to make checks active:

- F HZSPROC,ACTIVATE,CHECK=(IBM*,*MIG*)
 - F HZSPROC,ACTIVATE,CHECK=(IBM*,ICSMIG*)
 - F HZSPROC,ACTIVATE,CHECK=(IBM*,ZOSMIG*)
3. Review the migration check output and rerun checks. Any exceptions should be addressed in your migration plan. If you can complete the migration action before you move to the new z/OS release, you can rerun the check to verify that it was completed correctly on your current system. In some cases, the check might be available for running on the new z/OS release for verification after that release is IPLed.
 4. Deactivate the migration checks if you want. If you no longer desire to have the migration checks active, you can deactivate them similar to the way you activated them. For example:
 - F HZSPROC,DEACTIVATE,CHECK=(IBM*,*MIG*)
 - F HZSPROC,DEACTIVATE,CHECK=(IBM*,ICSMIG*)
 - F HZSPROC,DEACTIVATE,CHECK=(IBM*,ZOSMIG*)

Within this document, the migration actions that have checks are clearly identified within the migration actions.

Not all migration actions in this document are addressed by checks; many migration actions do not lend themselves to programmatic checking. Therefore, use this document to prepare your migration plan and do not rely on checks only.

System REXX considerations

Several IBM Health Checker for z/OS migration health checks are written in compiled System REXX. These health checks rely on System REXX customization and runtime activities being completed. If System REXX and the security environment that System REXX requires has not been properly customized, the System REXX health checks will not run successfully. Also, the compiled REXX execs must have the proper runtime support from the Alternate Library for REXX (available in z/OS since V1R9) or from IBM Library for REXX on zSeries (5695-014).

Note: To allow System REXX to use JES services, the AXRnn address spaces are started under the primary subsystem. Therefore, you must end the AXRnn address spaces before you shut down JES2. You do not have to stop the AXR address space; this action only affects the secondary AXRnn address spaces.

More information is available in the following references:

- For information about System REXX customization, see the topic on System REXX in *z/OS MVS Programming: Authorized Assembler Services Guide*.
- For compiled REXX exec runtime availability, see “Alternate Library for REXX Customization Considerations” in the *z/OS Program Directory*, or see the product documentation that accompanies IBM Alternate Library for REXX.

Elements and features that do not have migration actions

The following z/OS V2R2 elements and features do not have migration actions on either the z/OS V2R1 or z/OS V1R13 to z/OS V2R2 path, and thus are not discussed:

- Alternate Library for REXX
- BDT
- BDT File-to-File
- BDT SNA NJE
- BookManager[®] READ
- Communications Server Security Level 3
- EREP

z/OS Migration process: an introduction

- ESCON Director Support
- FFST
- GDDM
- GDDM-PGF
- GDDM-REXX
- HCM
- HLASM Toolkit
- Metal C Runtime Library
- MICR/OCR
- NFS
- Runtime Library Extensions
- SMP/E
- TIOC
- z/OS Security Level 3
- 3270 PC File Transfer Program

Chapter 2. General migration actions for everyone migrating to z/OS V2R2

This chapter contains general z/OS migration actions for both z/OS V1R13 and z/OS V2R1 users who are migrating to z/OS V2R2.

Migration actions for everyone moving to z/OS V2R2

This topic describes general migration actions that apply to everyone, regardless of which elements and features you use.

Migration actions for everyone before installing z/OS V2R2

This topic describes general migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Review PSP buckets Description

You should check the preventive service planning (PSP) “buckets” for important software and hardware installation and maintenance information that occurs too late in the development cycle to be included in the product publications. Included are PTFs for both service and small programming enhancements (SPEs).

Table 1 provides more details about this migration action. Use this information to plan your changes to the system.

Table 1. Information about this migration action

Element or feature:	Multiple
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Identify which PSP buckets to review. For this task you will need to know:
 - PSP bucket upgrade IDs (or “upgrades”). The most relevant upgrades are those related to z/OS V2R2 and its servers. The z/OS V2R2 upgrade is ZOSV2R2; the server upgrades are shown in Table 2 on page 6.

General migration actions for everyone

- FIXCAT values if you use the SMP/E REPORT MISSINGFIX command in conjunction with the FIXCAT type of HOLDDATA (as mentioned in the tip that follows). The FIXCAT values are shown in Table 2.

Note:

- The values shown are for the minimum support necessary for the servers. If you exploit additional functions on a server, the FIXCAT value will have additional qualifiers.
 - You must run z/OS V2R2 on a z10 EC or z10 BC or later. See “Ensure that you are running on supported servers and storage controllers” on page 85.
2. Obtain the PSP buckets from <http://www14.software.ibm.com/webapp/set2/psp/srchBroker> or from IBMLink.
 3. Review the PSP buckets and take whatever actions are prescribed.

Tip: To simplify finding the appropriate PSP bucket and identifying which PTFs listed in the PSP bucket need to be installed on your system, you can use SMP/E FIXCATs and the REPORT MISSINGFIX command. The FIXCAT values are shown in Table 2.

Table 2. Servers, upgrades, and FIXCAT values

Server	Upgrade	FIXCAT value
z13	2964DEVICE	IBM.Device.Server.z13-2964
z13s™	2965DEVICE	IBM.Device.Server.z13S-2965
zBC12	2828DEVICE	IBM.Device.Server.zBC12-2828
zEC12	2827DEVICE	IBM.Device.Server.zEC12-2827
z114	2818DEVICE	IBM.Device.Server.z114-2818
z196	2817DEVICE	IBM.Device.Server.z196-2817
z10 EC	2097DEVICE	IBM.Device.Server.z10-EC-2097
z10 BC	2098DEVICE	IBM.Device.Server.z10-BC-2098

Reference information

For more information, see the following references:

- For z/OS subsets, see *z/OS Program Directory* at the z/OS installation related information website.
- For details about the SMP/E REPORT MISSINGFIX command, see *SMP/E for z/OS Commands*.

Install coexistence and fallback PTFs

Description

By installing coexistence and fallback PTFs on your pre-z/OS V2R2 systems, you allow the systems to coexist with z/OS V2R2 systems during your migration. Installing coexistence and fallback PTFs also allows for fallback to the previous systems, if necessary. Coexistence and fallback are important because they allow you to migrate systems in a multisystem configuration to z/OS V2R2 using rolling IPLs (one system at a time), allowing for continuous application availability.

Table 3 provides more details about this migration action. Use this information to plan your changes to the system.

Table 3. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action that is not tied to a specific release.

Table 3. Information about this migration action (continued)

Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	Install the appropriate PTFs.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Before you introduce z/OS V2R2 into your environment, install coexistence and fallback PTFs on all pre-z/OS V2R2 systems with which your z/OS V2R2 system will coexist.

Use the SMP/E REPORT MISSINGFIX command with the FIXCAT type of HOLDDATA as follows:

1. Obtain and RECEIVE the latest HOLDDATA onto your pre-z/OS V2R2 systems. Use your normal service acquisition portals or download the HOLDDATA directly from <http://service.software.ibm.com/holdata/390holddata.html>. Select Full from the Download NOW column to receive the FIXCAT HOLDDATA; the other files do not contain FIXCATs.
2. Run the SMP/E REPORT MISSINGFIX command on your pre-z/OS V2R2 systems and specify a Fix Category (FIXCAT) value of "IBM.Coexistence.z/OS.V2R2". The report identifies the missing coexistence and fallback PTFs for that system. For more information about the REPORT MISSINGFIX command, see *SMP/E for z/OS Commands*.
3. Periodically, you might want to obtain the latest HOLDDATA and rerun the REPORT MISSINGFIX command to find out whether there are any new coexistence and fallback PTFs.

Reference information

For an explanation of the z/OS coexistence-migration-fallback policy, see the coexistence and fallback topic in *z/OS Planning for Installation*.

Use zSoftCap to identify the effect of capacity changes

Description

The zSoftware Migration Capacity Planning Aid (zSoftCap) is a PC-based tool that evaluates the effects of software release migrations.

Table 4 provides more details about this migration action. Use this information to plan your changes to the system.

Table 4. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended to help in assessing processor capacity and available resources when migrating to new software levels.

General migration actions for everyone

Table 4. Information about this migration action (continued)

Target system hardware requirements:	This tool runs on your workstation. The requirements are: <ul style="list-style-type: none">• A dual-core technology, or faster, processor.• An SVGA display 1024 x 768 or better.• Approximately 5 MB of hard disk space for the zSoftCap application and user's guide, plus 80 MB for the IBM Java 1.6 runtime environment.
Target system software requirements:	This tool runs on your workstation. Requirements are: <ul style="list-style-type: none">• Windows 7.• IBM Java™ 1.6, or later, runtime environment. This environment is available with the tool.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Download zSoftCap from one of the following web sites:
 - Customers: <http://www.ibm.com/support/techdocs/atmastr.nsf/WebIndex/PRS268>.
 - Business partners: https://www.ibm.com/partnerworld/wps/servlet/ContentHandler/tech_PRS1762. Note that this requires an ID on PartnerWorld®.
- Run zSoftCap to determine your expected increase in CPU utilization (if any).

Reference information

For more information, see *zSoftCap User's Guide*, which is provided with the tool.

Add or change volumes to keep your z/OS root file system in a single data set Description

Because of release enhancements and service, the size of the z/OS root file system (or version root file system) continues to grow from release to release. The size of the z/OS root file system, whether HFS or zFS, is expected to closely approach, if not exceed, the limit of 3339 cylinders on a 3390-3 device.

It is advisable to have the z/OS root file system within a single data set for ease of management.

Note: As of z/OS V2R1, there is another file system delivered with z/OS, the font file system. See *z/OS Planning for Installation* for information about the size and contents of this file system.

Table 5 provides more details about this migration action. Use this information to plan your changes to the system.

Table 5. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.

Table 5. Information about this migration action (continued)

Is the migration action required?	No, but recommended for ease of management if your z/OS root file system resides on a 3390-3 volume (or another DASD volume that is close to the 3390-3 limit of 3339 cylinders).
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	Use IBM Health Checker for z/OS check CHECK(IBMUSS, ZOSMIGREC_ROOT_FS_SIZE) to determine if a volume has enough space for the z/OS root file system.

Steps to take

To keep the z/OS root file system in a single data set, do one of the following:

- Move your z/OS root file system to a larger DASD volume geometry
- Use multiple volumes for the z/OS root file system data set.

If your z/OS root data set cannot fit on the volume or volumes you have defined for it, divide the z/OS root, with the smaller file systems being managed together.

Remember that all systems to which you deploy the z/OS root file system need sufficient DASD space to hold the z/OS root.

Tip: File systems for subsystems and products other than the z/OS product itself might also increase in size. When examining the volume for how much space your z/OS file system is using, check other product file system sizes too.

Reference information

For more information about multivolume data sets, see *z/OS DFSMS Implementing System-Managed Storage*.

Verify that you have enough XCF groups and XCF group members

Description

Over time, as various z/OS functions and applications exploit XCF services, you must ensure that there is enough space in the sysplex couple data set for all the XCF groups and members that are to be defined by the exploiters. It is possible that your sysplex couple data set could contain an inadequate number of XCF groups or members.

Note: Starting with z/OS V1R13, JES2 is using new XCF groups for its spool migration enhancement. JES2 spool migration utilizes tasks on all members of a MAS to manage the migration of a spool volume's data and the access to that migrating or migrated data. These various tasks communicate using messages sent through JESXCF services. The JESXCF services utilize one XCF group for each active migration to identify what messages are for which active migration. XCF groups are a limited system resource, so JES2 limits the number of concurrent active migrations to five. If you plan to perform spool migrations, verify that you have up to five XCF groups available if you intend to have up to five spool migrations active at any given time. JES2 will only utilize the number of XCF groups available, up to five, for spool migrations.

General migration actions for everyone

Table 6 provides more details about this migration action. Use this information to plan your changes to the system.

Table 6. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended to ensure that you have an adequate number of XCF groups and members formatted in your sysplex couple data sets.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	Use IBM Health Checker for z/OS check XCF_SYSPLEX_CDS_CAPACITY, which checks the adequacy of the number of groups, members, and systems for which a sysplex CDS is formatted.

Steps to take

Follow these steps:

1. Issue the DISPLAY XCF,COUPLE command on your current system. Notice the values of MAXGROUP and PEAK for your sysplex couple data sets. These values show you the maximum number of XCF groups that the couple data sets can support, and the peak number of XCF groups ever in use in the sysplex. Also notice the values of MAXMEMBER and PEAK for your sysplex couple data sets. These values show you the maximum number of members that the couple data set can support in one group, and the greatest number of members ever in use in the largest group in the sysplex.
2. If your peak member value is close to the maximum member value, you might want to reformat your sysplex couple data sets to support a larger maximum number of members to be used by any one group.

Reference information

For more information, see the following references:

- For information about formatting sysplex couple data sets with the MAXGROUP and MAXMEMBER parameters, see *z/OS MVS Setting Up a Sysplex*.
- For information about the DISPLAY XCF command, see *z/OS MVS System Commands*.

Reference information

For more information, see the following references:

- For information about formatting sysplex couple data sets with the MAXGROUP and MAXMEMBER parameters, see *z/OS MVS Setting Up a Sysplex*.
- For information about the DISPLAY XCF command, see *z/OS MVS System Commands*.
-
-

Ensure that the CustomPac Installation Dialog is updated

Description

As of May 22, 2016, you can no longer download orders from IBM download servers by using standard FTP.

To download your ServerPac or dump-by-data-set SystemPac order securely, you require a sufficient level of the RECEIVE job that is provided in the CustomPac Installation Dialog. The specific level that is required depends on the download method to be used, as follows:

FTP over SSL (FTPS)

To download your order securely by using FTP over SSL (FTPS), you require the updated RECEIVE job that is provided in the CustomPac Installation Dialog level 27.12.00 or higher.

HTTPS

HTTPS To download your order securely by using HTTPS, you require the updated RECEIVE job that is provided in the CustomPac Installation Dialog level 27.20.00 or higher.

To determine the current level of the CustomPac Installation Dialog in use on your system, check the primary panel CPPPPOLI.

To prepare for downloading an order, IBM recommends that you begin by visiting the Connectivity Test website to verify your system setup. No change is required for using Download Director with encryption; however, you can also verify Download Director with the Connectivity Test. The Connectivity Test can be found at Connectivity Test for SW Download Readiness (www.ibm.com/marketing/iwm/iwm/web/preLogin.do?lang=en_US&source=cbct).

Table 7 provides more details about this migration action. Use this information to plan your changes to the system.

Table 7. Information about this migration action

Element or feature:	Customized Offerings for z/OS
When change was introduced:	General migration action that is not tied to a specific release. See Washington Systems Center Flash 10863 at IBM Technical Support Flashes site (www.ibm.com/support/techdocs/atsmastr.nsf/Web/Flashes).
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if your existing CustomPac Installation Dialog is not at a sufficient level, such as 27.12.00 or 27.20.20.
Target system hardware requirements:	None.
Target system software requirements:	See “Identifying driving system software requirements for installing z/OS using ServerPac or dump-by-data-set SystemPac” in <i>z/OS Planning for Installation</i> .
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Failure to update the CustomPac Installation Dialog to a sufficient level can result in the RECEIVE job failing or the inability to download your order securely.
Related IBM Health Checker for z/OS check:	None.

General migration actions for everyone

Steps to take

Follow these steps:

- For ServerPac customers, see the topic on updating your dialogs in *ServerPac: Using the Installation Dialog*. Refer to the section for your order's delivery media (tape, DVD, or internet delivery) to determine the steps to take.
- For CustomPac customers, see the topic on updating your dialogs in *CustomPac: Using the Installation Dialog*. Refer to the section for your order's delivery media (tape, DVD, or internet delivery) to determine the steps to take.

Reference information

For more information, see the following references:

- For more information about the internet delivery method to choose for downloading your ServerPac or CustomPac (SystemPac, ProductPac, FunctionPac) Internet Delivery order, see "Choosing the Internet download method: direct or intermediate" in *z/OS Planning for Installation*.
- For ServerPac customers who want more information about updating your CustomPac Installation Dialog, see "Updating Your Dialogs" in *ServerPac: Using the Installation Dialog*. Refer to the section for your order's delivery media.
- For ServerPac customers who want more information about receiving an order from a server by using the CustomPac Installation Dialog, see "Receiving an Order from a Server" in *ServerPac: Using the Installation Dialog*. Refer to the section for your order's delivery media.
- For CustomPac customers who want more information about updating your CustomPac Installation Dialog, see the topic on updating your dialogs in *CustomPac: Installation Dialog Reference Manual*.
- For CustomPac customers who want more information about receiving an order from a server by using the CustomPac Installation Dialog, see "Receiving an Order from a Server" in *CustomPac: Installation Dialog Reference Manual*.
- See the README and Checklist documents on the Shopz download pages for your order.

Consider using the new JOB statement for the CustomPac installation dialog Description

A new default JOB statement with the LINES parameter is provided with CustomPac dialog level 27.20.00. If you want to use the new default JOB statement, ensure that the CPP@JOB member is not present in data set *userid.ISPF.ISPPROF* before you start the installation dialog. However, if you want to continue to use your existing JOB statement for the RECEIVE job and installation jobs, do nothing.

The LINES parameter indicates the maximum amount of output, in thousands of lines, that a job can print to its SYSOUT data set. The LINES parameter also specifies the action that the system is to take if this maximum is exceeded. In CustomPac dialog level 27.20.00, the LINES parameter in the default JOB statement is set to the following specification:

```
LINES=(999999,WARNING)
```

As a result, the CustomPac jobs can print up to 999999 lines of output before the system issues a warning to the system operator.

Table 8 provides more details about this migration action. Use this information to plan your changes to the system.

Table 8. Information about this migration action

Element or feature:	Customized Offerings for z/OS
When change was introduced:	General migration action that is not tied to a specific release.

Table 8. Information about this migration action (continued)

Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you want to use the new default JOB statement.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Failure to remove your existing CPP@JOB member from the <i>userid.ISPF.ISPPROF</i> data set means that the existing JOB statement is used instead of the new default JOB statement.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. If your installation uses a customized JOB statement with the RECEIVE and installation jobs, determine whether to use the default JOB statement instead. The JOB statement is contained in the CPP@JOB member in data set *userid.ISPF.ISPPROF*.
2. To use the new JOB statement, remove the CPP@JOB member from data set *userid.ISPF.ISPPROF* before you start the installation dialog. Otherwise, do nothing; the CustomPac jobs continue to use your existing JOB statement values.

Reference information

For more information, see the following references:

- For ServerPac users who want more information about updating the CustomPac Installation Dialog, see “Updating Your Dialogs” in *ServerPac: Using the Installation Dialog*.
- For CustomPac users who want more information about updating the CustomPac Installation Dialog, see “Updating Your Dialogs” in *CustomPac: Installation Dialog Reference Manual*.

Migration actions for everyone before the first IPL of z/OS V2R2

This topic describes general migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Set up an IPCS environment

Description

The interactive problem control system (IPCS) is a tool in the BCP that provides formatting and analysis support for dumps and traces. You must set up an IPCS environment so that you can process any dumps taken on the newly-built z/OS system.

Table 9 provides more details about this migration action. Use this information to plan your changes to the system.

Table 9. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.

General migration actions for everyone

Table 9. Information about this migration action (continued)

Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the target system cannot be used for native IPCS and usage of IPCS for information produced by the target system is necessary.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	<p>The version and release level of IPCS must match the level of the system that produced the dump. You must use the z/OS MVS libraries of IPCS code, for example, to analyze a dump or trace produced by that level of the z/OS MVS system.</p> <p>Tip: If it is necessary to have unique IPCS data set names for your current system (because you already have the IPCS data sets with similar names on your earlier system), you can create a unique alias in your catalog that resolves to the current IPCS data sets. This will allow you to have duplicately-named IPCS data sets that are uniquely referenced.</p> <p>When using unique aliases, you might have to update the security definition for the unique high-level qualifier used in the catalog.</p>
Restrictions	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Set up an IPCS environment; for guidance, see the documents that are listed in “Reference information” on page 15. During setup, ensure that your logon procedure points to the target system’s level of IPCS data sets, which are shown in Table 10.

Note: As of z/OS V1R13, it is enforced that GTF data cannot be properly formatted or used on a system that is a different level from the system on which it was gathered. Plan on using the IPCS level associated with the GTF data that you collect.

Table 10. IPCS data set requirements for a logon procedure or DD name allocation

DD name	Data set name	Notes
IATTABL	SYS1.SIATTBL0, if applicable	This is a JES3 data set.
IPCSPARM Note: This DD name is needed if one of the following is true: <ul style="list-style-type: none"> • The system on which the dump was taken has different BCP and JES levels than the system on which the dump will be examined using IPCS. • You have not specified these data sets in your system's parmlib concatenation. 	SYS1.PARMLIB	This is the data set that contains all the shipped z/OS V2R2 parmlib IPCS members. If the copies of BLSCECT and all the other IPCS members are not at z/OS V2R2 level, then IPCS might fail when you attempt to use it.

Table 10. IPCS data set requirements for a logon procedure or DD name allocation (continued)

DD name	Data set name	Notes
IPCSPARM	SYS1.SHASPARM, if applicable	This is a JES2 data set.
IPCSPARM	SYS1.SIATPARM, if applicable	This is a JES3 data set.
ISPMLIB	SYS1.SBLMSG0	
ISPMLIB	SYS1.SIATMSG0, if applicable	This is a JES3 data set.
ISPPLIB	SYS1.SBLSPNL0	
ISPPLIB	SYS1.SHASPNL0, if applicable	This is a JES2 data set.
ISPPLIB	SYS1.SIATPNL0, if applicable	This is a JES3 data set.
ISPSLIB	SYS1.SBLSKEL0	
ISPTLIB	SYS1.SBLSTBL0	
STEPLIB Note: This DD name is needed if the system on which the dump was taken has different BCP and JES levels than the system on which the dump will be examined using IPCS.	SYS1.MIGLIB	
STEPLIB	SYS1.SIEAMIGE	This data set was added in z/OS V1R7. It is a PDSE data set that complements SYS1.MIGLIB. This data set is used along with SYS1.MIGLIB for IPCS.
STEPLIB	SYS1.SHASMIG, if applicable	This is a JES2 data set.
STEPLIB	SYS1.SIATMIG, if applicable	This is a JES3 data set.
SYSEXEC	SYS1.SIATCLI0, if applicable	This is a JES3 data set.
SYSPROC	SYS1.SBLSCLI0	

Reference information

For more information, see the following references:

- For more information about IPCS, see *z/OS MVS IPCS Customization*.
- For information about updating the logon procedure, see *z/OS Program Directory* at the z/OS installation related information website.
- For information about setting up the JES2 IPCS environment, see *z/OS JES2 Diagnosis*.
- For information about setting up the JES3 IPCS environment, see *z/OS JES3 Diagnosis*.
- For information about running different levels of IPCS, see *z/OS MVS IPCS User's Guide*.

Use IBM-supplied parmlib and proclib members

Description

Ensure that all new and changed parmlib and proclib members that are shipped in z/OS V2R2 are updated in your parmlib and proclib concatenations.

Table 11 provides more details about this migration action. Use this information to plan your changes to the system.

Table 11. Information about this migration action

Element or feature:	Multiple.
---------------------	-----------

General migration actions for everyone

Table 11. Information about this migration action (continued)

When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- For parmlib, add the data set pointed to by the z/OS V2R2 PARMLIB DDDEF to your parmlib concatenation. The data set should generally be added last in the concatenation, and you should make sure that the other data sets in the concatenation do not have members with the same names as IBM-supplied members. If you place the data set on the system residence volume and use an indirect catalog entry, future migrations will not require this particular migration step.
- For proclib:
 1. Ensure that the default proclib members have been copied to your default proclib to pick up the new and changed members.
 2. Update individual sample members provided and ensure they are accessible to the system, as shown in the table of proclib member updates in *z/OS Program Directory*.
 3. Ensure that the procedure libraries listed in the table of libraries to be added to the proclib concatenation in *z/OS Program Directory* are placed in the necessary procedure library concatenations and are available to the system.

Reference information

For the parmlib and proclib members that are shipped that are shipped in z/OS, see *z/OS Program Directory* at the z/OS installation related information website.

Migrate /etc and /var system control files

Description

The /etc and /var directories contain system control files. The /etc directory contains customization data that you maintain and the /var directory contains customization data that IBM maintains.

The following elements and features use /etc:

- BCP (Predictive Failure Analysis).
- CIM.
- Communications Server (IP Services component). See “IP Services: Update /etc configuration files” on page 142.
- Cryptographic Services (PKI Services and System SSL components).
- DFSMSrmm.
- Distributed File Service. The SMB server uses /etc/dfs.
- IBM HTTP Server.
- IBM Tivoli Directory Server (TDS). The LDAP server component uses /etc/ldap.

- Infoprint Server. See “Remount the Printer Inventory and copy files that were customized” on page 205.
- Integrated Security Services. The Network Authentication Service component uses /etc/skrb.
- Library Server. See “Library Server actions to perform before the first IPL of z/OS V2R2” on page 218.
- z/OS UNIX.

The following elements and features use /var:

- Cryptographic Services (OCSF component). See “OCSF: Migrate the directory structure” on page 156.
- DFSMSrmm.
- IBM Tivoli Directory Server (TDS). The LDAP server component uses /var/ldap.
- IBM z/OS Management Facility (z/OSMF).
- Infoprint Server. See “Remount the Printer Inventory and copy files that were customized” on page 205.
- Integrated Security Services. The Network Authentication Service component uses /var/skrb.

During installation, subdirectories of /etc and /var are created. If you install z/OS using ServerPac, some files are loaded into /etc and /var because of the customization performed in ServerPac. You have to merge the files in /etc 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 V2R2 /etc and /var subdirectories.

After merging or copying the contents of /etc and /var, you have to inspect and modify the files as necessary to reflect z/OS V2R2 requirements.

Table 12 provides more details about this migration action. Use this information to plan your changes to the system.

Table 12. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Copy files from your old system to the z/OS V2R2 /etc and /var subdirectories, and then modify the files as required for z/OS V2R2. If you have other files under your existing /var directory, you must merge the old and new files under /var. The easiest way to do this is to create a clone of your current /var file system and then copy the new /var files into the clone.

Many z/OS UNIX utilities are available for comparing and copying directory structures and files. Two that are especially helpful for /etc and /var migration work are:

- **diff** (with the **-r** option, for recursion). This utility is very useful for comparing the path structures and file contents, and has many options available. The **dircmp** utility has fewer options for directory comparisons, and the **cmp** utility stops after the first difference in a file comparison and has output that is more cumbersome.

General migration actions for everyone

- **pax**. The **-rw** option works like a copy (instead of making or extracting from a single file archive) for directories, symbolic links, and files. Consider the **-pe** option for saving the attributes when doing the copy. The **-k** option prevents overwriting of existing files. The **-C** option causes **pax** to continue after encountering an error on the source file system. That is, **pax** prints an error message and returns a nonzero value after the command ends. Errors on the target file system (such as out of space or write errors) still cause the **pax** command to end as it always has.

To determine what you need to migrate, first compare the ServerPac /etc and /var file systems with your existing /etc and /var file systems. Mount a copy of your existing /etc and /var file systems to a location outside of the ServerPac file system. For instance, you might have your ServerPac file systems at /ServerPac/zOS_Rx/etc and /ServerPac/zOS_Rx/var, and your existing file systems at /Service/ImageX/etc and /Service/ImageX/var. You might have several file systems to mount that are copies of each of your image's /etc and /var file systems (ImageX, ImageY, and ImageZ, for instance). To compare the ServerPac and existing system's /etc and /var, you can run two z/OS UNIX commands, such as:

```
diff -r /ServerPac/zOS_Rx/etc /Service/ImageX/etc
diff -r /ServerPac/zOS_Rx/var /Service/ImageX/var
```

These command results will give you a list of the changes that your existing system's /etc and /var file systems are missing—both the structure differences and the file content differences.

After you determine which directories, symbolic links, and files you are missing from your existing system, you can use one of several ways to propagate the ServerPac information forward:

- You could use the **pax** command (with the **-k** option) to copy from the ServerPac /etc and /var file systems to each of your existing system's /etc and /var file systems. For example:

```
cd /ServerPac/zOS_Rx/etc
pax -rvwkC -pe * /Service/ImageX/etc
```

Another example:

```
cd /ServerPac/zOS_Rx/var
pax -rvwkC -pe * /Service/ImageX/var
```

The **pax** command is a good choice because it copies all files, directories, and symbolic links for each file system from the ServerPac system using a single command without overlaying any existing files.

- You could rerun the product-supplied MKDIR jobs to recreate the directories and symbolic links on each of your existing system's /etc and /var file systems. (A list of the MKDIR jobs is found in *z/OS Program Directory* and the other program directories for the products that were in your ServerPac order.) MKDIR jobs are designed to be run multiple times without damaging your existing file system. For the files under /var/ocsf, rerun the OCSF-supplied ocsf_install_crypto installation script. Or, you can combine these jobs and script them into a single batch job to make the execution more consolidated and repeatable.

After you have made the changes to a copy of your existing image's /etc and /var file systems, you can unmount them and use them for your deployment of the ServerPac system, as your schedule indicates. Remember, you are using *copies* of your existing /etc and /var file systems, and you are *preserving* what you had previously by modifying copies, so your customization for those specific existing images is not lost.

Reference information

For more information, see *z/OS Program Directory* at the z/OS installation related information website.

Update automation and procedures for changed and deleted messages

Description

Every release, many messages change and some are deleted. If you use automation programs to handle messages, or you have operator or other procedures that deal with messages, you should update the programs or procedures.

Table 13 provides more details about this migration action. Use this information to plan your changes to the system.

Table 13. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action that is not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use automation programs or other procedures to handle messages.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Review the lists of changed and deleted messages in *z/OS Summary of Message and Interface Changes*. Update programs that automate on these messages and make other necessary accommodations.

Also, see the following migration actions, which have more details about particular message changes:

- “Update automation for changed DFSORT messages” on page 396
- “Update automation that handles messages IEE302I, IEE303I, IEE1302I, IEE1303I, and IOS566I” on page 272
- “IP Services: Update automation to monitor resolver address space initialization completion messages” on page 328
- “IP Services: Update automation on D TCPIP,tproc,<Telnet>,CONN for the expanded EN TY column in message EZZ6064I” on page 327

Reference information

For a list of new, changed, and deleted messages, see *z/OS Summary of Message and Interface Changes*.

Rework and install user modifications

Description

A user modification is a change constructed by a user to modify an existing function, add to an existing function, or add a user-defined function. Common types of user modifications are:

- User-written and vendor-written exit routines.
- User-written and vendor-written SVCs.

General migration actions for everyone

- User-written and vendor-written termination routines.
- Modifications of IBM source code.
- Unit information modules (UIMs) for non-IBM hardware.
- User-written and vendor-written modules that are listed in a NUCLSTxx parmlib member.
- Updates to default modules to set site defaults differently than the IBM-supplied defaults, such as for the following element and features:
 - XL C/C++
 - DFSORT. Consider using ICEPRMxx parmlib members, introduced in z/OS V1R10, to eliminate the assembler language installation option modules.
 - HLASM.
 - ISPF (specifically, the ISPF configuration table).
 - Language Environment[®]. Consider using the CEEROPT module, which can be used to specify runtime options for CICS[®], IMS[™] LRR, and other LRR users. Beginning in z/OS V2R1, for other assembler language runtime option modules, you must migrate to use the CEEPRMxx parmlib member. See “Convert to CEEPRMxx to set system-level default runtime options” on page 453 for more information about CEEPRMxx.
 - SDSF. See “Use dynamic statements for ISFPARMS to avoid reassembly” on page 226 for more information.

If you made any user modifications, you must determine which ones need to be reworked and which ones just need to be reinstalled.

Table 14 provides more details about this migration action. Use this information to plan your changes to the system.

Table 14. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2
Is the migration action required?	Yes, if you made any user modifications.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Use the z/OS SMP/E Planning and Migration Assistant to help determine which user modifications need to be reworked and which just have to be reinstalled. The Top or New Intermediate Product Migration Changes Report uses data found on your system, combined with IBM-supplied information from the Software Information Base, to show you the current levels of products available as well as product migration and functional changes using a comparison of FMIDs. You can use this report to determine the product migration impacts by reviewing the “changed” FMIDs. This can help you assess how many user modifications have to be reworked if you issued the LIST SYSMOD USERMOD FORFMID (listing the “changed” FMIDs) command. All other user modifications can be reinstalled without having to be reworked.

Note: IBM recommends using exit routines for any user modifications where possible, and installing the exit routines with SMP/E. By using SMP/E, it is easier to bring forward modifications to the z/OS release you are installing.

Reference information

For more information, see the following references:

- For information about SDSF customization, see *z/OS SDSF Operation and Customization*.
- For information about XL C/C++ customization, see *z/OS XL C/C++ User's Guide*.
- For information about DFSORT customization, see *z/OS DFSORT Installation and Customization*.
- For information about HLASM customization, see *HLASM Installation and Customization Guide*.
- For information about ISPF customization, see *z/OS V2R2 ISPF Planning and Customizing*.
- For information about Language Environment customization, see *z/OS Language Environment Customization*.

Reconnect non-IBM products

Description

If you use any independent software vendor (ISV) products, you must make them usable with the new system.

Table 15 provides more details about this migration action. Use this information to plan your changes to the system.

Table 15. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use any ISV products and need to reconnect them after performing a ServerPac installation.
Target system hardware requirements:	None.
Target system software requirements :	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Check with your ISVs to make sure the product levels you are using support the new z/OS release, and then reconnect your ISV products to the new release of z/OS following the instructions provided by the ISVs. If any ISV products do not need to be installed in the same libraries and zones as z/OS, place them in their own sets of libraries and SMP/E zones. This means that, unless you have to change ISV product code, such as installing PTFs, or obtain a new level of the product, you will not need to reinstall it after you install a new ServerPac.

Reference information

For more information, see the following references:

General migration actions for everyone

- For a list of independent software vendors (ISVs) that support z/OS, and announcements, testimonials, and other information, see <http://www.ibm.com/systems/z/solutions/isv/>.
- For a directory of ISV products that support z/OS, see the Global Solutions Directory at <http://www.ibm.com/software/solutions/isv>.

Reconnect subsystems

Description

If you use subsystems, you need to make them usable with the new system.

Table 16 provides more details about this migration action. Use this information to plan your changes to the system.

Table 16. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action that is not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use CICS, DB2 [®] , IMS, or NCP on your new system.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Ensure that any required target system PTFs are installed before you use the subsystem with the new z/OS system. This work includes any required SVCs, system modifications, parmlib setup, and proclib setup. Follow the instructions for the subsystem that you need to reconnect.

Tip: The required IBM PTFs for z/OS V2R2 are identified with the FIXCAT IBM.TargetSystem-RequiredService.z/OS.V2R2

Reference information

None.

Update operational and other procedures

Description

Depending on which method you used to install (ServerPac, CBPDO, or another deliverable), and which functions you plan to exploit, you might need to update the operation, automation, administration, security, backup, and recovery procedures for your site.

Table 17. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.

Table 17. Information about this migration action (continued)

Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Review your operation, automation, administration, security, backup, and recovery procedures, and make any necessary changes depending on how you installed and which functions you plan to exploit. Some possible changes are:

- Allowing applicable users access to new high-level qualifiers. The default new high-level qualifiers are shown in “Add references to new data sets and paths” on page 36.
- Updating and testing your backup and recovery procedures to accommodate the new target system.
- Updating and testing any disaster recovery procedures.
- Updating and testing any automation procedures to take advantage of new functions.
- Updating security system definitions, such as defining new users and resources, permitting users to use new resources, and defining new profiles in the RACF FACILITY class.

Reference information

None.

Verify that virtual storage limits are set properly

Description

Virtual storage requirements can grow from release to release. You should review the virtual storage limits that you want to set. Generally, there are two areas of concern: common areas (above and below the 16 MB line) and individual address spaces. An increase in virtual storage for common areas reduces the virtual storage size of all address spaces. An increase in virtual storage for individual address spaces impacts only the individual address spaces.

Table 18 provides more details about this migration action. Use this information to plan your changes to the system.

Table 18. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.

General migration actions for everyone

Table 18. Information about this migration action (continued)

Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	Use IBM Health Checker for z/OS to help determine whether your virtual storage limits are set properly. The check RSM_MEMLIMIT checks the current setting for the MEMLIMIT parameter in SMFPRMxx, which affects the amount of virtual storage above the 2 GB bar that is available to jobs. This check verifies that a nonzero MEMLIMIT value is in use.

Steps to take

Determine how much virtual storage use to allow above the 2 GB bar. While there is no practical limit to the number of virtual addresses an address space can request above the bar, the system can limit the amount of virtual storage above the bar that an address space is allowed to use. The amount of virtual storage above the bar is determined as follows. The MEMLIMIT parameter in parmlib member SMFPRMxx sets the default system-wide limit, which defaults to 2 GB as of z/OS V1R10 (and zero before z/OS V1R10). However, the system-wide default MEMLIMIT can be overridden by specifying REGION=0M or MEMLIMIT on JOB or EXEC statements in JCL. To set a limit on the use of virtual storage above the bar, use the SMF exit IEFUSI. For more information, see “Limiting the use of memory objects” in *z/OS MVS Programming: Extended Addressability Guide*.

If you want to control the use of virtual storage above the 2 GB bar, do one or more of the following:

- The MEMLIMIT default is 2 GB. If this 2 GB default value is acceptable to you, no change to SMFPRMxx is necessary. (Before z/OS V1R10, the default MEMLIMIT was zero, and you had to specify a nonzero MEMLIMIT in an active SMFPRMxx member of parmlib to establish a system default other than zero for available virtual storage above 2 GB.)
- You can specify MEMLIMIT explicitly in JCL to override the system default that was set (or allowed to default) in SMFPRMxx.
- You can specify REGION=0M on the job statement in JCL to implicitly set MEMLIMIT to NOLIMIT, which also overrides the system default (from SMFPRMxx).
- You can use IEFUSI both to establish a system default MEMLIMIT for different classes of work (for example, JOB, TSO, STC) and limit the amount of virtual storage that can be used above the bar, provided that an explicit or implicit nonzero MEMLIMIT is in effect from JCL or SMFPRMxx. As of z/OS V1R10, keyword HONORIEFUSIREGION | NOHONORIEFUSIREGION is available in SCHEDxx to identify if the region and MEMLIMIT settings specified through or otherwise affected by the IEFUSI exit are to take effect for a program. If you are overriding the attribute of HASJES20 (JES2) in SCHEDxx parmlib member, specify NOHONORIEFUSIREGION explicitly so the default of HONORIEFUSIREGION is not used for this program.

Reference information

For more information, see the following references:

- Information about how to evaluate the real storage configuration can be found in the IBM Washington Systems Center (WSC) white paper *z/OS Performance: Managing Processor Storage in an all “Real” Environment* at <ftp://public.dhe.ibm.com/software/mktsupport/techdocs/allreal.pdf>. Search for “WP100269”.
- For more information about controlling region size and region limits by using the IEFUSI exit, see *z/OS MVS Initialization and Tuning Guide*.

- For more information about the HONORIEFUSIREGION keyword, see *z/OS MVS Initialization and Tuning Reference*.
- Consider using the functions that are available through the new SMFLIMxx parmlib member and REGIONX JCL keyword. See *z/OS MVS Initialization and Tuning Guide* and *z/OS MVS JCL Reference*.

Back virtual storage with sufficient real and auxiliary storage

Description

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.

Table 19 provides more details about this migration action. Use this information to plan your changes to the system.

Table 19. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Using an RMF™ report, determine whether additional real or auxiliary storage is needed by checking the following real storage concentration indicators:

- UIC and average available frames
- Demand page rates
- Percentage of auxiliary slots in use

Reference information

For more information about memory objects, see the following references:

- *z/OS MVS Programming: Extended Addressability Guide*.
- Washington Systems Center flash 10165 at <http://www.ibm.com/support/techdocs>. Search for “flash10165”.

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

Description

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 V2R2:

- CATALOG_ATTRIBUTE_CHECK

General migration actions for everyone

- CTRACE_DEFAULT_OR_MIN
- DMO_REFUCB
- ICSF_KEY_EXPIRATION (added in ICSF FMID HCR77B0)
- IOS_DYNAMIC_ROUTING
- JES3_DATASET_INTEGRITY
- JES3_DOT_POOL_USAGE
- JES3_JET_POOL_USAGE
- JES3_OST_POOL_USAGE
- JES3_SEE_POOL_USAGE
- PFA_PRIVATE_STORAGE_EXHAUSTION
- RACF_ENCRYPTION_ALGORITHM
- RACF_PASSWORD_CONTROLS
- RACF_RRSF_RESOURCES
- TSOE_OPERSEWAIT_SETTING
- USS_KERNEL_RESOURCES_THRESHOLD
- ZFS_CACHE_REMOVALS

The following Health Checks are changed by IBM in z/OS V2R2:

- ASM_PLPA_COMMON_SIZE
- ASM_PLPA_COMMON_USAGE
- CNZ_Task_Table
- RACF_SENSITIVE_RESOURCES
- RSM_HVSHARE
- USS_KERNEL_PVTSTG_THRESHOLD
- XCF_CF_STR_PREFLIST
- ZFS_VERIFY_CACHESIZE
- ZOSMIGREC_SUP_TIMER_INUSE
- ZOSMIGV2R1_ZFS_VERIFY_CACHESIZE

The following Health Checks are deleted by IBM in z/OS V2R2:

- USS_KERNEL_STACKS_THRESHOLD
- ZOSMIGREC_ZFS_RM_MULTIFS
- ZOSMIGV1R13_ZFS_FILESYS
- ZOSMIGV2R1_CS_GATEWAY
- ZOSMIGV2R1_CS_LEGACYDEVICE
- ZOSMIGV2R1_DEFAULT_UNIX_ID

The following Health Checks were new in z/OS V2R1:

- CATALOG_RNLS
- ICSF_COPROCESSOR_STATE_NEGCHANGE
- ICSF_MASTER_KEY_CONSISTENCY
- ICSFMIG_DEPRECATED_SERV_WARNINGS
- IOS_IORATE_MONITOR
- IOS_FABRIC_MONITOR
- RACF_AIM_STAGE
- RACF_CERTIFICATE_EXPIRATION
- RACF_UNIX_ID
- SUP_SYSTEM_SYMBOL_TABLE_SIZE. See “Accommodate the SETLOAD xx,IEASYM command to update system symbols” on page 300.
- SYSTRACE_MODE
- SYSTRACE_BRANCH
- OCE_XTIOT_CHECK
- USS_KERNEL_PVTSTG_THRESHOLD
- USS_KERNEL_STACKS_THRESHOLD
- VLF_MAXVIRT
- XCF_CF_STR_SCM_UTILIZATION

- XCF_CF_SCM_UTILIZATION
- XCF_CF_STR_MAXSCM
- XCF_CF_STR_MAXSPACE
- XCF_CF_STR_SCM_MAXSIZE
- ZOSMIGV2R2_Next_CS_SENDMAILDAEMN
- ZOSMIGV2R2_Next_CS_SENDMAILCLIEN
- ZOSMIGV2R2_Next_CS_SENDMAILMTA
- ZOSMIGV2R2_Next_CS_SENDMAILMSA
- ZOSMIGV2R2_Next_CS_SMTPDDAEMON
- ZOSMIGV2R2_Next_CS_SMTPDMTA
- ZOSMIGV2R2_NEXT_CS_LEGACYDEVICE

The following Health Checks were changed by IBM in z/OS V2R1:

- ASM_LOCAL_SLOT_USAGE
- ASM_PLPA_COMMON_USAGE
- ASM_PLPA_COMMON_SIZE
- CATALOG_IMBED_REPLICATE
- RACF_classname_ACTIVE
- RACF_SENSITIVE_RESOURCES
- SLIP_PER
- VSM_CSA_LARGEST_FREE
- VSM_CSA_THRESHOLD
- VSM_SQA_THRESHOLD
- ZOSMIGV1R11_CS_DNSBIND

The following Health Checks were deleted by IBM in z/OS V2R1:

- CEE_USING_LE_PARMLIB
- PFA_FRAMES_AND_SLOTS_USAGE

Table 20 provides more details about this migration action. Use this information to plan your changes to the system.

Table 20. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	No, but recommended to ensure that your checks continue to work as you intend them to work.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	See "Steps to take."

Steps to take

Follow these steps:

1. Refer to the updated checks in *IBM Health Checker for z/OS User's Guide*.
2. Review changes you made for those checks, in HZSPRMxx parmlib members, for example.

General migration actions for everyone

3. Make any further updates for the checks to ensure that they continue to work as intended.

Reference information

For information about updating the checks, see *IBM Health Checker for z/OS User's Guide*.

Remove deleted data sets, paths, and references

Description

Data sets and paths are routinely removed from z/OS for reasons such as consolidation of data sets and removal of elements and features. You must determine whether these changes affect your environment.

Table 21 provides more details about this migration action. Use this information to plan your changes to the system.

Table 21. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Using Table 22 on page 29 and Table 23 on page 36 as a guide, remove data sets and paths that do not exist in the current release (z/OS V2R2). Also, remove references to them. You might find references in the following places:

- Parmlib
- Proclib
- Logon procedures
- Catalogs
- Security definitions, including program control definitions
- DFSMS ACS routines
- /etc/profile
- SMP/E DDDEF entry
- Backup and recovery procedures, as well as any references to them

In the tables, the data sets are identified as distribution library (DLIB) data sets or target library data sets.

Note: Do not remove any data sets, paths, or references that are needed by earlier-level systems until those systems no longer need them.

General migration actions for everyone

Table 22. Data sets and paths deleted from z/OS V2R2 (in alphabetic order by DDDEF name)

DDDEF	Data set name or path (high-level qualifiers are defaults)	DLIB or target	From element or feature	When deleted	Why deleted
AEOYADEU	EOY.AEOYADEU	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYAENU	EOY.AEOYAENU	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYAESP	EOY.AEOYAESP	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYAFRA	EOY.AEOYAFRA	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYAFRC	EOY.AEOYAFRC	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYAPTB	EOY.AEOYAPTB	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYIDEU	EOY.AEOYIDEU	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYIENU	EOY.AEOYIENU	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYIESP	EOY.AEOYIESP	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYIFRA	EOY.AEOYIFRA	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYIFRC	EOY.AEOYIFRC	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYIPRF	EOY.AEOYIPRF	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYIPTB	EOY.AEOYIPTB	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYMC30	EOY.AEOYMC30	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYMC40	EOY.AEOYMC40	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYODEU	EOY.AEOYODEU	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYOENU	EOY.AEOYOENU	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYOESP	EOY.AEOYOESP	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYOFRA	EOY.AEOYOFRA	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYOFRC	EOY.AEOYOFRC	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOYOPTB	EOY.AEOYOPTB	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOY1DEU	EOY.AEOY1DEU	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS

General migration actions for everyone

Table 22. Data sets and paths deleted from z/OS V2R2 (in alphabetic order by DDDEF name) (continued)

DDDEF	Data set name or path (high-level qualifiers are defaults)	DLIB or target	From element or feature	When deleted	Why deleted
AEOY1ENU	EOY.AEOY1ENU	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOY1ESP	EOY.AEOY1ESP	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOY1FRA	EOY.AEOY1FRA	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOY1FRC	EOY.AEOY1FRC	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOY1PTB	EOY.AEOY1PTB	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOY2DEU	EOY.AEOY2DEU	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOY2ENU	EOY.AEOY2ENU	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOY2ESP	EOY.AEOY2ESP	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOY2FRA	EOY.AEOY2FRA	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOY2FRC	EOY.AEOY2FRC	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOY2PTB	EOY.AEOY2PTB	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOY4DEU	EOY.AEOY4DEU	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOY4ENU	EOY.AEOY4ENU	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOY4ESP	EOY.AEOY4ESP	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOY4FRA	EOY.AEOY4FRA	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOY4FRC	EOY.AEOY4FRC	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOY4PTB	EOY.AEOY4PTB	DLIB	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AIMWEMOD	IMW.AIMWEMOD	DLIB	IBM HTTP Server powered by Domino	z/OS V2R2	Element was removed from z/OS
AIMWHENU	IMW.AIMWHENU	DLIB	IBM HTTP Server powered by Domino	z/OS V2R2	Element was removed from z/OS
AIMWHJPN	IMW.AIMWHJPN	DLIB	IBM HTTP Server powered by Domino	z/OS V2R2	Element was removed from z/OS
AIMWSAM1	IMW.AIMWSAM1	DLIB	IBM HTTP Server powered by Domino	z/OS V2R2	Element was removed from z/OS
AISFMOD1	ISF.AISFMOD1	DLIB	SDSF JES2 support	z/OS V2R2	Obsolete

General migration actions for everyone

Table 22. Data sets and paths deleted from z/OS V2R2 (in alphabetic order by DDDEF name) (continued)

DDDEF	Data set name or path (high-level qualifiers are defaults)	DLIB or target	From element or feature	When deleted	Why deleted
AISFSRC1	ISF.AISFSRC1	DLIB	SDSF JES2 support	z/OS V2R2	Obsolete
AISFJCL1	ISF.AISFJCL1	DLIB	SDSF JES2 support	z/OS V2R2	Obsolete
	/usr/lpp/pkiserv/samples/ihs7		PKI Services	V2R2	Removed the configuration samples for IBM HTTP Server powered by Domino.
SEOYADEU	EOY.SEOYADEU	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOYAENU	EOY.SEOYAENU	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOYAESP	EOY.SEOYAESP	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOYAFRA	EOY.SEOYAFRA	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOYAFRC	EOY.SEOYAFRC	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOYAPTB	EOY.SEOYAPTB	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOYIDEU	EOY.SEOYIDEU	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOYIENU	EOY.SEOYIENU	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOYIESP	EOY.SEOYIESP	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOYIFRA	EOY.SEOYIFRA	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOYIFRC	EOY.SEOYIFRC	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOYIPRF	EOY.SEOYIPRF	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOYIPTB	EOY.SEOYIPTB	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOYMC30	EOY.SEOYMC30	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOYMC40	EOY.SEOYMC40	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOYODEU	EOY.SEOYODEU	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOYOENU	EOY.SEOYOENU	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOYOESP	EOY.SEOYOESP	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOYOFRA	EOY.SEOYOFRA	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS

General migration actions for everyone

Table 22. Data sets and paths deleted from z/OS V2R2 (in alphabetic order by DDDEF name) (continued)

DDDEF	Data set name or path (high-level qualifiers are defaults)	DLIB or target	From element or feature	When deleted	Why deleted
SEYOFRFC	EOY.SEYOFRFC	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEYOPTB	EOY.SEYOPTB	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOY1DEU	EOY.SEOY1DEU	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOY1ENU	EOY.SEOY1ENU	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOY1ESP	EOY.SEOY1ESP	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOY1FRA	EOY.SEOY1FRA	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOY1FRC	EOY.SEOY1FRC	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOY1PTB	EOY.SEOY1PTB	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOY2DEU	EOY.SEOY2DEU	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOY2ENU	EOY.SEOY2ENU	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
AEOY2ESP	EOY.AEOY2ESP	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOY2FRA	EOY.SEOY2FRA	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOY2FRC	EOY.SEOY2FRC	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOY2PTB	EOY.SEOY2PTB	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOY4DEU	EOY.SEOY4DEU	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOY4ENU	EOY.SEOY4ENU	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOY4ESP	EOY.SEOY4ESP	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOY4FRA	EOY.SEOY4FRA	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOY4FRC	EOY.SEOY4FRC	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SEOY4PTB	EOY.SEOY4PTB	Target	BookManager BUILD	z/OS V2R2	Element was removed from z/OS
SIMWTBL	IMW.SIMWTBL1	Target	IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SISFMOD1	ISF.SISFMOD1	Target	SDSF JES2 support	z/OS V2R2	Obsolete

General migration actions for everyone

Table 22. Data sets and paths deleted from z/OS V2R2 (in alphabetic order by DDDEF name) (continued)

DDDEF	Data set name or path (high-level qualifiers are defaults)	DLIB or target	From element or feature	When deleted	Why deleted
SISFSRC1	ISF.SISFSRC1	Target	SDSF JES2 support	z/OS V2R2	Obsolete
SISFJCL1	ISF.SISFJCL1	Target	SDSF JES2 support	z/OS V2R2	Obsolete
SIMWIB	/usr/lpp/internet/bin/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWINC	/usr/lpp/internet/C/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWINJ	/usr/lpp/internet/Ja_JP/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWIS	/usr/lpp/internet/sbin/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSA	/usr/lpp/internet/samples/API/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSAWC	/usr/lpp/internet/server_root/admin-bin/webexec/C/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSAWJ	/usr/lpp/internet/server_root/admin-bin/webexec/Ja_JP/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSCC	/usr/lpp/internet/samples/config/C/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSCJ	/usr/lpp/internet/samples/config/Ja_JP/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSPJC	/usr/lpp/internet/server_root/pub/reports/javelin/C/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSPJJ	/usr/lpp/internet/server_root/pub/reports/javelin/Ja_JP/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSPPC	/usr/lpp/internet/server_root/pub/PICSxmp/C/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSPPJ	/usr/lpp/internet/server_root/pub/PICSxmp/Ja_JP/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSPRJ	/usr/lpp/internet/server_root/pub/reports/java/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS

General migration actions for everyone

Table 22. Data sets and paths deleted from z/OS V2R2 (in alphabetic order by DDDEF name) (continued)

DDDEF	Data set name or path (high-level qualifiers are defaults)	DLIB or target	From element or feature	When deleted	Why deleted
SIMWSRA	/usr/lpp/internet/ server_root /Admin/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRAB	/usr/lpp/internet/ server_root /admin-bin/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRAC	/usr/lpp/internet/ server_root /Admin/C/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRAJ	/usr/lpp/internet/ server_root /Admin/Ja_Jp/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRAW	/usr/lpp/internet/ server_root /admin-bin/ webexec/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRCB	/usr/lpp/internet/ server_root /cgi-bin/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRCO	/usr/lpp/internet/ server_root /Counters/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRDC	/usr/lpp/internet/ server_root /Docs/C/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRDJ	/usr/lpp/internet/ server_root /Docs/Ja_Jp/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRFB	/usr/lpp/internet/ server_root /fcgi-bin/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRFC	/usr/lpp/internet/ server_root /Counters/Fonts/C/ IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRFJ	/usr/lpp/internet/ server_root /Counters/Fonts/ Ja_Jp/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRI	/usr/lpp/internet/ server_root /icons/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRIB	/usr/lpp/internet/ server_root /img-bin/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRLC	/usr/lpp/internet/ server_root /labels/C/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS

General migration actions for everyone

Table 22. Data sets and paths deleted from z/OS V2R2 (in alphabetic order by DDDEF name) (continued)

DDDEF	Data set name or path (high-level qualifiers are defaults)	DLIB or target	From element or feature	When deleted	Why deleted
SIMWSRLJ	/usr/lpp/internet/ server_root /labels/Ja_Jp/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRPC	/usr/lpp/internet/ server_root /pub/C/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRPJ	/usr/lpp/internet/ server_root /pub/Ja_Jp/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRPR	/usr/lpp/internet/ server_root /pub/reports/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRRC	/usr/lpp/internet/ server_root /pub/reports/C/ IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRRJ	/usr/lpp/internet/ server_root /pub/reports/Ja_JP/ IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRWA	/usr/lpp/internet/ server_root /admin-bin/ webexec/com/ibm /webexec/applets/ IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRWH	/usr/lpp/internet/ server_root /admin-bin/ webexec/com/ibm /webexec/herald/ IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRWM	/usr/lpp/internet/ server_root /admin-bin/ webexec/com/ibm /webexec/msgarea/ IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRWN	/usr/lpp/internet/ server_root /admin-bin/ webexec/com/ibm /webexec/navarea/ IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSRWS	/usr/lpp/internet/ server_root /admin-bin/ webexec/servlets/ IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS

General migration actions for everyone

Table 22. Data sets and paths deleted from z/OS V2R2 (in alphabetic order by DDDEF name) (continued)

DDDEF	Data set name or path (high-level qualifiers are defaults)	DLIB or target	From element or feature	When deleted	Why deleted
SIMWSRWU	/usr/lpp/internet/ server_root /admin-bin/ webexec/com/ibm /webexec/util/IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS
SIMWSS	/usr/lpp/internet/ samples/SNMP/ IBM/		IBM HTTP Server - powered by Domino	z/OS V2R2	Element was removed from z/OS

Table 23. Data sets and paths deleted from z/OS V2R1 (in alphabetic order by DDDEF name)

DDDEF	Data set name or path (high-level qualifiers are defaults)	DLIB or target	From element or feature	When deleted	Why deleted
AEPHGIF	EPH.AEPHGIF	DLIB	Library Server	z/OS V2R1	Not needed for z/OS V2R1
AFOMDATA	SYS1.AFOMDATA	DLIB	z/OS UNIX	z/OS V2R1	ICLI removed from z/OS
SFOMDATA	SYS1.SFOMDATA	Target	z/OS UNIX	z/OS V2R1	ICLI removed from z/OS
SFOMEHFS	/usr/lpp/icli/IBM	Target	z/OS UNIX	z/OS V2R1	ICLI removed from z/OS
SFOMESBN	/usr/lpp/icli/sbin/IBM	Target	z/OS UNIX	z/OS V2R1	ICLI removed from z/OS

Reference information

None.

Add references to new data sets and paths

Description

New data sets and paths are routinely added to z/OS for reasons such as consolidation of data sets and addition of new elements and features. You must determine whether these additions affect your environment.

Table 24 provides more details about this migration action. Use this information to plan your changes to the system.

Table 24. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.

Table 24. Information about this migration action (continued)

Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Using Table 25 and Table 26 on page 38 as a guide, add references in the following places for data sets and paths that have been added to z/OS:

- Parmlib
- Proclib
- Logon procedures
- Catalogs
- Security definitions, including program control definitions
- DFSMS ACS routines
- /etc/profile
- SMP/E DDDEF entry
- Backup and recovery procedures, as well as any references to them

Restriction: Some of the data sets shipped with z/OS are PDSEs and are most likely in your LNKST. If one or more are in your LNKST and on your system residence volume, adhere to the following PDSE sharing rules to avoid data set corruption:

- If you specified PDSESHARING(NORMAL), do not share PDSE data sets beyond the scope of the global resource serialization complex.
- If you specified PDSESHARING(EXTENDED), do not share PDSE data sets beyond the scope of the sysplex.

In the tables, the data sets are identified as distribution library (DLIB) data sets or target library data sets.

Table 25. Data sets added to z/OS V2R2 (in alphabetic order by DDDEF name)

DDDEF	Data set name (high-level qualifiers are defaults) or path	DLIB or target	To element or feature	When added	Why added
ACCNSR2	CBC.ACCNSR2	DLIB	XL C/C++	V2R2	New data set for XL C/C++
ACCNSR3	CBC.ACCNSR3	DLIB	XL C/C++	V2R2	New data set for XL C/C++
ACCNSR4	CBC.ACCNSR4	DLIB	XL C/C++	V2R2	New data set for XL C/C++
ACCNSR5	CBC.ACCNSR5	DLIB	XL C/C++	V2R2	New data set for XL C/C++
AHAPEXE3	HAP.AHAPEXE3	DLIB	IBM HTTP Server - Powered by Apache	V2R2	New data set for IBM HTTP Server - Powered by Apache
AHAPINC3	HAP.AHAPINC3	DLIB	IBM HTTP Server - Powered by Apache	V2R2	New data set for IBM HTTP Server - Powered by Apache
AHAPJCL3	HAP.AHAPJCL3	DLIB	IBM HTTP Server - Powered by Apache	V2R2	New data set for IBM HTTP Server - Powered by Apache
AHKCKC4Z	HKC.AHKCKC4Z	DLIB	IBM Knowledge Center for z/OS	V2R2	New data set for IBM Knowledge Center for z/OS
AIZUFS	IZU.AIZUFS	DLIB	IBM z/OS Management Facility	V2R2	New data set for IBM z/OS Management Facility
SCCNM10	CBC.SCCNM10	Target	XL C/C++	V2R2	New data set for XL C/C++

General migration actions for everyone

Table 25. Data sets added to z/OS V2R2 (in alphabetic order by DDDEF name) (continued)

DDDEF	Data set name (high-level qualifiers are defaults) or path	DLIB or target	To element or feature	When added	Why added
SCCNM11	CBC.SCCNM11	Target	XL C/C++	V2R2	New data set for XL C/C++
SCCNN10	CBC.SCCNN10	Target	XL C/C++	V2R2	New data set for XL C/C++
SCCNN11	CBC.SCCNN11	Target	XL C/C++	V2R2	New data set for XL C/C++
SHAPBIN3	/usr/lpp/ihsa_zos/IBM	Target	IBM HTTP Server - Powered by Apache	V2R2	New path for IBM HTTP Server - Powered by Apache
SHAPEXE3	HAP.SHAPEXE3	Target	IBM HTTP Server - Powered by Apache	V2R2	New data set for IBM HTTP Server - Powered by Apache
SHAPJCL3	HAP.SHAPJCL3	Target	IBM HTTP Server - Powered by Apache	V2R2	New data set for IBM HTTP Server - Powered by Apache
SHKCKC4Z	/usr/lpp/kc4z/IBM	Target	IBM Knowledge Center for z/OS	V2R2	New path for IBM Knowledge Center for z/OS
SIZUFSD	/usr/lpp/zosmf/IBM	Target	IBM z/OS Management Facility	V2R2	New path for IBM z/OS Management Facility

Table 26. Data sets added to z/OS V2R1 (in alphabetic order by DDDEF name)

DDDEF	Data set name (high-level qualifiers are defaults) or path	DLIB or target	To element or feature	When added	Why added
AEPHPLIB	EPH.AEPHPLIB	DLIB	Library Server	z/OS V2R1	New data set for Library Server.
AEPHTAB	EPH.AEPHTAB	DLIB	Library Server	z/OS V2R1	New data set for Library Server.
AFNT300	SYS1.AFNT300	DLIB	z/OS Font Collection	z/OS V2R1	Previously existing non-z/OS data set now ships with the z/OS product as of z/OS V2R1. Previously owned by AFP Font Collection.
AFNTDLIB	SYS1.AFNTDLIB	DLIB	z/OS Font Collection	z/OS V2R1	Previously existing non-z/OS data set now ships with the z/OS product as of z/OS V2R1. Previously owned by AFP Font Collection.
AFNTILIB	SYS1.AFNTILIB	DLIB	z/OS Font Collection	z/OS V2R1	Previously existing non-z/OS data set now ships with the z/OS product as of z/OS V2R1. Previously owned by General Font Library.
AFNTLIB	SYS1.AFNTLIB	DLIB	z/OS Font Collection	z/OS V2R1	Previously existing non-z/OS data set now ships with the z/OS product as of z/OS V2R1. Previously owned by Compatibility Fonts feature.

General migration actions for everyone

Table 26. Data sets added to z/OS V2R1 (in alphabetic order by DDDEF name) (continued)

DDDEF	Data set name (high-level qualifiers are defaults) or path	DLIB or target	To element or feature	When added	Why added
AFNTLIBB	SYS1.AFNTLIBB	DLIB	z/OS Font Collection	z/OS V2R1	Previously existing non-z/OS data set now ships with the z/OS product as of z/OS V2R1. Previously owned by AFP Font Collection.
AFONTHFS	SYS1.AFONTHFS	DLIB	z/OS Font Collection	z/OS V2R1	New data set as of z/OS V2R1
FONT300	SYS1.FONT300	Target	z/OS Font Collection	z/OS V2R1	Previously existing non-z/OS data set now ships with the z/OS product as of z/OS V2R1. Previously owned by AFP Font Collection
FONTLIB	SYS1.FONTLIB	Target	z/OS Font Collection	z/OS V2R1	Previously existing non-z/OS data set now ships with the z/OS product as of z/OS V2R1. Previously owned by Compatibility Fonts feature.
FONTLIBB	SYS1.FONTLIBB	Target	z/OS Font Collection	z/OS V2R1	Previously existing non-z/OS data set now ships with the z/OS product as of z/OS V2R1. Previously owned by AFP Font Collection.
SEPHPLIB	/usr/lpp/booksrv/plugins/IBM/	Target	Library Server	z/OS V2R1	New path for Library Server.
SFNTILIB	SYS1.SFNTILIB	Target	z/OS Font Collection	z/OS V2R1	Previously existing non-z/OS data set now ships with the z/OS product as of z/OS V2R1. Previously owned by General Font Library. Note: If you refer to the SYS1.FONTOLN font library for AFP outline fonts, replace the references with SYS1.SFNTILIB, which is the AFP outline font library for z/OS Font Collection.
SFNTWTYP	/usr/lpp/fonts/worldtype/IBM/	Target	z/OS Font Collection	z/OS V2R1	New path as of z/OS V2R1.
SFONDLIB	SYS1.SFONDLIB	Target	z/OS Font Collection	z/OS V2R1	Previously existing non-z/OS data set now ships with the z/OS product as of z/OS V2R1. Previously owned by AFP Font Collection.

General migration actions for everyone

Table 26. Data sets added to z/OS V2R1 (in alphabetic order by DDDEF name) (continued)

DDDEF	Data set name (high-level qualifiers are defaults) or path	DLIB or target	To element or feature	When added	Why added
SHZCINC	/usr/lpp/hzc/include/IBM/	Target	z/OS UNIX	z/OS V2R1	New file system path for zEnterprise Data Compression (zEDC).
SHZCLIB	/usr/lpp/hzc/lib/IBM/	Target	z/OS UNIX	z/OS V2R1	New file system path for zEnterprise Data Compression (zEDC).

Reference information

None.

Verify your IFAPRDxx Product ID is correct for z/OS Version 2 Description

Because z/OS has changed from Version 1 (V1) to Version 2 (V2), the IFAPRDxx parmlib member Product ID should reflect the new program number for z/OS. The Version, Release, and Modification values also found in IFAPRDxx should be specified as "*", so those values do not have to change; only the Product ID is affected by this change.

Table 27 provides more details about this migration action. Use this information to plan your changes to the system.

Table 27. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	If you are sharing the IFAPRDxx parmlib member between z/OS V1 and V2 systems, keep the V1 Product ID statements (for 5694-A01). You can have both the V1 Product ID and the V2 Product ID statements in the same IFAPRDxx parmlib member. After you have completed your migration to z/OS V2, you can remove the V1 Product ID statement from your IFAPRDxx parmlib member.
Restrictions:	None.
System impacts:	Failure to update IFAPRDxx with the correct Product ID statement for z/OS V2 will result in various initialization failures. An example of one of these failures is the following: <pre> IFA104I REGISTRATION HAS BEEN DENIED FOR PRODUCT WITH OWNER=IBM CORP NAME=z/OS FEATURE=TCP/IP BASE VERSION=.. ID=5650-ZOS </pre>

Table 27. Information about this migration action (continued)

Related IBM Health Checker for z/OS check:	None.
--	-------

Steps to take

Follow these steps:

- If you use ServerPac, the customized IFAPRDxx parmlib member has been shipped to you in CPAC.PARMLIB. Verify that you are either using that parmlib member, or have copied its contents to a parmlib member you are using.
- If you are using CBPDO, use provided job ZOSREG in the RIMLIB, to place a customized IFAPRD00 member into your parmlib.

Note: Customers must ensure that the policy in IFAPRDxx enables only the version/release at which they are licensed. Use of and enablement of z/OS features is subject to the z/OS license terms and conditions and must be done with the knowledge of your asset manager according to the terms and conditions for z/OS. For additional license terms and conditions, see the “Usage Restriction” section in the *z/OS Licensed Program Specifications*.

Reference information

For more information, see the following references:

- *z/OS MVS Initialization and Tuning Reference*
- *z/OS Planning for Installation*
- *z/OS Program Directory*, see the z/OS installation related information website.

Accommodate new address spaces

Description

The MAXUSER value in parmlib member IEASYSxx 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.

The following elements add new address spaces for z/OS V2R2:

- IBM HTTP Server - Powered by Apache, which has one or more new address spaces that are associated with it. For information about setting up IBM HTTP Server - Powered by Apache, see *z/OS V2R2.0 HTTP Server - Powered by Apache User's Guide*.
- IBM Knowledge Center for z/OS. This new element in z/OS V2R2 is started in an address space that is an instance of the WebSphere Liberty Profile, which is installed with z/OSMF. For information about setting up IBM Knowledge Center for z/OS, see *IBM Knowledge Center for z/OS Configuration and User Guide*.
- IBM z/OS Management Facility (z/OSMF), which has the address spaces IZUANG1 and IZUSVR1. For information about setting up z/OSMF, see *IBM z/OS Management Facility Configuration Guide*.

The following address spaces were new for z/OS V2R1:

- SDSFAUX (SDSF). With APAR PI43902 (also applicable to z/OS V2R2), SDSF is enhanced with a new, optional address space called SDSFAUX, which provides information about the systems in the sysplex, and their various data set concatenations. The information is shown on the following new SDSF panels and their associated commands: APF, LNK, LPA, PAG, PARM, and SYS.
 - The SDSFAUX address space is automatically started by the SDSF server address space when the server starts, and is automatically stopped when the SDSF server is stopped.
 - For more information about SDSFAUX, see *z/OS SDSF Operation and Customization*.

General migration actions for everyone

- PCIE (PCI Express) and FPGHWAM (Hardware Accelerator Manager). These address spaces provide the infrastructure for PCI Express I/O and hardware accelerator activities. They are started automatically, if z/OS is IPLed on a hardware server capable of supporting the appropriate z/OS PCIE facilities, even if the PCIE facilities are not available on the server. This capability is available on a zEC12 or zBC12 or later. They are persistent address spaces. It is recommended that you do not stop them if any other subsystem relies on them.

When the PCIE and FPGHWAM address spaces are successfully initialized, the following message is displayed:

```
IQP002I PCIE INITIALIZATION COMPLETE
```

If z/OS is IPLed on a server that precedes the zEC12 or zBC12, the following message is written to the hardcopy log:

```
IQP031I REQUESTED SERVICE IS UNSUPPORTED BY HARDWARE
```

For information about the PCIE messages, see *z/OS MVS System Messages, Vol 9 (IGF-IWM)*. For information about the FPGHWAM (Hardware Accelerator Manager) messages, see *z/OS MVS System Messages, Volume 5 (EDG-GFS)*.

PCIE and FPGHWAM do not require any security customization. However, if you are using any enhancements that use this infrastructure, check the documentation for those enhancements to ensure that you apply any specific security customization that might be required for their use.

- IBM Health Checker for z/OS. As of z/OS V2R1 the system starts IBM Health Checker for z/OS address space automatically during system initialization.

For information, see “Convert your existing IBM Health Checker for z/OS setup for automatic start-up” on page 266.

- JES2 Converter/Interpreter. A new persistent address space is used when the interpretation process is performed for a job during the JES2 conversion phase. The address space is only created when INTERPRET=JES is specified on JOBDEF. The number of address spaces that are used depends on the CISUB_PER_AS setting on JOBDEF. The number of conversion processes (PCEDEF CNVTNUM=) divided by the number of subtasks per address space (CISUB_PER_AS) gives the number of address spaces created. The default number of created address spaces is 2 and the maximum number is 25.

The address spaces are named jesxCInn, where jesx is the JES2 subsystem name and xx is a number (01 - 25) to create uniqueness. This address space accesses the PROCLIB data sets defined in the JES2 start PROC and using the JES2 dynamic PROCLIB service.

You must ensure that a proper user ID is assigned to the address space (presumably the same user ID that is assigned to the JES2 address space) by using entries in either the started procedures table (ICHRIN03) or that a STARTED class profile has been defined that matches each new address space names. If you prefer, both the started procedures table and STARTED class profile might be in place. This action ensures that the correct user ID is assigned.

- Generic Tracker (GTZ). As of z/OS V2R1, GTZ replaces the Console Tracking Facility with enhanced capabilities to track use of system functions. For information, see “Move from the console tracking facility to the Generic Tracker” on page 264.

Table 28 provides more details about this migration action. Use this information to plan your changes to the system.

Table 28. Information about this migration action

Element or feature:	BCP, JES, and RMF.
When change was introduced:	<ul style="list-style-type: none"> • z/OS V2R1 for the following: <ul style="list-style-type: none"> – BCP PCIE (PCI Express) and FPGHWAM (Hardware Accelerator Manager). – IBM Health Checker for z/OS – JES2 – GTZ

Table 28. Information about this migration action (continued)

Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	No, but recommended to ensure that your MAXUSER value in parmlib member IEASYSxx is adequate.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If necessary, increase your MAXUSER value in parmlib member IEASYSxx to accommodate the new address spaces. One way to determine how many address spaces you use is to enter the **DISPLAY A,L** command. Then, add the number of address spaces in the IEE114I and IEE115I messages on the old and new systems to determine the total number.

Note:

- A modest overspecification of MAXUSER should not affect system performance.
- The number of total address spaces is the sum of M/S, TS USERS, SYSAS, and INITS.
- If you change the MAXUSER value, you must re-IPL to make the change effective.

Reference information

For more information about the MAXUSER parameter, see *z/OS MVS Initialization and Tuning Reference*.

Migration actions for everyone after the first IPL of z/OS V2R2

This topic describes migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

Hardware migration actions

This topic describes hardware migration actions. The information in this topic is not specifically related to migrating to z/OS V2R2; it only applies if you are changing hardware. Therefore, this topic does not categorize the actions in terms of when they should be performed (before installing, before the first IPL, or after the first IPL).

Migrate to an IBM z13 or IBM z13s server

Description

- | The IBM z13™ (z13) and IBM z13s™ (z13s) are the newest IBM z Systems mainframes, and are distinct from the earlier zEnterprise and other systems. In this publication, these systems are referred to as the z13 and the z13s. z/OS V2R2 running on the z13 or z13s sets the groundwork for digital business by providing the foundation you need to support demanding workloads, such as operational analytics and clouds, and your traditional mission-critical applications.

General migration actions: Hardware

In a Parallel Sysplex that includes a z13 or z13s with either a z/OS system running in at least one LPAR or at least one LPAR being used as a coupling facility (CF), you can include the following servers:

- z13 and z13s servers
- zEC12 and zBC12 servers
- zEnterprise servers (z196 or z114)

The specific z13 and z13s functions, including base support, that are used by z/OS depend on the z/OS release. PTFs might be required for many of these functions. See “Actions you can take before you order a z13 or z13s server” on page 52 for information about finding the appropriate PTFs.

Table 29. z13 and z13s™ server functions included in the base support for z/OS V1R13, z/OS V2R1, and z/OS V2R2

z13 and z13s function included in base z/OS support (Y/N)	V1R13 ¹	V2R1 ¹	V2R2 ¹
Base support	Y	Y	Y
CHPID type CS5 for coupling	Y	Y	Y
CHPID type OSE supporting 4 or 2 ports per feature	Y	Y	Y
CHPID type OSM for intranode management network (INMN)	Y	Y	Y
CHPID type OSN for OSA-Express for NCP (LPAR-to-LPAR)	Y	Y	Y
CPU measurement facility	Y	Y	Y
Crypto Express5S Toleration	Y	Y	Y
FICON® Express® 8S (CHPID FC)	Y	Y	Y
FICON Express16S (CHPID FC)	Y	Y	Y
IBM z BladeCenter Extension (zBX) Model 004	Y	Y	Y
IBM z Unified Resource Manager	Y	Y	Y
New z13 machine instruction (assembler support)	Y	Y	Y
OSA-Express4S (GbE LX and SX, 1000BASE-T, 10 GbE LR and SR)	Y	Y	Y
OSA-Express5S (GbE LX and SX, 1000BASE-T, 10 GbE LR and SR)	Y	Y	Y
Parallel Sysplex InfiniBand (PSIFB) Coupling Link	Y	Y	Y
z/OS global resource serialization (GRS) support for FICON CTCs	Y	Y	Y

Note:

1. PTFs for base support have the following fix category:
 - For z13: “IBM.Device.Server.z13-2964.RequiredService”
 - For z13s: “IBM.Device.Server.z13S-2965.RequiredService”

Table 30. Exploitation of z13 and z13s™ server functions supported by z/OS V1R13, z/OS V2R1, and z/OS V2R2

z13 and z13s function included in base z/OS support (Y/N)	V1R13 ²	V2R1 ²	V2R2 ²
Coupling Facility Control Code (CFCC) Level 20	Y	Y	Y

General migration actions: Hardware

Table 30. Exploitation of z13 and z13s™ server functions supported by z/OS V1R13, z/OS V2R1, and z/OS V2R2 (continued)

z13 and z13s function included in base z/OS support (Y/N)	V1R13 ²	V2R1 ²	V2R2 ²
CFCC Dump Reasons support for CFCC Level 21	N	N	Y
Crypto Express5S support for up to 85 Domains	Y	Y	Y
High Performance FICON (zHPF)	Y	Y	Y
IBM Integrated Coupling Adapter (ICA SR)	Y	Y	Y
Support for 256 coupling CHPIDs	Y	Y	Y
2 GB Large Pages	Y (with the z/OS V1.13 RSM Enablement Offering web deliverable installed)	Y	Y
Checksum offload for IPv6 packets (CHPID OSD)	Y	Y	Y
Checksum offload for LPAR-to-LPAR traffic for IPv4 and IPv6 packets (CHPID OSD)	Y	Y	Y
Crypto Express5S support of VISA Format Preserving Encryption (FPE), Next Generation Coprocessor support	Y (with the Enhanced Cryptographic Support for z/OS V1.13 - V2.1 web deliverable installed)	Y (with the Enhanced Cryptographic Support for z/OS V1.13 - V2.1 web deliverable installed)	Y
Flash Express (Storage Class Memory or SCM)	Y (with the z/OS V1.13 RSM Enablement Offering web deliverable installed)	Y	Y
IBM System Advanced Workload Analysis Reporter (IBM zAware)	Y	Y	Y
Inbound workload queuing for Enterprise Extender (CHPID OSD)	Y	Y	Y
Large Send for IPv6 packets (CHPID OSD)	Y	Y	Y
Manage FICON Dynamic Routing Support	Y	Y	Y
Transactional memory	Y	Y	Y
Up to 4 Subchannels Sets per CSS (z13)	Y	Y	Y
Up to 3 Subchannels Sets per CSS (z13s)	Y	Y	Y
Up to 85 LPARs (z13)	Y	Y	Y
Up to 40 LPARs (z13s)	Y	Y	Y

General migration actions: Hardware

Table 30. Exploitation of z13 and z13s™ server functions supported by z/OS V1R13, z/OS V2R1, and z/OS V2R2 (continued)

z13 and z13s function included in base z/OS support (Y/N)	V1R13 ²	V2R1 ²	V2R2 ²
Greater than 100 CPs per z/OS system image	N	Y (z13 only). The z13 can have a maximum of 128 CPs in non-SMT mode, or up to 213 threads in SMT mode. The z13s can have a maximum of 40 CPs in non-SMT mode, or up to 66 threads in SMT mode.	Y (z13 only). The z13 can have a maximum of 128 CPs in non-SMT mode, or up to 213 threads in SMT mode. The z13s can have a maximum of 40 CPs in non-SMT mode, or up to 66 threads in SMT mode.
Miscellaneous PCIe enhancements	N	Y	Y
RoCE Express for Shared Memory Communications-Remote (SMC-R) Direct Memory Access including shared RoCE Express support	N	Y	Y
Shared Memory Communications-Direct Memory Access (SMC-D)	N	N	Y
Simultaneous multithreading (SMT)	N	Y	Y
Single Instruction Multiple Data (SIMD) instruction set	N	Y	Y
XL C/C++ support of ARCH(11) and TUNE(11) parameters	N	Y (with XL C/C++ V2R1M1 web deliverable with z13 support for z/OS V2.1 installed)	Y
zEDC capability using zEDC Express	N (toleration support provided for software decompression)	Y (requires the z/OS zEDC software feature to be enabled)	Y (requires the z/OS zEDC software feature to be enabled)

Notes:

- PTFs for base support have the following fix category:
 - For z13: "IBM.Device.Server.z13-2964.RequiredService"
 - For z13s: "IBM.Device.Server.z13S-2965.RequiredService"
- PTFs for exploitation have the following fix category:
 - For z13: "IBM.Device.Server.z13-2964.Exploitation"
 - For z13s: "IBM.Device.Server.z13S-2965.Exploitation"

Web deliverables are available from the z/OS downloads page: <http://www.ibm.com/systems/z/os/zos/tools/downloads/index.html>.

Table 31 provides more details about this migration action. Use this information to plan your changes to the system.

Table 31. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	<ul style="list-style-type: none"> IBM z13, which first shipped March 2015. z13s, which first shipped March 2016.
Applies to migration from:	z/OS V2R2, z/OS V2R1, and z/OS V1R13.

Table 31. Information about this migration action (continued)

Timing:	Anytime before you introduce a z13 or z13s server into your environment.
Is the migration action required?	Yes, if you want to run z/OS V2R2, z/OS V2R1, or z/OS V1R13 on a z13 or z13s server, or if you want to run a coupling facility on a z13 or z13s server. If you plan to run only a coupling facility on a z13 or z13s system, only the sysplex-related actions are relevant. However, you must install the appropriate z/OS service for systems that are running on other servers that use the z13 or z13s coupling facilities.
Target system hardware requirements:	<ul style="list-style-type: none"> • A z13 or z13s • Additional hardware required for specific functions. <ul style="list-style-type: none"> – IBM devices previously attached to zEC12, zBC12, and zEnterprise servers are supported for attachment to z13 or z13s channels, unless otherwise noted. The subject I/O devices must meet FICON architecture requirements – IBM zAware requires the following server firmware: <ul style="list-style-type: none"> - IBM zAware 10 pack FC #1010 - IBM zAware 10 pack on a Disaster Recovery Server FC #1011 – Flash Express requires FC #0403 – zEDC Express requires FC #0420 – 10 GbE RoCE Express FC #0411 – Use of IBMWebSphere DataPower® Integration Appliance XI50 for zEnterprise (DataPower XI50z) or select IBM BladeCenter PS701 Express blades or IBM BladeCenter HX5 blades requires a z BladeCenter Extension (zBX) Model 004 – z BladeCenter Extension (zBX) Model 004 requires: <ul style="list-style-type: none"> - AIX® 5.3, AIX 6.1, AIX 7.1 and up, and PowerVM® Enterprise Edition (on POWER7® blade) - Red Hat RHEL 5.5, 6.0, 7.0 and up, SLES 10 (SP4), 11 (SP1), 12 and up, 64-bit only (on HX5 blade) - Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2008 R2, and Microsoft Windows Server 2008 (SP2) (Datacenter Edition recommended), 64-bit only (on HX5 blade) – Use of hardware acceleration for cryptographic operations, including the use of Visa Data Secure Platform (DSP) functions requires a CPACF (FC #3863) or a CEX5S (FC #0890) feature, or both. <p>See Table Note 1.</p> <ul style="list-style-type: none"> • - Use of a Trusted Key Entry (TKE) workstation requires FC #0878.
Target system software requirements:	See the topic “Support is delivered by service, z/OS features, and web deliverables” in “General recommendations and considerations for a z13 or z13s server” on page 48 and “Install the necessary z/OS service”, as indicated in the PSP buckets that are described in “Actions you can take before you order a z13 or z13s server” on page 52.

General migration actions: Hardware

Table 31. Information about this migration action (continued)

Other system (coexistence or fallback) requirements:	<ul style="list-style-type: none">• It is recommended that you install and run the required service on your existing server. This will enable you to fall back from a hardware perspective, yet maintain your software level.• If you have not installed the preconditioning and exploitation PTFs for CFCC Levels 17-19, note that those PTFs are required to be installed throughout your sysplex before implementing CFCC Level 20 or CFCC Level 21..• If you plan to implement zEDC, you should install the z/OS toleration PTFs on systems that access data that is compressed using zEDC Express on a z13 or z13s server.• If you are using ICSF and plan to share keys with other z/OS systems that have an earlier level of ICSF, you should install the ICSF coexistence PTFs on those earlier levels of ICSF.
Restrictions:	See “Restrictions for a z13 or z13s server” on page 50.
System impacts:	None.
Related IBM Health Checker for z/OS check:	A health check for FICON dynamic routing, CHECK(IBMIOS,IOS_FABRIC_MONITOR), is available with the PTF for APAR OA40548 for z/OS V1R13 and V2R1, and included in z/OS V2R2. This health check is designed to check all components of a dynamic routing fabric, the channel subsystem, and disk control units to make sure that dynamic routing requirements are met if dynamic routing is enabled for one or more FICON switches. This support is intended to help you identify misconfiguration errors that can result in data integrity exposures.

Table Note:

1. IBM z Systems cryptography features include Visa Format Preserving Encryption technology (FPE), which is owned by Visa. Clients who wish to use the FPE functionality of IBM z Systems cryptography features must first enter into a separate agreement with Visa for use of this advanced technology; such Clients should contact either their Visa account manager or Visa at P2PE@visa.com. Clients who use IBM z Systems cryptography features, but do not make use of the FPE functionality, are not required to enter into any such agreement with Visa.

Steps to take

Follow the “General recommendations and considerations for a z13 or z13s server,” adhere to the “Restrictions for a z13 or z13s server” on page 50, and perform the tasks that are described in the following topics.

Reference information

None.

General recommendations and considerations for a z13 or z13s server

As you plan your migration to a z13 or z13sTM server, consider the following:

1. **Relatively few migration actions are new when coming from an IBM zEnterprise EC12 or zEnterprise BC12 server.** Migration to an IBM z13 or IBM z13s server has, as its base, a migration to the IBM zEnterprise EC12 or zEnterprise BC12 servers. This means that if you are migrating to a z13 or z13s server from a zEC12 or zBC12 server, and have performed the migration actions associated

with the zEC12 or zBC12, you have fewer migration actions than if you were migrating from an earlier generation server and have not yet performed the migration actions associated with these servers. It is important to note that you can migrate directly to a z13 or z13s server without installing the intermediate servers, but you still need to ensure that any migration considerations are satisfied for the servers that you “skipped.” To read about z196, z114, zEC12, and zBC12 server migration actions, see “Migrate to an IBM zEnterprise z196 or z114 server” on page 72 and “Migrate to an IBM zEnterprise EC12 or IBM zEnterprise BC12 server” on page 60.

2. **Support is delivered by service, z/OS features, and web deliverables.** The base support for the z13 and z13s is delivered by service (PTFs).

- The PSP bucket that contains the required list of PTFs for the z13 server is: Upgrade 2964DEVICE, Subset 2964/ZOS and is identified by the following SMP/E Fix Category IBM.Device.Server.z13-2964.RequiredService
- The PSP bucket that contains the required list of PTFs for the z13s server is: Upgrade 2965DEVICE, Subset 2965/ZOS and is identified by the following SMP/E Fix Category IBM.Device.Server.z13S-2965.RequiredService.

Exploitation of some functions requires a web deliverable. Specifically:

- If you are running z/OS V2R1 and require Crypto Express4S functionality for CCA 4.4 and other EP11 cryptographic enhancement support which includes: RKX Key Export Wrap, UDX Reduction/simplification, additional EP11 algorithms, expanded EMV support, AP Configuration simplification, CTRACE Enhancements, and KDS Key Utilization Stats, then you must download and install the Cryptographic Support for z/OS V1R13-z/OS V2R1 web deliverable (FMID HCR77A1) or the Cryptographic Support for z/OS V1R13 - z/OS V2R2 web deliverable (HCR77B1).

If you are using either of these web deliverables (HCR77A1 or HCR77B1) and sharing keys with other z/OS systems that have a lower-level of ICSF, you require the coexistence PTFs identified by the appropriate Fix Category: IBM.Coexistence.ICSF.z/OS_V1R13-z/OS_V2R1-HCR77A1 or IBM.Coexistence.ICSF.z/OS_V1R13-z/OS_V2R1-HCR77B1.

- If you are running z/OS V2R1 and require Crypto Express5S exploitation support for the next Generation Coprocessor support or VISA Format Preserving Encryption (FPE), you must download and install the Enhanced Cryptographic Support for z/OS V1R13-z/OS V2R1 web deliverable (FMID HCR77B0) or the Cryptographic Support for z/OS V1R13 - z/OS V2R2 web deliverable (HCR77B1).

If you are using either of these web deliverables (HCR77B0 or HCR77B1) and sharing keys with other z/OS systems that have a lower-level of ICSF, you require the coexistence PTFs identified by the appropriate Fix Category: IBM.Coexistence.ICSF.z/OS_V1R13-z/OS_V2R1-HCR77B0 or IBM.Coexistence.ICSF.z/OS_V1R13-z/OS_V2R1-HCR77B1.

- If you are running z/OS V2R1 and require exploitation of new hardware instructions using XL C/C++ ARCH(11) and TUNE(11) including SIMD, vector programming, MASS and ATLAS libraries, you must download and install the XL C/C++ V2R1M1 web deliverable with z13 support for z/OS 2.1.
- If you are running z/OS V1R13 and want to exploit Flash Express (including pageable 1 MB Large Page Support, optional paging of PLPA and Common (CSA, ECSA) pages to Flash Express, and Dynamic reconfiguration support for Flash Express); or 2 GB Large Page support, you must download and install the z/OS V1.13 RSM Enablement Offering Web deliverable and install the required PTFs identified by the Fix Category.
- If you are running z/OS V1R13, you might need to install a Cryptographic Support web deliverable, depending on which ICSF functions you require.

3. **Larger coupling facility structure sizes might be necessary.** When you change coupling facility control code (CFCC) levels, your coupling facility structure sizes might change. If, as part of your migration to a z13 server, you change CFCC levels, you might have larger structure sizes than you did previously. If your CFCC levels are identical, structure sizes are not expected to change when you migrate from a previous server to a newer generation server. In addition, similar to CF Level 17 and later, ensure that the CF LPAR has at least 512MB of storage. CFCC Levels 20 and 21, introduced on the z13 and 13s, support the Coupling Facility use of Large Memory to improve availability for larger

General migration actions: Hardware

CF cache structures and data sharing performance with larger DB2 Group Buffer Pools (GBP). This support removes inhibitors to using large CF cache structures, enabling use of Large Memory to appropriately scale to larger DB2 Local Buffer Pools (LBP) and Group Buffer Pools (GBP) in data sharing environments.

4. **Use the same software level throughout a sysplex.** Having members of a sysplex at the same software level (other than during brief migration periods) is good software management policy.
5. **Migrate hardware and software at different times.** To minimize the amount of change (and therefore risk) that you experience at one time, do not migrate your software release level at the same time that you migrate your hardware.
6. **Update SCRT to latest version.** If you use SCRT, make sure it is at the latest level. This is a requirement for sub-capacity pricing, as well as when you upgrade servers. The latest level of SCRT can be downloaded from the SCRT web site at <http://www.ibm.com/eserver/zseries/swprice/scrt/>.

Restrictions for a z13 or z13s server

Restrictions associated with z13 and z13sTM servers are described as follows:

1. **Functional limitations.** Not all z13 or z13s functions are available in every z/OS release. See Table 29 on page 44 and Table 30 on page 44 for a list of the z13 and z13s functions available in each z/OS release. Some functions have migration or exploitation considerations (see “Actions you can take before you order a z13 or z13s server” on page 52 and “Migration and exploitation considerations for z13 and z13s server functions” on page 56.) Many functions are enabled or disabled, based on the presence or absence of the required hardware and software. If you plan to exploit new z13 or z13s functions, you can install the software and hardware in either order; that is, there is no requirement to install either software or hardware first to exploit a specific function. However, because of outage windows and testing considerations, you might want to consider installing all the software and PTFs required for the machine and the functions you plan to exploit first, then upgrade the hardware and, finally, update your customization to exploit the new functions.
2. **z13 and z13s servers in a sysplex.**
 - A Parallel Sysplex that contains a z13 or z13s server either for a z/OS image or a CF image can only contain other z13 or z13s servers, or z196, z114, zEC12, or zBC12 servers.

If you are running z/OS on any servers earlier than a z196 or z114 server, you cannot add a z13 or z13s server to that sysplex; that is, you will not be able to perform rolling IPLs to introduce a z13 or z13s server if you have any of the earlier servers as z/OS images or coupling facility images in the sysplex.

The earlier servers in the sysplex must be upgraded to z196, z114, or later to have z13 or z13s servers supported in the sysplex. If you have any z/OS images or coupling facility images on an earlier server, and you intend to introduce a z13 or z13s server into that sysplex, you must migrate those images to a z196, z114, or later server before introducing the z13 or z13s server.

GRS supports the use of FICON CTCs for Ring configurations on z/OS V1R13 with a PTF and on z/OS Version 2. However, if you are currently using ESCON CTCs for GRS ring configurations within a sysplex, consider converting to GRS Star if possible, or using XCF signalling in a GRS ring configuration. XCF sysplex signalling is preferred instead of GRS CTC connections.
 - InterSystem Channel 3 (ISC-3) and Integrated Cluster Bus 4 (ICB-4) Coupling Links are not supported on z13 or z13s CPC. Instead, the IBM Integrated Coupling Adapter (ICA SR), introduced on the z13 and z13s, is a two-port, short distance coupling fanout that utilizes a new coupling channel type: CS5. The ICA SR can only be used for coupling connectivity between z13 or z13s servers, and the ICA SR can only connect to another ICA SR. IBM recommends that you order ICA SR (#0172) on the z13 processors used in a Parallel Sysplex to help ensure coupling compatibility with future processor generations. You can also use 12x InfiniBand coupling links, which are designed to replace Integrated Cluster Bus 4 (ICB-4), and to complement 1x InfiniBand and ISC-3 on a z13 or z13s server. InfiniBand coupling can provide significantly improved service times compared to ISC-3s for distances up to 150 meters. You can read about coupling links in *IBM System z[®] Connectivity Handbook* (SG24-5444).

- The z13 or z13s server cannot be connected to a Sysplex Timer (9037-002). The Server Time Protocol (STP) feature is the follow-on to the Sysplex Timer. STP is designed to allow multiple servers and coupling facilities to maintain time synchronization with each other without requiring a Sysplex Timer. STP is a hardware feature of the z13, z13s, zEC12, zBC12, z196, and z114. To implement STP, see the STP web site and the publications and other resources listed there. The STP web site is at <http://www.ibm.com/systems/z/advantages/pso/stp.html> .

The STP design introduced a concept called Coordinated Timing Network (CTN). A CTN is a collection of servers and coupling facilities that are time-synchronized to a time value called Coordinated Server Time. A CTN can be configured in two ways:

- STP-only CTN, which does not require a Sysplex Timer. A z13 or z13s must participate in an STP-only CTN.
- Mixed-CTN (External Time Reference and STP), which does require a Sysplex Timer. zEC12 and zBC12 were the last servers to support mixed-CTN. The z13 and z13s do not support connections to a Mixed-CTN. All servers in the network must be configured in STP-only mode. Consider migrating servers that require time synchronization, such as to support a base or Parallel Sysplex, to the Server Time Protocol (STP).

For more information, see the following references:

- For more information about GRS, see *z/OS MVS Planning: Global Resource Serialization*.
- For more information on CTC definitions, see:
 - *z/OS HCD User's Guide*
 - *z/OS HCD Planning*

3. **Plan for discontinued functions.** For a list of functions on the z13 server that are planned to be discontinued on future servers, see “Accommodate functions for the z13 server or z13s to be discontinued on future servers” on page 59.
4. **Unsupported hardware features.** The following hardware features cannot be ordered and cannot be carried forward from an upgrade on an earlier server to the z13 server.
 - HCA2-O
 - HCA2-O LR
 - ISC-3 links
 - CHPID type OSN (OSA-Express for NCP) is not supported on the OSA-Express5S GbE LX feature
 - Crypto Express3 (#0864)
 - Crypto Express4S (#0865)
 - STP Mixed CTN. The zEC12 and zBC12 were the last z Systems™ servers to support connections to an STP Mixed CTN. This also includes the Sysplex Timer (9037). Starting with z13, servers that require Time synchronization, such as to support a base or Parallel Sysplex, will require Server Time Protocol (STP) and all servers in that network must be configured in STP-only mode.
 - IBM System z Application Assist Processor (zAAP). IBM continues to support running zAAP workloads on IBM System z Integrated Information Processors (zIIPs). IBM has removed the restriction preventing zAAP-eligible workloads from running on zIIPs when a zAAP is installed on the CEC. This was intended to help facilitate migration and testing of zAAP workloads on zIIPs. With a z13, one CP must be installed with the installation of any zIIPs or prior to the installation of any zIIPs. The total number of zIIPs purchased cannot exceed twice the number of CPs purchased. However, for upgrades from zEC12s with zAAPs, conversions from zAAPs may increase this ratio to 4:1.
5. **Carry forward hardware features.** The following hardware features are not orderable on z13 servers. If they are installed on your existing server at the time of an upgrade to a z13 server, they can be retained or carried forward.
 - HMC #0091
 - HCA2-C Fanout #0162
 - IFB-MP Daughter Card #0326
 - STI-A8 Mother Card #0327

General migration actions: Hardware

- Flash Express #0402 and #0403
- OSA-Express4S 1 GbE LX #0404
- OSA-Express4S 1 GbE SX #0405
- OSA-Express4S 10 GbE LR #0406
- OSA-Express4S 10 GbE SR #0407
- OSA-Express4S 1000BASE-T #0408
- OSA-Express5S GbE LX #0413
- OSA-Express5S GbE SX #0414
- OSA-Express5S 10 GbE LR #0415
- OSA-Express5S 10 GbE SR #0416
- OSA-Express5S 1000BASE-T #0417
- TKE workstation #0842
- Addl smart cards #0884
- TKE Smart Card Reader #0885
- FICON Express8 10KM LX #3325
- FICON Express8 SX #3326
- FICON Express8S 10Km LX #0409
- FICON Express8S SX #0410
- 10GbE RoCE Express #0411
- zEDC Express #0420
- Fill and Drain Kit #3378
- Universal Lift Tool/Ladder #3759

Also, FICON Express8 will not be supported on future high-end z Systems servers as carry forward on an upgrade. The z13 and z13s servers will be the last z Systems servers to offer ordering of FICON Express8S channel features. Enterprises that have 2GB device connectivity requirements must carry forward these channels.

See “Ensure that you are running on supported servers and storage controllers” on page 85 for more information.

Actions you can take before you order a z13 or z13s server

You can perform the following migration actions before you order or install a z13 or z13s™ server:

1. **Review the sysplex configuration in which the z13 or z13s server will participate.** See “Restrictions for a z13 or z13s server” on page 50 for a description of the limitations when using z13 or z13s servers with certain earlier servers in a Parallel Sysplex.
2. **Implement an STP timing network.** This action is needed because Sysplex Timers (9037-002) are not supported on z13 or z13s servers.
3. **Migrate from ISC-3 links to Infinband or Integrated Coupling Adapter (ICA) links.** This action is needed because ISC-3 links are not supported on z13 or z13s servers. If desired, you can take this action after you order a z13 or z13s server, as you upgrade to the new server.
4. **Migrate from unsupported hardware features to newer technology.** This action is needed because ESCON, FICON Express4, Crypto Express3, and OSA-Express3 are not supported on z13 or z13s servers. See “Restrictions for a z13 or z13s server” on page 50, “Replace unsupported devices” on page 87, and “Provide for new device installations” on page 88.
5. **Determine the level of cryptographic support you require on a z13 or z13s server.** The level of function provided for cryptographic support differs by z/OS release and the installed ICSF web deliverable. Also, toleration PTFs are available for some cryptographic web deliverables.
For z/OS V2R2, consider the following:
 - If you are using the level of ICSF that is shipped as part of z/OS V2R2, you can use the most functions of the Crypto Express5 feature on a z13 or z13s server.
 - The Cryptographic Support for z/OS V1R13 - z/OS V2R2 web deliverable (FMID HCR77B1) provides some additional function and also incorporates enhancements that are available in PTFs for the base level of ICSF included in z/OS V2R1. The web deliverable includes new operator commands with Parallel Sysplex wide scope that can be used to perform certain cryptographic administrative functions. These functions include activating, deactivating, and restarting

cryptographic coprocessors. This support can also be used to display status for available cryptographic devices and information about active key data sets (KDSs).

For z/OS V2R1, consider the following:

- If you are using the level of ICSF that is shipped as part of z/OS V2R1, you can tolerate Crypto Express5 on a z13 or z13s server, which treats Crypto Express5S cryptographic coprocessors and accelerators as Crypto Express4S coprocessors and accelerators. However, you must install the required PTFs identified by the SMP/E fix category:
 - For the z13: `IBM.Device.Server.z13-2964.RequiredService`
 - For the z13s: `IBM.Device.Server.z13S-2965.RequiredService`
- If you require support for greater than 16 domains (up to 85) on Crypto Express5S, you must install the PTFs that are identified by the appropriate fix category `IBM.Device.Server.z13-2964.Exploitation` or `IBM.Device.Server.z13S-2965.Exploitation`, or install the Enhanced Cryptographic Support for z/OS V1R13-z/OS V2R1 web deliverable (FMID HCR77B0) or a later ICSF web deliverable.
- If you require Crypto Express4S functionality for CCA 4.4 and other EP11 cryptographic enhancement support which includes: RKX Key Export Wrap, UDX simplification, additional EP11 algorithms, expanded EMV support, AP Configuration simplification, CTRACE Enhancements, and KDS Key Utilization stats, you must download and install the Cryptographic Support for z/OS V1R13-z/OS V2R1 web deliverable (FMID HCR77A1) or the Enhanced Cryptographic Support for z/OS V1R13-z/OS V2R1 web deliverable (FMID HCR77B0) or a later ICSF web deliverable.

Note: If you are using the Cryptographic Support for z/OS V1R13-z/OS V2R1 web deliverable (FMID HCR77A1) or a later ICSF web deliverable, and sharing keys with other z/OS systems that have a lower-level of ICSF, you require the coexistence PTFs listed here, which are identified by fix category: `IBM.Coexistence.ICSF.z/OS_V1R13-z/OS_V2R1-HCR77A1`, or the FIXCAT for the ICSF level that you are using.

- If you require Crypto Express5S exploitation support for the next Generation Coprocessor support or VISA Format Preserving Encryption (FPE), you must download and install the Enhanced Cryptographic Support for z/OS V1R13-z/OS V2R1 web deliverable (FMID HCR77B0) or a later ICSF web deliverable.

Note: If you are using the Enhanced Cryptographic Support for z/OS V1R13-z/OS V2R1 Web Deliverable (FMID HCR77B0) or a later ICSF web deliverable, and sharing keys with other z/OS systems that have a lower-level of ICSF, you require the coexistence PTFs listed here, which are identified by fix category: `IBM.Coexistence.ICSF.z/OS_V1R13-z/OS_V2R1-HCR77B0`, or a later ICSF web deliverable.

For z/OS V1R13, consider the following:

- If you are using the level of ICSF that is shipped as part of z/OS V1.13 you can tolerate Crypto Express5 on a z13 server which treats Crypto Express5S cryptographic coprocessors and accelerators as Crypto Express4S coprocessors and accelerators. However you must install the required PTFs identified by the fix category:
 - For the z13: `IBM.Device.Server.z13-2964.RequiredService`
 - For the z13s: `IBM.Device.Server.z13S-2965.RequiredService`
- If you require Crypto Express4S support of expanded key support for AES algorithm, enhanced ANSI TR-31 Secure Key Exchange, PIN block decimalization table protection, PKA RSA OAEP with SHA-256 algorithm, or additional Elliptic Curve Cryptography (ECC) functions, then you must download and install the Cryptographic Support for z/OS V1R11-V1R13 (or higher) web deliverable (FMID HCR7790) and the PTFs identified by the fix category:
 - For the z13: `IBM.Device.Server.z13-2964.Exploitation`
 - For the z13s: `IBM.Device.Server.z13S-2965.Exploitation`

General migration actions: Hardware

Note: If you are using the Cryptographic Support for z/OS V1R11-V1R13 Web Deliverable (FMID HCR7790) and sharing keys with other z/OS systems that have a lower-level of ICSF, you require the coexistence PTFs that are identified by fix category IBM.Coexistence.ICSF.z/OS_V1R11-V1R13-HCR7790, or a later ICSF web deliverable.

- If you require Crypto Express4S functionality including: Enterprise Security PKCS #11-Hardware Security Module (HSM), DUKPT for MAC and Data Encryption, Cipher Text Translate CCA Verb, PKDS/TKDS Constraint Relief, Random Number Cache, FIPS on Demand, or Wrapping Keys with Strong Keys, then you must download and install the Cryptographic Support for z/OS V1R12-V1R13 (or higher) web deliverable (FMID HCR77A0). The APARs/PTFs required to provide support for PKCS#11 are identified by the fix category:
 - For the z13: IBM.Device.Server.z13-2964.Exploitation
 - For the z13s: IBM.Device.Server.z13S-2965.Exploitation

Note: If you are using the Cryptographic Support for z/OS V1R12-V1R13 Web Deliverable (FMID HCR77A0) and sharing keys with other z/OS systems that have a lower-level of ICSF, you require the coexistence PTFs listed here, which are identified by fix category IBM.Coexistence.ICSF.z/OS_V1R12-V1R13-HCR77A0.

- If you require Crypto Express4S functionality for CCA 4.4 and other EP11 cryptographic enhancement support which includes: RKX Key Export Wrap, UDX Reduction/simplification, additional EP11 algorithms, expanded EMV support, AP Configuration simplification, CTRACE Enhancements, and KDS Key Utilization Stats; then you must download and install the Cryptographic Support for z/OS V1R13-z/OS V2R1 (or higher) web deliverable (FMID HCR77A1). The APARs and PTFs that are required to provide support for PKCS#11 are identified by the fix category:
 - For the z13: IBM.Device.Server.z13-2964.Exploitation
 - For the z13s: IBM.Device.Server.z13S-2965.Exploitation

Note: If you are using the Cryptographic Support for z/OS V1R13-z/OS V2R1 Web Deliverable (FMID HCR77A1) and sharing keys with other z/OS systems that have a lower-level of ICSF, you require the coexistence PTFs that are identified by fix category IBM.Coexistence.ICSF.z/OS_V1R13-z/OS_V2R1-HCR77A1, or the FIXCAT for the ICSF level that you are using.

- If you require support for greater than 16 domains (up to 85) on Crypto Express5S, you must install the PTFs that are identified by the fix category: IBM.Device.Server.z13-2964.Exploitation or IBM.Device.Server.z13S-2965.Exploitation, or install the Enhanced Cryptographic Support for z/OS V1R13-z/OS V2R1 web deliverable (FMID HCR77B0)
- If you require Crypto Express5S exploitation support for the next Generation Coprocessor support or VISA Format Preserving Encryption (FPE), you must download and install the Enhanced Cryptographic Support for z/OS V1R13-z/OS V2R1 web deliverable (FMID HCR77B0).

Note: If you are using the Enhanced Cryptographic Support for z/OS V1R13-z/OS V2R1 Web Deliverable (FMID HCR77B0) and sharing keys with other z/OS systems that have a lower-level of ICSF, you require the coexistence PTFs listed here, which are identified by fix category IBM.Coexistence.ICSF.z/OS_V1R13-z/OS_V2R1-HCR77B0, or the FIXCAT for the ICSF level that you are using.

6. **Install the necessary z/OS service, as indicated in PSP buckets.** You must obtain all of the appropriate Preventive Service Planning (PSP) buckets. In addition to the hardware PSP buckets, you must also obtain the software PSP buckets. Use the Fix Categories that are specified in the associated FIXCAT HOLDDATA to identify PTFs required for the z13 server, PTFs needed to exploit z13 capabilities, and PTFs recommended to fix known problems. Specifically, fixes in the following categories:

- For the z13:
 - IBM.Device.Server.z13-2964.RequiredService
 - IBM.Device.Server.z13-2964.Exploitation
 - IBM.Device.Server.z13-2964.RecommendedService

- | • For the z13s:
 - | – IBM.Device.Server.z13S-2965.RequiredService
 - | – IBM.Device.Server.z13S-2965.Exploitation
 - | – IBM.Device.Server.z13S-2965.RecommendedService

Fixes required for several zEnterprise functions (such as Parallel Sysplex InfiniBand Coupling Links, Server Time Protocol (STP), the Unified Resource Manager, High Performance FICON (zHPF), and zEnterprise Data Compression (zEDC) are not listed in the hardware PSP bucket, but can be found by using the following Fix Categories:

- For the z13:
 - IBM.Device.Server.z13-2964.ParallelSysplexInfiniBandCoupling
 - IBM.Device.Server.z13-2964.ServerTimeProtocol
 - IBM.Device.Server.z13-2964.UnifiedResourceManager
 - IBM.Device.Server.z13-2964.zHighPerformanceFICON
 - IBM.Function.zEDC
- | • For the z13s:
 - | – IBM.Device.Server.z13S-2965.ParallelSysplexInfiniBandCoupling
 - | – IBM.Device.Server.z13S-2965.ServerTimeProtocol
 - | – IBM.Device.Server.z13S-2965.UnifiedResourceManager
 - | – IBM.Device.Server.z13S-2965.zHighPerformanceFICON
 - | – IBM.Function.zEDC

Note that because the PTFs associated with these Fix Categories are not specific to a z13 server, you should consider specifying a generic wildcard for the server to ensure that you have all the appropriate service installed. For example:

- IBM.Device.Server.*.ParallelSysplexInfiniBandCoupling
- IBM.Device.Server.*.ServerTimeProtocol
- IBM.Device.Server.*.UnifiedResourceManager
- IBM.Device.Server.*.zHighPerformanceFICON

Similarly, fixes needed for zBX or to support the IBM DB2 Analytics Accelerator (IDAA) are not listed in the hardware PSP bucket, but can be found by using the following Fix Categories:

- IBM.Device.Server.zBX-2458
- IBM.DB2.AnalyticsAccelerator.*

If you are upgrading from a server generation prior to the zEC12 or zBC12 servers (such as a z196, z114, z10 EC, z10 BC, z9 EC, or z9 BC), you must install all the maintenance and perform required migration actions for the servers that you are skipping. To read about z196, z114, zEC12, and zBC12 server migration actions, see “Migrate to an IBM zEnterprise z196 or z114 server” on page 72 and “Migrate to an IBM zEnterprise EC12 or IBM zEnterprise BC12 server” on page 60.

If you are exploiting z13 capabilities by installing a web deliverable, you must install the PTFs listed in the software PSP buckets for each of the web deliverables that you are installing. See the Program Directory associated with the web deliverable to identify the required software PSP buckets.

The REPORT MISSINGFIX command checks your GLOBAL zone for FIXCAT HOLDDATA matching the FIXCAT values specified on the command. The command then compares the APARs identified in that FIXCAT HOLDDATA with the PTFs installed in the specified zones, and produces a report to identify any APARs not resolved. In other words, it reports which PTFs (fixes) are missing for the specified fix categories. Furthermore, the command produces a customized job used to obtain any PTFs not already RECEIVED via the RECEIVE ORDER command, and install any missing service via the APPLY CHECK command.

Note the FIXCAT operand on the REPORT MISSINGFIX command can list multiple fix categories, as well as using the same wildcarding techniques described in this topic for the SOURCEID operand. Because both of these techniques are simple and integrated into basic SMP/E commands, use them periodically to ensure the latest PTFs specified in the hardware and software PSP buckets are installed (since PSP buckets can be updated daily). SMP/E also provides an Explorer function which helps in identifying new fix categories which may be of interest. See the IBM fix category Values and

General migration actions: Hardware

Descriptions page for a description of all the fix categories: <http://www.ibm.com/systems/z/os/zos/features/smpe/fix-category.html>. For complete information about the REPORT MISSINGFIX command, see *SMP/E for z/OS Commands*.

7. **Run the CFSIZER tool.** If you are moving your coupling facilities and the coupling facility structures will be on higher CFCC levels than they were previously, run the Coupling Facility Structure Sizer (CFSIZER) tool to find out if you have to increase coupling facility structure sizes. Prepare to make the necessary changes to the CFCC level as indicated by the tool.

You can download the CFSIZER tool at Coupling Facility sizer (www.ibm.com/systems/support/z/cfsizer). Also see “Update your CFRM policy with coupling facility structure size changes” on page 89.

Note: After you make a coupling facility available on the new hardware, you can run the Sizer utility, an authorized z/OS program, to evaluate structure size changes. The Sizer utility is distinct from CFSizer, and should be run after the new hardware (CFLEVEL) is installed, but before any CF LPAR on the new hardware is populated with structures. You can download the Sizer utility at <http://www.ibm.com/systems/support/z/cfsizer/altsize.html>.

8. **Prepare for the new machine instruction mnemonics.** In support of the z13 server, there are new machine instructions. The new machine instructions (mnemonics) may collide with (be identical to) the names of Assembler macro instructions you use. In the event of such collisions, the Assembler’s default opcode table (UNI) will treat specification of these names as instructions when the z13 required service is installed, probably causing Assembler error messages and possibly causing generation of incorrect object code. If you write programs in Assembler Language, compare the names of Assembler macro instructions used to the new machine instructions (documented in the latest *z/Architecture Principles of Operation*, SA22-7832) to identify any such conflicts or collisions that would occur. Identical names will cause Assembler errors or the generation of incorrect object code when you assemble your programs. For a tool to help in identifying mnemonic conflicts, see *Techdoc PRS5289* at the IBM Techdocs website.

If a conflict is identified, take one of these actions:

- Change the name of your macro instruction.
- Specify PARM='...OPTABLE(YOP)...' (or some other earlier opcode table).
- Specify a separate ASMAOPT file containing assembler options such as in the previous method (this method requires no changes to source code or JCL).
- Add as the first statement of your source program: *PROCESS OPTABLE(YOP) (or some other earlier opcode table).
- Specify the PROFILE option either in JCL or the ASMAOPT file, and the specified or default member of the SYSLIB data set is copied into the front of the source program.
- If you must use both a new instruction and a macro with the same name in an assembly you can use a coding technique that permits both use of a new instruction and a macro with the same name in an assembly such as HLASM mnemonic tags (:MAC :ASM).

9. **Decide on the steps to take for your migration to a z13 server.** Besides the steps listed here, see the following topic for guidance “Migration and exploitation considerations for z13 and z13s server functions.”

Migration and exploitation considerations for z13 and z13s server functions

The following z13 and z13sTM functions have considerations when you are planning for migration and exploitation. For PTF information, see the Notes[®] for Table 29 on page 44.

1. **Large Systems Performance Reference (LSPR) method.** LSPR is designed to provide comprehensive z/Architecture[®] processor capacity ratios for different configurations of central processors (CPs) across a wide variety of system control programs and workload environments.
2. **Simultaneous multithreading (SMT).** Incremental throughput is achieved partly because the new processor chip offers intelligently implemented 2-way simultaneous multithreading. Simultaneous multithreading allows two active instruction streams per core, each dynamically sharing the core's

execution resources. SMT is available on the z13 for workloads that are running on the Integrated Facility for Linux (IFL) and the IBM z Integrated Information Processor (zIIP).

3. **CFCC Level 20 and CFCC Level 21 support.** CFCC Levels 20 and 21 support the Coupling Facility use of Large Memory to improve availability for larger CF cache structures and data sharing performance with larger DB2 Group Buffer Pools. This support removes inhibitors to using large CF cache structures, enabling use of Large Memory to appropriately scale to larger DB2 Local Buffer Pools and Group Buffer Pools in data sharing environments.
4. **Coupling links.** IBM z13 introduced new PCIe (Integrated Coupling Adapter – ICA SR) based Short Reach coupling links using a new CHPID type, CS5. ICA-SR links can only connect z13 and z13s CPCs to other z13 and z13s CPCs.

IBM z13 and z13s CPC now support up to 256 links. A single z/OS or a CF Image supports a maximum of 128 links. When displaying STP (DISPLAY ETR) from a z/OS image, information is provided for the entire CPC. If more than 128 links are defined, the z/OS support must be installed on all z/OS releases running on that CPC, so that information about more than 128 links, including STP timing information, can be displayed.
5. **SIMD.** z/OS V2R1 (and later) is designed to support the new vector extension facility (Single Instruction Multiple Data, SIMD) instructions available on IBM z13 servers. SIMD provides a powerful framework for development of new Business Analytics workloads, porting math-intensive workloads from other platforms, and accelerating Business Analytics workloads on IBM z13 and z13s servers. High Data Intensity, High Computational Intensity, Predictive IT Analytics, Advanced Security/Crypto, BI Reporting, Perspective Analytics, and Next-Generation Data Warehousing are some of the workloads that may benefit from Data Parallelism (SIMD). z/OS support includes enablement of Vector Registers (VR) on IBM z13 and z13s servers, Mathematical Acceleration Subsystem (MASS), and Automatically Tuned Linear Algebra Software (ATLAS) support, as well as Language Environment enablement for C runtime functions.
6. **Cryptographic Enhancements.** Cryptographic enhancements for z/OS V2R1 (and later) on z13 servers include:
 - VISA Format Preserving Encryption (VFPE). Support for VFPE algorithms in CCA-based callable services helps legacy databases to contain encrypted data of sensitive fields without having to restructure the database or applications. This support relies on the Crypto Express5S coprocessor.
 - Greater than 16 Domain support. This support allows a cryptographic coprocessor to be shared across more than 16 domains, up to the maximum number of LPARs on the system. This support relies on enhanced firmware available with a minimum microcode level for the Crypto Express5S coprocessor.
 - Trusted Key Entry (TKE) 8.0 Licensed Internal Code (LIC). This support includes Crypto Express5S Coprocessor support, FIPS Certified Smart Card, Crypto Coprocessors with more than 16 domains, a full-function migration wizard for EP11 coprocessors, new master key management functions, a Smart Card Readers Available indicator, a Configure Displayed Hash Size utility, ECC Authority Signature Keys, print capability, new features in the Crypto Node Management (CNM) utility, ENC-Zero verification pattern for 24-byte DES operational keys, and usability enhancements.

See **Decide on the steps you will take for your migration to a z13 server** in “Actions you can take before you order a z13 or z13s server” on page 52

7. **IBM zAware system.** The IBM zAware feature is designed to offer a near real-time, continuous learning, and diagnostics capability intended to help you pinpoint and resolve potential problems quickly enough to minimize impacts to your business. The new version of IBM zAware introduces a new generation of technology with improved analytics to provide better results. After you order a z13 or z13s server, you can prepare to set up an IBM zAware environment by defining the IBM zAware logical partition, defining and using OPERLOG log streams, and network definitions to connect the z/OS LPAR to the zAware LPAR. For more information, see *IBM System z Advanced Workload Analysis Reporter (IBM zAware) Guide*, (SC27-2623), and *z/OS MVS Setting Up a Sysplex*.
8. **Java exploitation.** This support is added by:
 - IBM 31-bit SDK for z/OS, Java Technology Edition, Version 8 (5655-DGG)

General migration actions: Hardware

- IBM 64-bit SDK for z/OS, Java Technology Edition, Version 8 (5655-DGH)
9. **Flash Express.** With this support, z/OS is designed to help improve system availability and responsiveness by using Flash Express across transitional workload events such as market openings, and diagnostic data collection. z/OS is also designed to help improve processor performance by supporting middleware exploitation of pageable large (1 MB) pages. This support requires the Flash Express hardware feature.
 10. **2GB Large Page support.** This support includes support for 2 GB large fixed pages.
 11. **New z/Architecture instructions: XL C/C++ ARCH(11) and TUNE(11) parameters.** This function provides new hardware instruction support, including support for the vector facility, the decimal floating point packed conversion facility, and numerous performance improvements (machine model scheduling and code generation updates). Single Instruction Multiple Data (SIMD) instruction set and execution support is provided through the new vector support in the compiler, including Business Analytics vector processing through the MASS and ATLAS libraries. Unlike prior generations of servers, to use any of these functions on z/OS V2R1, you must download and install the XL C/C++ V2R1M1 web deliverable with z13 support for z/OS 2.1.
 12. **FICON Express16S.** FICON Express16S supports a link data rate of 16 gigabits per second (GBPS) and auto-negotiation to 4 or 8 GBPS for synergy with existing switches, directors, and storage devices. With support for native FICON, High Performance FICON for System z (zHPF), and Fibre Channel Protocol (FCP), the new FICON Express16S channel is designed to work with your existing fiber optic cabling environment. The FICON Express16S feature running at end-to-end 16 GBPS link speeds provides reduced latency for large read/write operations, and increased bandwidth compared to the FICON Express8S feature.
 13. **FICON Dynamic Routing.** With z13, FICON channels are no longer restricted to the use of static Storage Area Network (SAN) routing policies for Inter-Switch Links (ISLs) for cascaded FICON directors. You need to ensure that all devices in your FICON SAN support FICON Dynamic Routing before implementing this feature.
 14. **Improved High Performance FICON for System z (zHPF) I/O Execution at Distance.** High Performance FICON for System z (zHPF) has been enhanced to allow all large write operations (> 64 KB) at distances up to 100 km to be executed in a single return trip to the control unit, thereby not elongating the I/O service time for these write operations at extended distances.
 15. **Improved Channel Subsystem (CSS) Scalability.** The IBM z Systems servers have improved the channel subsystem (CSS) scalability, as follows:
 - The z13 server improves CSS scalability with support for six logical channel subsystems (LCSSs), which are required to support the 85 LPARs for z13, four subchannel sets (to support more devices per logical channel subsystem), and 32K devices per FICON channel, up from 24K channels in the previous generation. Additionally, a fourth subchannel set for each LCSS is provided to facilitate elimination of single points of failure for storage after a disk failure.
 - The z13s server improves CSS scalability with support for three logical channel subsystems (LCSSs) which are required to support the 40 LPARs for IBM z13s, three subchannel sets (to support more devices per logical channel subsystem), and 32K devices per FICON channel up from 24K channels in the previous generation. Additionally, a third subchannel set for each logical channel subsystem (LCSS) is provided to facilitate elimination of single points of failure for disk storage devices.
 16. **PCIe and HCD Definitions.** z/OS V2R1, and z/OS V2R1 HCD (FMID HCS7790) support full exploitation for z13 and z13s processors (types 2964 and 2965) with support for up to 6 channel subsystems and 4 subchannel sets. To support PCIe functions for systems that are running on zEC12, zBC12, z13, or z13s servers, HCD introduced a new dialog for defining PCIe functions and assigning the functions to LPARs.

z/OS V1R13 HCD (HCS7780) supports limited exploitation for z13 and z13s servers (types 2964 and 2965). For PCIE functions, it is possible to define complete types 2964 and 2965 servers, including PCIe functions and the new channel types and capabilities. However, a processor configuration can

be dynamically changed or activated only if it contains neither PCIe function nor a PNETID attribute. For a software activation with hardware validation, PCIe functions and the PNETID attribute are ignored.

IBM recommends that you define and activate all the new hardware definitions on a z/OS V2R2 system, or on a V2R1 system with the appropriate HCD PTF (APAR OA44294) installed and perform software activations (with hardware validation) only on lower-level systems.

17. **Consider the changes in the CPU Measurement Facility counters.** The number of CPU measurement facility counters for z13 and z13s servers remains at 128. Though the structure of the SMF 113 record does not change, the values, interpretations, and frequency of certain sections do change; therefore, current tools that use the data must be updated for the z13 and z13s servers.

For example, consider the following SMF record field:

- SMF113_2_CtrVN2 identifies how to interpret the MT-Diagnostic, Crypto, and Extended Counter Sets. As described in *The IBM CPU Measurement Facility Extended Counters Definition for z10 and z196*, SA23-2260, this field is set to 1 (for z10), 2 (for z196 or z114), 3 (for zEC12 and zBC12), or 4 (for z13 and z13s).

Note: As of z/OS V2R1, if you use the CPU Measurement Facility, IBM recommends that your installation collect SMF 113 subtype 1 and 2 records. IBM also recommends that products process SMF 113 subtype 1 records when available because that is where future enhancements will be made. If subtype 1 records are not available, products can process subtype 2 records.

Accommodate functions for the z13 server or z13s to be discontinued on future servers

Note: IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Description

The following changes in hardware support could affect your environment. Make the appropriate changes, as needed.

- **Removal of support for running an operating system in ESA/390 architecture mode.** The z13 and z13sTM are the last z Systems servers to support running in ESA/390 mode. All future systems will only support operating systems running in z/Architecture mode. However, all 24-bit and 31-bit problem-state application programs originally written to run on the ESA/390 architecture will be unaffected by this change.
- **Removal of support for Classic Style User Interface on the Hardware Management Console and Support Element.** The z13 and z13s are the last z Systems servers to support Classic Style User Interface. In the future, user interface enhancements will be focused on the Tree Style User Interface.
- **Removal of support for the Hardware Management Console Common Infrastructure Model (CIM) Management Interface.** The z13 and z13s are the last z Systems servers to support the Hardware Management Console Common Infrastructure module (CIM) Management Interface. The Hardware Management Console Simple Network Management Protocol (SNMP), and Web Services Application Programming Interfaces (APIs) will continue to be supported.
- **Removal of FICON Express8 support.** The z13 and z13s are the last z Systems servers to support FICON Express8. You should begin migrating from FICON Express8 channel features (#3325, #3326) to FICON Express16S channel features (#0418, #0419). FICON Express8 will not be supported on future high-end z Systems servers as carry forward on an upgrade.

General migration actions: Hardware

- **Removal of support for ordering FICON Express8S channel features.** Enterprises that have 2GB device connectivity requirements must carry forward these channels.
- **Removal of an option for the way shared logical processors are managed under PR/SM™ LPAR.** The z13 and z13s are the last z Systems servers to support selection of the option “Do not end the timeslice if a partition enters a wait state” when the option to set a processor run-time value has been previously selected in the CPC RESET profile. The CPC RESET profile applies to all shared logical partitions on the machine, and is not selectable by logical partition.
- **Removal of support for configuring OSN CHPID types.** OSN CHPIDs are used to communicate between an operating system instance running in one logical partition and the Communications Controller for Linux (CCL) product in another logical partition on the same CPC. See announcement letter #914-227 dated 12/02/2014 for details regarding withdrawal from marketing for the CCL product.

Migrate to an IBM zEnterprise EC12 or IBM zEnterprise BC12 server

Description

An IBM zEnterprise EC12 (zEC12) and IBM zEnterprise BC12 (zBC12) server can include the following in a zEnterprise environment:

- IBM zEnterprise EC12 server Central Processing Complex (CPC) or IBM zEnterprise BC12 server CPC
- zEnterprise BladeCenter Extension (zBX) Model 003 with its integrated optimizers or select IBM blades
- zEnterprise Unified Resource Manager (Unified Resource Manager)

The zEC12 and zBC12 are distinct from the earlier zEnterprise and other servers. In this publication, the IBM zEnterprise EC12 server is referred to as the model zEC12 server and the IBM zEnterprise BC12 server is referred to as the model zBC12 server.

In a Parallel Sysplex you can include the following servers:

- zEC12 and zBC12 servers
- zEnterprise servers (z196 or z114)
- z10 EC and z10 BC servers.

The specific zEC12 and zBC12 functions including base support that are used by z/OS depend on the z/OS release. Availability and other restrictions are noted in the “Notes” column. PTFs might be required for many of these functions. See “Actions you can take before you order a zEC12 or zBC12 server” on page 66 for information about finding the appropriate PTFs.

Table 32. zEC12 and zBC12 server functions included in the base support for z/OS V2R1 and z/OS V2R2

zEC12 and zBC12 function included in base z/OS support (Y/N)	V2R1 ¹	V2R2 ¹
Base support	Y	Y
OSA-Express4S (GbE LX and SX, 1000BASE-T, 10 GbE LR and SR)	Y	Y
OSA-Express5S (GbE LX and SX, 1000BASE-T, 10 GbE LR and SR)	Y	Y
FICON Express 8S (CHPID FC)	Y	Y
High Performance FICON (zHPF)	Y	Y
Parallel Sysplex InfiniBand (PSIFB) Coupling Link	Y	Y
CPU measurement facility	Y	Y
New z/Architecture instructions: XL C/C++ ARCH(10) and TUNE(10) parameters	Y	Y
Crypto Express3 Toleration (if carried forward)	Y	Y

Table 32. zEC12 and zBC12 server functions included in the base support for z/OS V2R1 and z/OS V2R2 (continued)

zEC12 and zBC12 function included in base z/OS support (Y/N)	V2R1 ¹	V2R2 ¹
IBM zEnterprise Unified Resource Manager	Y	Y
IBM zEnterprise BladeCenter Extension (zBX) Model 3	Y	Y
GRS FICON CTC toleration	Y (requires additional PTFs for exploitation) ²	Y

Notes:

- PTFs for base support have a fix category of either:
 - For zEC12: IBM.Device.Server.zEC12-2827
 - For zBC12: IBM.Device.Server.zBC12-2828
- PTFs for exploitation have a fix category of either:
 - For zEC12: IBM.Device.Server.zEC12-2827.Exploitation
 - For zBC12: IBM.Device.Server.zEC12-2828.Exploitation
- PTFs for zEDC exploitation or software decompression have a fix category (for both zEC12 and zBC12) of IBM.Function.zEDC.

Table 33. Exploitation of zEC12 and zBC12 server functions supported by z/OS V2R1 and z/OS V2R2

zBC12 functional exploitation of z/OS support (Y/N)	V2R1 ²	V2R2 ²
Coupling Facility Control Code (CFCC) Level 18	Y	Y
Coupling Facility Control Code (CFCC) Level 19	Y	Y
Coupling Facility Control Code (CFCC) Level 19 Coupling thin interrupt support	Y	Y
Crypto Express4S (#0865) exploitation, including Enterprise Security PKCS #11-Hardware Security Module (HSM), DUKPT for MAC and Data Encryption, Cipher Text Translate CCA Verb, PKDS/TKDS Constraint Relief, Random Number Cache, FIPS on Demand, and Wrapping Keys with Strong Keys	Y	Y
Crypto Express4S CCA enhancements, including: Export TDES key under AES transport key, Diversified Key Generation CBC, IPEK, RKX key wrapping method, and Integration of UDX into CCA	Y (requires the Cryptographic Support for z/OS V1R13-z/OS V2R1 web deliverable (FMID HCR77A1) .	Y
Crypto Express4S: EP11 enhancements when the Crypto Express4S PCIe adapter is configured as an EP11 coprocessor, including: (PKCS #11 v2.1 PSS, EP11 Key agreement algorithms, and Offload Generation of Domain Parameters)	Y (requires the Cryptographic Support for z/OS V1R13-z/OS V2R1 web deliverable (FMID HCR77A1)	Y
Crypto Express4S support of greater than 16 Domains	Y	Y
Flash Express (Storage Class Memory or SCM)	Y	Y
Pageable 1 MB Large Page Support.	Y	Y
Dynamic reconfiguration support for Flash Express.	Y	Y
2 GB Large Page support.	Y	Y
Optional PLPA/common page data set support.	Y	Y
10GbE RoCE Express	Y	Y

General migration actions: Hardware

Table 33. Exploitation of zEC12 and zBC12 server functions supported by z/OS V2R1 and z/OS V2R2 (continued)

zBC12 functional exploitation of z/OS support (Y/N)	V2R1 ²	V2R2 ²
Java Exploitation of Transactional Execution (requires Java7 SR3)	Y	Y
IBM System Advanced Workload Analysis Reporter (IBM zAware)	Y	Y
New z/Architecture instructions: XL C/C++ ARCH(10) and TUNE(10) parameters	Y	Y
New z/Architecture Assembler Language instruction mnemonic	Y	Y
zEDC capability using zEDC Express	Y ³ (requires the z/OS zEDC software feature to be enabled)	Y ³ (requires the z/OS zEDC software feature to be enabled)

Notes:

- PTFs for base support have a fix category of either:
 - For zEC12: IBM.Device.Server.zEC12-2827
 - For zBC12: IBM.Device.Server.zBC12-2828
- PTFs for exploitation have a fix category of either:
 - For zEC12: IBM.Device.Server.zEC12-2827.Exploitation
 - For zBC12: IBM.Device.Server.zEC12-2828.Exploitation
- PTFs for zEDC exploitation or software decompression have a fix category (for both zEC12 and zBC12) of IBM.Function.zEDC.

Table 34 provides more details about this migration action. Use this information to plan your changes to the system.

Table 34. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	<ul style="list-style-type: none"> IBM zEnterprise EC12, which first shipped September 2012. IBM zEnterprise BC12 (zBC12), which first shipped September 2013.
Applies to migration from:	z/OS V2R2, z/OS V2R1, and z/OS V1R13.
Timing:	Anytime before you introduce a zEC12 or zBC12 server into your environment.
Is the migration action required?	Yes, if you want to run z/OS V2R2, z/OS V2R1 and z/OS V1R13 on a zEC12 or zBC12 server, or if you want to run a Coupling Facility on a zEC12 or zBC12 server. If you will run only a Coupling Facility on a zEC12 or zBC12 system, only the sysplex-related actions are relevant.

Table 34. Information about this migration action (continued)

Target system hardware requirements:	<ul style="list-style-type: none"> • A zEC12 or zBC12 • Additional hardware required for specific functions. <ul style="list-style-type: none"> – IBM devices previously attached to IBM System z10, z196 and zSeries servers are supported for attachment to zEC12 channels, unless otherwise noted. The subject I/O devices must meet FICON architecture requirements – IBM zAware requires the IBM zAware server firmware (FC #0011, #0101, and #0102) – Flash Express requires FC #0402 – zEDC Express requires FC #0420 – 10 GbE RoCE Express FC #0411 – Use of IBMWebSphere DataPower Integration Appliance XI50 for zEnterprise (DataPower XI50z) or select IBM BladeCenter PS701 Express blades or IBM BladeCenter HX5 blades requires a zEnterprise BladeCenter Extension (zBX) Model 003
Target system software requirements:	<ol style="list-style-type: none"> 1. See the list of PTFs in the Software Service Level section of the PSP buckets and use the SMP/E Fix Categories: <ul style="list-style-type: none"> • For zEC12 base support: IBM.Device.Server.zEC12-2827 • For zBC12 base support: IBM.Device.Server.zBC12-2828 • For zEC12 exploitation: IBM.Device.Server.zEC12-2827.Exploitation • For zBC12 exploitation: IBM.Device.Server.zBC12-2828.Exploitation • For zEC12 and zBC12 zEDC exploitation or toleration: IBM.Function.zEDC 2. See “Support is delivered by service, z/OS features, and web deliverables” described in “General recommendations and considerations for a zEC12 or zBC12 server” on page 64 and “Install the necessary z/OS service”, as indicated in PSP buckets described in “Actions you can take before you order a zEC12 or zBC12 server” on page 66.
Other system (coexistence or fallback) requirements:	<ul style="list-style-type: none"> • It is recommended that you install and run the zEnterprise required service on your existing server. This will enable you to fall back from a hardware perspective, yet maintain your software level. • If you have not installed the preconditioning and exploitation PTFs for CFCC Level 17, note that these PTFs are required to be installed throughout your sysplex before implementing CFCC Level 18 or 19. • If you plan to implement zEDC, you should install the z/OS toleration PTFs on systems that access data that is compressed using zEDC Express on a zEC12 or zBC12 server.
Restrictions:	See “Restrictions for a zEC12 or zBC12 server” on page 65.
System impacts:	None.

General migration actions: Hardware

Table 34. Information about this migration action (continued)

Related IBM Health Checker for z/OS check:	IBM Health Checker for z/OS check, SUP_HiperDispatchCPUConfig, was added to z/OS V1R12 with APAR OA30476. This check verifies that HiperDispatch is enabled on a z196 or later system.
--	--

Steps to take

Follow the “General recommendations and considerations for a zEC12 or zBC12 server,” adhere to the “Restrictions for a zEC12 or zBC12 server” on page 65, and perform the tasks that are described in the following topics.

Reference information

None.

General recommendations and considerations for a zEC12 or zBC12 server

As you plan your migration to a zEnterprise server, consider the following:

1. **Relatively few migration actions are new when coming from a z196 or z114 server.** Migration to an IBM zEnterprise EC12 or zEnterprise BC12 server has, as its base, a migration to the z196 or z114 servers. This means that if you are migrating to a zEnterprise server from a z196 or z114 server, and have performed the migration actions associated with the z196 or z114, you have fewer migration actions than if you were migrating from an earlier generation server and have not yet performed the migration actions associated with these servers. It is important to note that you can migrate directly to a zEC12 or zBC12 server without installing the intermediate servers, but you still need to ensure that any migration considerations are satisfied for the servers that you “skipped.” To read about z196 and z114 server migration actions, see “Migrate to an IBM zEnterprise z196 or z114 server” on page 72.
2. **Support is delivered by service, z/OS features, and web deliverables.** The base support for an zEC12 or zBC12 server is delivered by service (PTFs).
 - The PSP bucket that contains the required list of PTFs for zBC12 is: Upgrade 2828DEVICE, Subset 2828/ZOS and is identified by the following SMP/E Fix Category IBM.Device.Server.zBC12-2828.
 - The PSP bucket that contains the required list of PTFs for zEC12 is: Upgrade 2827DEVICE, Subset 2827/ZOS

and is identified by the following SMP/E Fix Category IBM.Device.Server.zEC12-2827.

For Flash Express support (including dynamic reconfiguration support and optional PLPA/Common page data set support), pageable 1 MB Large Page support, and 2 GB Large Page Support, a separate web deliverable for z/OS V1R13 (the z/OS V1R13 RSM Enablement Offering web deliverable) is required. (See “Decide on the steps you will take for your migration to a zEC12 or zBC12 server” in “Actions you can take before you order a zEC12 or zBC12 server” on page 66 for further information.)

3. **Larger coupling facility structure sizes might be necessary.** When you change coupling facility control code (CFCC) levels, your coupling facility structure sizes might change. zEC12 servers that are ordered before September 2013 initially ship with CFCC level 18, zEC12 or zBC12 models ordered after September 2013 initially ship with CFCC level 19. If, as part of your migration to a zEC12 or zBC12 server, you change CFCC levels, you might have larger structure sizes than you did previously. If your CFCC levels are identical, structure sizes are not expected to change when you migrate from a previous server to a newer generation server. In addition, similar to CF Level 17 and later, ensure that the CF LPAR has at least 512MB of storage. CFLEVEL 19 introduces support for storage-class (flash) memory in the CF and Coupling thin interrupt support. CF structures that exploit SCM may require significantly more CF real storage than they did before storage class memory exploitation.
4. **Use the same software level throughout a sysplex.** Having members of a sysplex at the same software level (other than during brief migration periods) is good software management policy.

5. **Migrate hardware and software at different times.** To minimize the amount of change (and therefore risk) that you experience at one time, do not migrate your software release level at the same time that you migrate your hardware.
6. **Update SCRT to latest version.** If you use SCRT, make sure it is at the latest level. This is a requirement for sub-capacity pricing, as well as when you upgrade servers. The latest level of SCRT can be downloaded from the SCRT web site at <http://www.ibm.com/eserver/zseries/swprice/scrt/>.

Restrictions for a zEC12 or zBC12 server

Restrictions associated with zEnterprise servers are:

1. **Functional limitations.** Not all zEC12 or zBC12 functions are available in every z/OS release. See the following for a list of the zEC12 and zBC12 functions available in each z/OS release:

- Table 32 on page 60
- Table 33 on page 61

Some functions have migration or exploitation considerations (see “Actions you can take before you order a zEC12 or zBC12 server” on page 66 and “Migration and exploitation considerations for zEC12 and zBC12 server functions” on page 69.) Many functions are enabled or disabled, based on the presence or absence of the required hardware and software. If you wish to position yourself to exploit any new zEC12 or zBC12 functions, you can install the software and hardware in either order; that is, there is no requirement to install either software or hardware first to exploit a specific function. However, because of outage windows and testing considerations, you might want to consider installing all the required software first, then upgrading the hardware and, finally, updating your customization to exploit the new functions.

2. **zEC12 and zBC12 servers in a sysplex.**

- A Parallel Sysplex that contains an zEC12 or zBC12 server either for a z/OS image or a CF image can only contain other zEC12 or zBC12 servers or zEnterprise z196, z114, z10 EC, or z10 BC servers. If you are running z/OS on any servers earlier than a z10 EC or z10 BC server, you cannot add a zEC12 or zBC12 server to that sysplex; that is, you will not be able to perform rolling IPLs to introduce a zEC12 or zBC12 server if you have any of the earlier servers either as z/OS images or coupling facility images in the sysplex.

The earlier servers in the sysplex must be upgraded to System z10 or later to have zEC12 or zBC12 servers supported in the sysplex. If you have any z/OS images or coupling facility images on an earlier server, and you intend to introduce a zEC12 or zBC12 server into that sysplex, you must migrate those images to a System z10 (or later) server before introducing the zEC12 or zBC12 server.

If you are currently using ESCON CTCs for GRS ring configurations within a sysplex, consider using XCF signalling in a GRS ring configuration. XCF sysplex signalling is preferred instead of GRS CTC connections.

- The Integrated Cluster Bus 4 (ICB-4) Coupling Links are not supported on a zEC12 or zBC12 CPC. Use 12x InfiniBand coupling links, which are designed to replace Integrated Cluster Bus 4 (ICB-4), and to complement 1x InfiniBand and ISC-3 on a zEC12 or zBC12 server. InfiniBand coupling can provide significantly improved service times compared to ISC-3s for distances up to 150 meters. You can read about InfiniBand coupling links in *IBM System z Connectivity Handbook (SG24-5444)*.
- The zEC12 or zBC12 server cannot be connected to a Sysplex Timer (9037-002). The Server Time Protocol (STP) feature is the follow-on to the Sysplex Timer. STP is designed to allow multiple servers and coupling facilities to maintain time synchronization with each other without requiring a Sysplex Timer. STP is a hardware feature of the zEC12, zBC12, z196, z114, z10 EC, and z10 BC. To implement STP, see the STP web site and the publications and other resources listed there. The STP web site is at <http://www.ibm.com/systems/z/advantages/pso/stp.html>.

The STP design introduced a concept called Coordinated Timing Network (CTN). A CTN is a collection of servers and coupling facilities that are time-synchronized to a time value called Coordinated Server Time. A CTN can be configured in two ways:

- STP-only CTN, which does not require a Sysplex Timer.

General migration actions: Hardware

- Mixed-CTN (External Time Reference and STP), which does require a Sysplex Timer.
The Sysplex Timer provides the timekeeping information in a Mixed-CTN. Even though the zEC12 or zBC12 servers do not support attachment to a Sysplex Timer, they can participate in a Mixed-CTN that has a z10 server synchronized to the Sysplex Timer. This maintains the capability for enterprises to concurrently migrate from an existing External Time Reference (ETR) to a Mixed-CTN and from a Mixed-CTN to an STP-only CTN.

Note: The zEC12 and zBC12 will be the last high-end servers to support connections to an STP Mixed-CTN. All servers in the network must be configured in STP-only mode. Consider migrating servers that require time synchronization, such as to support a base or Parallel Sysplex, to the Server Time Protocol (STP).

3. For a list of functions on the zEC12 or zBC12 server that are planned to be discontinued on future servers, see “Accommodate functions for the zEC12 and zBC12 servers to be discontinued on future servers” on page 71
4. **Unsupported hardware features.** The following hardware features cannot be ordered and cannot be carried forward from an upgrade on an earlier server to the zEC12 or zBC12 server.
 - Power[®] Sequence Controller (PSC).
 - FICON Express. You should begin migrating to FICON Express8S channels.
 - FICON Express2. You should begin migrating to FICON Express8S channels.
 - FICON Express4 4KM LX. You should begin migrating to FICON Express8S channels.
 - OSA Express2. You should begin migrating to OSA-Express4S (GbE LX and SX, 1000BASE-T, 10 GbE LR and SR).
 - ESCON. You should begin migrating to FICON Express8S channels.
 - Dial up modems. The currently available Network Time Protocol (NTP) server option for ETS, as well as Internet time services available using broadband connections, can be used to provide the same degree of accuracy as dial-up time services. You should begin migrating from dial-up modems to broadband for RSF connections

Carry forward hardware features. The following hardware features are not orderable on zEC12 or zBC12 servers. If they are installed on your existing server at the time of an upgrade to a zEC12 or zBC12 server, they may be retained or carried forward.

- ISC-3. You should begin migrating from ISC-3 features (#0217, #0218, #0219) to 12x InfiniBand (#0163 - HCA2-O or #0171- HCA3-O fanout) or 1x InfiniBand (#0168 - HCA2-O LR or #0170 - HCA3-O LR fanout) coupling links.
- FICON Express4 10KM LX. You should begin migrating to FICON Express8S channels.
- FICON Express4 SX. You should begin migrating to FICON Express8S channels
- Crypto Express3

Also, see “Ensure that you are running on supported servers and storage controllers” on page 85

Actions you can take before you order a zEC12 or zBC12 server

You can perform the following migration actions before you order or install a zEC12 or zBC12 server:

1. **Review the sysplex configuration in which the zEC12 or zBC12 server will participate.** See “Restrictions for a zEC12 or zBC12 server” on page 65 for the limitations of using zEC12 or zBC12 servers with certain earlier servers in a Parallel Sysplex.
2. **Implement STP (or a Mixed-CTN) timing network.** This action is necessitated because Sysplex Timers (9037-002) are not supported on zEC12 or zBC12 servers.
3. **Migrate from ICB-4 to InfiniBand coupling links.** This action is necessitated because ICB-4 links are not supported on zEC12 or zBC12 servers. If desired, you can take this action after you order a zEC12 or zBC12 server, as you upgrade to the new server.
4. **Migrate from unsupported hardware features to newer technology.** This action is necessitated because FICON Express, FICON Express2, Crypto Express2, and OSA-Express2 10 GbE LR are not

supported on zEnterprise servers. See “Restrictions for a zEC12 or zBC12 server” on page 65, “Replace unsupported devices” on page 87, and “Provide for new device installations” on page 88.

5. Install the necessary z/OS service, as indicated in PSP buckets.

- For an IBM zEnterprise BC12 CPC, PTFs are identified in the in the 2828DEVICE PSP bucket (Subset 2828/ZOS).
- For an IBM zEnterprise EC12 CPC, PTFs are identified in the 2827DEVICE PSP bucket (Subset 2827/ZOS).
- For an IBM zEnterprise BladeCenter Extension (zBX) attached to your zEC12 CPC or zBC12 CPC, the PTFs are identified in the 2458DEVICE PSP bucket (Subset 2458/ZOS).

In each PSP bucket, the content is dependent on the z/OS release you will run on the zEnterprise server. If you reviewed the PSP buckets some time ago, review them again to ensure that any newly identified z/OS service has been installed. To assist you in determining if you have the recommended service (identified in these PSP buckets) installed on your system, you can use the SMP/E REPORT MISSINGFIX command in conjunction with the FIXCAT type of HOLDDATA, as follows:

- a. Acquire and RECEIVE the latest HOLDDATA onto your z/OS system(s). Use your normal service acquisition portals or download the two (2) year HOLDDATA directly from <http://service.software.ibm.com/holddata/390holddata.html>. Ensure you select **Full** from the Download NOW column (last 730 days) to receive the FIXCAT HOLDDATA, as the other files do not contain FIXCAT HOLDDATA.
- b. Run the SMP/E REPORT MISSINGFIX command on your z/OS systems and specify one or more of the following Fix Categories (FIXCAT):
 - IBM.Device.Server.zEC12-2827
 - IBM.Device.Server.zEC12-2827.Exploitation
 - IBM.Device.Server.zEC12-2827.ParallelSysplexInfiniBandCoupling
 - IBM.Device.Server.zEC12-2827.ServerTimeProtocol
 - IBM.Device.Server.zEC12-2827.zHighPerformanceFICON
 - IBM.Device.Server.zEC12-2827.UnifiedResourceManager
 - IBM.Function.zEDC
 - IBM.Device.Server.zBC12-2828
 - IBM.Device.Server.zEC12-2828.Exploitation
 - IBM.Device.Server.zBC12-2828.ParallelSysplexInfiniBandCoupling
 - IBM.Device.Server.zBC12-2828.ServerTimeProtocol
 - IBM.Device.Server.zBC12-2828.zHighPerformanceFICON
 - IBM.Device.Server.zBC12-2828.UnifiedResourceManager

The report will identify any missing coexistence and fallback PTFs for that system. For complete information about the REPORT MISSINGFIX command, see *SMP/E for z/OS Commands*.

- c. Periodically, you might want to acquire the latest HOLDDATA and rerun the REPORT MISSINGFIX command to find out if there are any new PTFs recommended for the zEnterprise servers.

Notes:

- a. You can also use Service Link's PSP Service Extraction tool.
 - b. Because the Enhanced PSP Tool (EPSPT) was removed the end of 2010, you can no longer use that tool to identify missing PSP bucket service. You should use SMP/E's Fix Category support, which is fully integrated into SMP/E procedures and IBM product and service deliverables.
6. **Run the CFSIZER tool.** If you are moving your coupling facilities and the coupling facility structures will be on higher CFCC levels than they were previously, run the Coupling Facility Structure Sizer (CFSIZER) tool to find out if you have to increase coupling facility structure sizes.

General migration actions: Hardware

If ordered before September 2013, zEC12 servers initially ship with CFCC Level 18. For zEC12 and zBC12 servers ordered after September 2013, the servers ship with CFCC Level 19; prepare to make the necessary changes as indicated by the tool.

You can download the CFSIZER tool at Coupling Facility sizer (www.ibm.com/systems/support/z/cfsizer). Also see “Update your CFRM policy with coupling facility structure size changes” on page 89.

Note: After you make a coupling facility available on the new hardware, you can run the Sizer utility, an authorized z/OS program, to evaluate structure size changes. The Sizer utility is distinct from CFSIZER, and should be run after the new hardware (CFLEVEL) is installed, but before any CF LPAR on the new hardware is populated with structures. You can download the Sizer utility at <http://www.ibm.com/systems/support/z/cfsizer/altsize.html>.

7. **Decide on the steps you will take for your migration to a zEC12 or zBC12 server.** In addition to the steps listed here in “Actions you can take before you order a zEC12 or zBC12 server” on page 66, as a guide, also see “Migration and exploitation considerations for zEC12 and zBC12 server functions” on page 69. Also, note the following web deliverables considerations.

The level of function provided for cryptographic support differs by z/OS release and the ICSF web deliverable that is installed. Toleration PTFs are also available for some cryptographic web deliverables:

Consider the following:

- For z/OS V1R13 and z/OS V2R1, if you require the cryptographic enhancements support for CCA (including Export TDES key under AES transport key, Diversified Key Generation CBC, IPEK, RKX key wrapping method, and integration of UDX into CCA), you must install the web deliverable Cryptographic Support for z/OS V1R13-z/OS V2R1 (FMID HCR77A1). You must also perform the required ICSF migration actions.
- **PTFs for coexistence:** Coexistence PTFs must be installed on older levels of ICSF. To assist in identifying the coexistence service, you can use the following Fix Categories:
 - IBM.Coexistence.ICSF.z/OS_V1R11-V1R13-HCR7790
 - IBM.Coexistence.ICSF.z/OS_V1R12-V1R13-HCR77A0
 - IBM.Coexistence.ICSF.z/OS_V1R13-V2R1-HCR77A1

If you plan to use the , then similar to what you might be doing today to enable other z/OS priced features, you must notify IBM that you are starting to use the feature, update the IFAPRDxx PARMLIB member to specify that the z/OS ZEDC software feature is enabled, and follow the z/OS V2R2 documentation to customize the exploiting functions. You should also ensure that all z/OS V1R13 systems that will access zEDC compressed data have the required toleration maintenance installed to enable software decompression.

8. **Review the new mnemonics introduced for the zEC12 or zBC12 server.** The new mnemonics might collide with (be identical to) the names of assembler macro instructions you use or provide. In the event of such collisions, the HLASM’s default opcode table (UNI) will treat specification of these names as instructions when APAR PM49761 and PM86821 are installed. This will probably cause assembler error messages and possibly cause generation of incorrect object code.

If you write programs in Assembler Language, you should compare the list provided in *z/Architecture Principles of Operation*, SA22-7832, to the names of assembler macro instructions you use or provide, to identify any such conflicts or collisions that would occur following installation of HLASM APAR PM49761 and PM86821. If a conflict is identified, take one of the following actions:

- Change the name of your macro instruction.
- Specify PARM=’...OPTABLE(YOP)...’ (or some other earlier opcode table).
- Specify a separate ASMAOPT file containing assembler options, such as in the previous method (this method requires no changes to source code or JCL).
- Add, as the first statement of your source program, *PROCESS OPTABLE(YOP).
- Specify the PROFILE option either in JCL or the ASMAOPT file, and the specified or default member of the SYSLIB data set is copied into the front of the source program.

- If you must use both a new instruction and a macro with the same name in an assembly, you can use the following technique (where XXX is a sample mnemonic):

```
Assume the default OPTABLE(UNI) is in effect
XXX  a,b      new instruction
PUSH  ACONTROL save current optable definition
ACONTROL OPTABLE(YOP) switch optable dynamically
XXX  r,s,t    macro invocation
POP   ACONTROL restore previous definition
XXX  c,d      new instruction
```

For more information about HLASM opcode table, see *HLASM Programmer's Guide*.

9. **Plan for changes to your global resource serialization complex with the zEC12 or zBC12 server.** If you use a global resource serialization ring complex that spans more systems than is part of the sysplex or does not use sysplex signalling for communications within the complex, you need to take migration actions. Instead of using global resource serialization ring, consider using the global resource serialization star configuration in a sysplex. You can take the following actions before you install the zEC12 or zBC12 server:
 - Migrate to a Parallel Sysplex that uses the recommended global resource serialization star complex.
 - Convert to a basic sysplex that uses XCF sysplex signalling with global resource serialization ring instead of GRS-managed channel-to-channel (CTC) communications.

Migration and exploitation considerations for zEC12 and zBC12 server functions

Consider the number of CPU measurement facility counters for zEC12 or zBC12. The number of CPU measurement facility counters for zEC12 and zBC12 is increased to 128. More extended counters means that more internal storage is required. Though the structure of the SMF 113 record does not change, the values, interpretations, and frequency of certain sections do change; therefore, current tools using the data must be updated for the zEC12 or zBC12.

For example, consider the following SMF record field:

- SMF113_2_CtrVN2 identifies how to interpret the Crypto and Extended counter sets. As described in *The IBM CPU Measurement Facility Extended Counters Definition for z10 and z196*, SA23-2260, this field is set to 1 (for z10), 2 (for z196 or z114), or 3 (for zEC12 and zBC12).

Note: As of z/OS V2R1, if you use the CPU Measurement Facility, IBM recommends that your installation collect SMF 113 subtype 1 and 2 records. IBM also recommends that products process SMF 113 subtype 1 records when available, because that is where future enhancements will be made. If subtype 1 records are not available, products can process subtype 2 records.

The following zEC12 and zBC12 functions are available on z/OS V2R1. For PTF information, see the “Notes” for Table 33 on page 61:

1. **CFCC Level 19 Coupling thin interrupt support.** With PTFs CFCC Level 19 provides coupling thin interrupt support that allows a shared logical coupling facility partition to be dispatched by PR/SM if not already dispatched and allows for more timely processing of events to which the CF must respond. It is designed to improve service times for shared engine coupling facilities, and to help improve the response time for asynchronous CF operations. This function requires CFCC Level 19.
2. **Cryptographic Enhancements.** Cryptographic enhancements for z/OS V2R1 on zEC12 and zBC12 server include:
 - Crypto Express4S CCA enhancements when the PCIe adapter is configured as CCA coprocessor including: Export TDES key under AES transport key, Diversified Key Generation CBC, IPEK, RKX key wrapping method, and Integration of UDX into CCA requires z/OS V2R1 with the Cryptographic Support for z/OS V1R13-z/OS V2R1 Web deliverable (FMID HCR77A1) installed.
 - Crypto Express4S EP11 enhancements when the Crypto Express4S PCIe adapter is configured as an EP11 coprocessor including: (PKCS #11 V2R1 PSS, EP11 Key agreement algorithms, and Offload Generation of Domain Parameters) and requires z/OS V2R1 with the Cryptographic Support for z/OS V1R13-z/OS V2R1 Web deliverable (FMID HCR77A1) to be installed.

General migration actions: Hardware

- Crypto Express4S (#0865) exploitation including Enterprise Security PKCS #11-Hardware Security Module (HSM), DUKPT for MAC and Data Encryption, Cipher Text Translate CCA Verb, PKDS/TKDS Constraint Relief, Random Number Cache, FIPS on Demand, and Wrapping Keys with Strong Keys.

See “Decide on the steps to take for your migration to a zEC12 or zBC12 server” in “Actions you can take before you order a zEC12 or zBC12 server” on page 66

3. **zEDC capability using zEDC Express.** zEDC provides IBM zEnterprise data compression/decompression capability. For z/OS V2R2, the zEDC software feature must be enabled with your product enablement policy (IFAPRDxx); then follow the z/OS V2R2 documentation to customize the exploiting functions. See “Verify your IFAPRDxx Product ID is correct for z/OS Version 2” on page 40
4. **IBM zAware system.** IBM zAware is designed to offer a near real-time, continuous learning, and diagnostics capability intended to help you pinpoint and resolve potential problems quickly enough to minimize impacts to your business. After you order a zEC12 or zBC12 you can prepare to set up an IBM zAware environment by defining the IBM zAware logical partition, defining and using OPERLOG log streams, and network definitions to connect the z/OS LPAR to the zAware LPAR. For more information, see *IBM System z Advanced Workload Analysis Reporter (IBM zAware) Guide*, (SC27-2623) and *z/OS MVS Setting Up a Sysplex*.
5. **Java Exploitation of Transactional Execution (requires Java 7 SR3).** This function provides support for Java exploitation of the Transaction Execution Facility on IBM zEnterprise zEC12 or zBC12. Transactional Execution will offer increased scalability and parallelism to drive higher transaction throughput. Java exploitation is planned with
 - IBM 31-bit SDK for z/OS, Java Technology Edition, V7.0.0 (5655-W43)
 - IBM 64-bit SDK for z/OS, Java Technology Edition, V7.0.0 (5655-W44).

Note: Using z/OS V1R13 XL C/C++ compiler and later, specify ARCH(10) to provide the hardware with built-in functions to enable applications to use the Java Transactional Execution Facility.

6. **Flash Express (Storage Class Memory or SCM).** This support includes pageable 1 MB Large Page support, dynamic reconfiguration support of SCM, and optional PLPA/Common page data set usage. This support requires the Flash Express hardware feature.
7. **2GB Large Page support.** This support includes support for 2 GB large fixed pages.
8. **CFCC Level 19 Flash Express.** This exploitation will provide improved resilience for MQ shared queues. The function requires CFCC Level 19 and is planned to be available in a future update.
9. **New z/Architecture instructions: XL C/C++ ARCH(10) and TUNE(10) parameters.** This function provides new zArchitecture instructions.
10. **Shared Memory Communications using RDMA (SMC-R) exploitation.** Shared Memory Communication using RDMA (Remote Direct Memory Access) enables transparent exploitation of RDMA technology for TCP/IP sockets based applications. It requires the 10GbE RoCE Express hardware feature.
11. **24k subchannels per channel (port) for the FICON Express features.** This is planned to help facilitate growth as well as continuing to enable server consolidation. You will be able to define more devices per FICON channel, which includes primary, secondary, and alias devices. This support applies to the FICON Express8S, FICON Express8, and FICON Express4 features when defined as CHPID type FC.
12. **OSA-Express5S.** OSA-Express5S provides a new generation of Ethernet features for use in the PCIe I/O drawer and continues to be supported by the 8 Gbps PCIe Gen2 host bus. This support includes: 1000BASE-T Ethernet for copper environments, in addition to 10 Gigabit Ethernet (10 GbE) and Gigabit Ethernet (GbE) for single-mode and multimode fiber optic environment.

Accommodate functions for the zEC12 and zBC12 servers to be discontinued on future servers

Description

The following changes in hardware support could affect your environment. Make the appropriate changes as needed.

- **Removal of support for connections to an STP Mixed CTN.** The zEC12 and zBC12 are the last System z servers to support connections to an STP Mixed CTN. This also includes the Sysplex Timer (9037). After the zEC12 and the zBC12, servers that require Time synchronization, such as to support a base or Parallel Sysplex, will Require Server Time Protocol (STP) and all servers in that network must be configured in STP-only mode.
- **Removal of support for Ethernet half-duplex operation and 10 Mbps link data rate.** The OSA-Express4S 1000BASE-T Ethernet feature is planned to be the last copper Ethernet feature to support half-duplex operation and a 10 Mbps link data rate. The zEC12 and zBC12 servers are planned to be the last IBM System z servers to support half-duplex operation and a 10 Mbps link data rate for copper Ethernet environments. Any future 1000BASE-T Ethernet feature will support full-duplex operation and auto-negotiation to 100 or 1000 Mbps exclusively. This hardware statement of direction is fulfilled with the delivery of OSA-Express5S.
- **Removal of ISC-3 support on System z.** The zEC12 and zBC12 are planned to be the last System z servers to offer support of the InterSystem Channel-3 (ISC-3) for Parallel Sysplex environments at extended distances. ISC-3 will not be supported on future System z servers as carry forward on an upgrade. Previously, it was announced that the IBM zEnterprise 196 (z196) and IBM zEnterprise 114 (z114) servers were the last to offer ordering of ISC-3. Enterprises should continue migrating from ISC-3 features (#0217, #0218, #0219) to 12x InfiniBand (#0171 - HCA3-O fanout) or 1x InfiniBand (#0170 - HCA3-O LR fanout) coupling links.
- **Removal of OSA-Express3 support on System z.** The zEC12 and zBC12 servers are planned to be the last System z servers to offer support of the Open System Adapter-Express3 (OSA-Express3 #3362, #3363, #3367, #3370, #3371) family of features. OSA-Express3 will not be supported on future System z servers as carry forward on an upgrade. Enterprises should continue migrating from the OSA-Express3 features to the OSA-Express4S (#0404, #0405, #0406, #0407, #0408) and OSA-Express5S features (#0413, #0414, #0415, #0416, #0417).
- **Removal of FICON Express4 support on System z.** The zEC12 and zBC12 servers are planned to be the last System z servers to offer support of the FICON Express4 features (#3321, #3322). FICON Express4 will not be supported on future System z servers as carry forward on an upgrade. Enterprises should continue migrating from the FICON Express4 features to the FICON Express8S features (#0409, #0410).
- **Removal of Crypto Express3 support on System z.** The zEC12 and zBC12 servers are planned to be the last System z servers to offer support of the Crypto Express3 features (#0864 and #0871 - zBC12). Crypto Express3 will not be supported on future System z servers as carry forward on an upgrade. Enterprises should continue migrating from the Crypto Express3 features to the Crypto Express4S feature (#0865).
- **IBM System z Integrated Information Processor (zIIP) and IBM System z Application Assist Processor (zAAP) simplification.** The zEC12 and zBC12 are planned to be the last System z servers to offer support for zAAP specialty engine processors. IBM intends to continue support for running zAAP workloads on zIIP processors (“zAAP on zIIP”). This is intended to help simplify capacity planning and performance management, while still supporting all the currently eligible workloads.
- **Removal of support for the HCA2-O fanouts for 12x IFB and 1x IFB InfiniBand coupling links.** The zEC12 and zBC12 are planned to be the last System z servers to support the following features as carry forward on an upgrade: HCA2-O fanout for 12x IFB coupling links (#0163) and HCA2-O LR fanout for 1x IFB coupling links (#0168). Enterprises should continue migrating to the HCA3-O fanout for 12x IFB (#0171) and the HCA3-O LR fanout for 1x IFB (#0170).
- **Removal of support for IEEE 802.3 Ethernet frame types.** The zEC12 and zBC12 are planned to be the last System z servers to support IEEE 802.3 Ethernet frame types. All OSA-Express features supported on future System z servers are planned to support DIX Version 2 (DIX V2) exclusively.

General migration actions: Hardware

Note: IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Table 35 provides more details about this migration action. Use this information to plan your changes to the system.

Table 35. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	<ul style="list-style-type: none">• 28 August 2012 in U.S. Announcement Letter for the zEC12.• 23 July 2013 in U.S. Announcement Letter for the zBC12.
Applies to migration from:	z/OS V2R2, V2R1 and z/OS V1R13.
Timing:	Before migrating to a zEC12 or zBC12 server.
Is the migration action required?	No, but recommended if you are using a zEC12 or zBC12 server because this is the last server that will support the changes mentioned in "Description".
Target system hardware requirements:	See "Description" on page 71.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Take into account the statements in "Description" on page 71 as you migrate to zEC12 or zBC12.

Reference information

None.

Migrate to an IBM zEnterprise z196 or z114 server Description

An IBM zEnterprise System includes a Central Processing Complex (CPC), either the IBM zEnterprise 196 (z196) server or the IBM zEnterprise 114 (z114) server, or both, the zEnterprise BladeCenter Extension (zBX) with its integrated optimizers or select IBM blades, and the zEnterprise Unified Resource Manager (Unified Resource Manager).

The z114 is an entry-level enterprise server with a smaller mainframe footprint than the IBM zEnterprise 196 (z196).

The specific zEnterprise functions including base support that are exploited by z/OS depend on the z/OS release, Table 36 on page 73 lists the z/OS functions that are included in the base support for the release.

Table 37 lists new functions that can be exploited by the release. For the PTFs that might be required, see “Actions you can take before you order a z196 and z114 server” on page 77.

Table 36. zEnterprise functions included in base z/OS supported for z/OS V2R1 and z/OS V2R2

zEnterprise function included in the base support (Y/N)	V2R1	V2R2
Base support	Y	Y
OSA-Express3 (GbE LX and SX, 1000BASE-T, 10 GbE LR and SR)	Y	Y
InfiniBand Coupling Links	Y	Y
New z/Architecture instructions	Y	Y
Up to 128 Coupling Links CHPIDs	Y	Y
FICON Express8 (CHPID FC)	Y	Y
IFAURP reporting	Y	Y
Greater than 64 CPs per server	Y (z196 only)	Y (z196 only)
Crypto toleration	Y	Y
OSA-Express3 (CHPID type OSD) with or without exploitation of two ports per CHPID	Y	Y
Up to 32 HiperSockets™	Y	Y
RMF postprocessor crypto activity report - 4096 bit	Y	Y
CPU measurement facility (HIS)	Y	Y
Greater than 64 CPs per LPAR	Y (z196 only)	Y (z196 only)
HiperDispatch cache and affinity node changes	Y	Y
HiperDispatch serviceability	Y	Y
LE high register resolution	Y	Y

Table 37. zEnterprise functions exploited by z/OS V2R1 and z/OS V2R2

zEnterprise function: exploitation of z/OS support • Y=Yes • N=No	V2R1	V2R2
Power save mode	Y (z196 only)	Y (z196 only)
OSA-Express4S (GbE LX and SX, and 10 GbE LR and SR)	Y	Y
OSA-Express4S improved port granularity	Y	Y
FICON Express8S support of zHPF single track operations	Y	Y
FICON Express8S support of zHPF multi-track operations	Y	Y
Coupling Facility Control Code (CFCC) Level 17	Y	Y
Three subchannel sets	Y (z196 only)	Y (z196 only)
IPL from alternate subchannel set	Y	Y
IBM zEnterprise Unified Resource Manager	Y	Y
IBM zEnterprise BladeCenter Extension (zBX) (Support for OSA CHPID types OSM and OSX.)	Y	Y

General migration actions: Hardware

Table 37. zEnterprise functions exploited by z/OS V2R1 and z/OS V2R2 (continued)

zEnterprise function: exploitation of z/OS support • Y=Yes • N=No	V2R1	V2R2
Crypto exploitation of ANSI X9.8 Pin security, enhanced Common Cryptographic Architecture (CCA), 64 Bit, CP Assist for Cryptographic Function (CPACF) enhancements, Secure Keyed-Hash Message Authentication Code (HMAC), CKDS Constraint Relief, PCI Audit, Elliptical Curve Cryptography (ECC) Digital Signature Algorithm, and CBC Key Wrap, PKA RSA OAEP with SHA-256.	Y	Y
Crypto exploitation. For Crypto Express3 feature when defined as a coprocessor: expanded support for AES algorithm, enhanced ANSI TR-31 Secure Key Exchange, PIN block decimalization table protection, and PKA RSA OAEP with SHA-256 algorithm, additional Elliptic Curve Cryptography (ECC) functions.	Y	Y
FICON Express8S (CHPID type FC)	Y	Y
zHPF performance improvements for FICON Express8S	Y	Y
z/OS Discovery and AutoConfiguration (zDAC) support	Y	Y
New OSA display command	Y	Y
OSA-Express3 and OSA-Express4S Inbound Workload Queuing (IWQ)	Y	Y
Inbound workload queuing for Enterprise Extender for the OSA-Express4S and OSA-Express3 features when defined as CHPID types OSD or OSX	Y	Y
OSA-Express4S checksum offload for LPAR-to-LPAR traffic for IPv4 and IPv6 packets (CHPID type OSD or OSX)	Y	Y
OSA-Express4S large send for IPv6 packets (CHPID types OSD and OSX)	Y	Y

Table 38 provides more details about this migration action. Use this information to plan your changes to the system.

Table 38. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	<ul style="list-style-type: none"> • The IBM zEnterprise 114 (z114), which shipped in September 2011. • The IBM zEnterprise 196 (z196), which first shipped in September 2010. • The IBM zEnterprise BladeCenter Extension (zBX), which shipped November 2010.
Applies to migration from:	z/OS V2R2, z/OS V2R1, and z/OS V1R13.
Timing:	Anytime before you introduce a z114 or z196 server into your environment.
Is the migration action required?	Yes, if you want to run z/OS V2R2, V2R1, or V1R13 on a z114 or z196 server, or if you want to run a Coupling Facility on a zEnterprise server. If you will run only a Coupling Facility on a z114 or z196 serversystem, then only the sysplex-related actions are relevant.

Table 38. Information about this migration action (continued)

Target system hardware requirements:	<ul style="list-style-type: none"> • A z196 or a z114 server. • Additional hardware required for specific functions. <ul style="list-style-type: none"> – zDAC requires: <ul style="list-style-type: none"> - Up-to-date controller microcode - Up-to-date switch microcode – IBM zEnterprise Blade Center Extension (zBX) is required for the IBM Smart Analytics Optimizer for DB2 for z/OS V1.1, the IBM WebSphere DataPower Integration Appliance XI50 for zEnterprise (DataPower XI50z), and select POWER7 and IBM System x blades. – An IBM System Storage® DS5020 is required for IBM Smart Analytics Optimizer.
Target system software requirements:	<ol style="list-style-type: none"> 1. See the list of PTFs in the Software Service Level section of the PSP buckets. 2. See “Install the necessary z/OS service, as indicated in PSP buckets” described in “General recommendations and considerations for a z196 or z114 server.”
Other system (coexistence or fallback) requirements:	<ul style="list-style-type: none"> • It is recommended that you install and run the z114 or z196 required service on your existing server. This will enable you to fall back from a hardware perspective, yet maintain your software level. • The PTFs to support CFCC Level 17 have coexistence (or sysplex preconditioning) PTFs that are required to be installed throughout your sysplex before implementing CFCC Level 17.
Restrictions:	See “Restrictions for a z196 or z114 server” on page 76.
System impacts:	None.
Related IBM Health Checker for z/OS check:	<p>IBM Health Checker for z/OS check, SUP_HiperDispatchCPUConfig, is added to z/OS V1R12 and available on z/OS V1R11. This check will verify that HiperDispatch is enabled on a zEnterprise system. For more information, see “HiperDispatch cache and affinity node changes” in “Migration and exploitation considerations for z196 and z114 server functions” on page 80.</p> <p>Note: The default of HIPERDISPATCH option in IEAOPTxx parmlib member was changed in z/OS V1R13 as follows:</p> <ul style="list-style-type: none"> • For IBM zEnterprise 196 (and follow-on processors): YES • For IBM System z10 processors: NO

Steps to take

Follow the “General recommendations and considerations for a z196 or z114 server,” adhere to the “Restrictions for a z196 or z114 server” on page 76, and perform the tasks described in the following topics.

Reference information

None.

General recommendations and considerations for a z196 or z114 server

As you plan your migration to a zEnterprise server, consider the following:

1. **Relatively few migration actions are new when coming from a z10 EC or a z10 BC server.** Migration to a zEnterprise server has, as its base, a migration to the z10 EC or z10 BC servers. This means that if you are migrating to a zEnterprise server from a z10 EC or z10 BC server, and have performed the migration actions associated with the z10 EC or z10 BC, you have fewer migration actions than if you were migrating from a server prior to the z10 EC or z10 BC and have not yet performed the migration actions associated with these servers. It is important to note that you can migrate directly to a zEnterprise server without installing the intermediate servers, but you still need to ensure that any migration considerations are satisfied for the servers that you “skipped.”

General migration actions: Hardware

2. **Support is delivered by service (and FMID web deliverables for ICSF).** The delta (from a z10 EC or z10 BC) support for a zEnterprise server, excluding cryptographic support, is delivered by service (PTFs) on older releases. The cryptographic support for the zEnterprise server continues to be FMIDs, many of which are still available in web deliverables. Different ICSF web deliverables, providing different levels of support, are available for different releases of z/OS. (See “Decide on the steps you will take for your migration to a zEnterprise server” in “Actions you can take before you order a z196 and z114 server” on page 77 for further information.)
3. **Larger coupling facility structure sizes might be necessary.** When you change coupling facility control code (CFCC) levels, your coupling facility structure sizes might change. zEnterprise servers initially ship with CFCC level 17. If, as part of your migration to a zEnterprise server, you change CFCC levels (either by placing a coupling facility on the zEnterprise server or by moving the coupling facility to a z10 EC or z10 BC at a later CFCC level), you might have larger structure sizes than you did previously. If your CFCC levels are identical, structure sizes are not expected to change when you migrate from a previous server to a newer generation server.
4. **Use the same software level throughout a sysplex.** Having members of a sysplex at the same software level (other than during brief migration periods) is good software management policy.
5. **Migrate hardware and software at different times.** To minimize the amount of change (and therefore risk) that you experience at one time, do not migrate your software release level at the same time that you migrate your hardware.
6. **Update SCRT to latest version.** If you use SCRT, make sure it is at the latest level. This is a requirement for vWLC, as well as when you upgrade servers. The latest level of SCRT can be downloaded from the SCRT web site at <http://www.ibm.com/eserver/zseries/swprice/scrt/>.

Restrictions for a z196 or z114 server

Restrictions associated with zEnterprise servers are:

1. **Functional limitations.** For a list of the zEnterprise functions that are available in each z/OS release, see Table 36 on page 73 and Table 37 on page 73. Some functions have migration or exploitation considerations (see “Migration and exploitation considerations for z196 and z114 server functions” on page 80). Many functions are enabled or disabled, based on the presence or absence of the required hardware and software. If you wish to position yourself to exploit any new zEnterprise functions, the software and hardware may be installed in either order. That is, there is no requirement to install either software or hardware first to exploit a specific function. However, due to outage windows and testing considerations, you might want to consider installing all the required software first, then upgrading the hardware and, finally, updating your customization to exploit the new functions.
2. **zEnterprise servers in a sysplex.**
 - zEnterprise servers z196 and z114 are supported in a Parallel Sysplex with other zEnterprise z196 and z114 servers, z10 EC and z10 BC servers, and z9 EC and z9 BC servers. If you introduce zEC12 or zBC12 into a sysplex with z196 or z114, ensure that you have satisfied the zEC12 or zBC12 sysplex restrictions in “Restrictions for a zEC12 or zBC12 server” on page 65. If you are running z/OS on zSeries z900, z800, z990, or z890 servers, then you cannot add a zEnterprise z196 and z114 server to that sysplex. That is, you will not be able to perform rolling IPLs to introduce a zEnterprise z196 and z114 server if you have any of the earlier (pre-System z) servers either as z/OS images or coupling facility images in the sysplex. The earlier servers in the sysplex must be upgraded to System z9 or later to have zEnterprise z196 and z114 servers supported in the sysplex. If you have any z/OS images or coupling facility images on an earlier server, and you intend to introduce a zEnterprise z196 and z114 server into that sysplex, you must migrate those images to System z9 (or later) server before introducing the zEnterprise z196 and z114 server.
 - The Integrated Cluster Bus 4 (ICB-4) Coupling Links are not supported on a zEnterprise CPC. Use 12x InfiniBand coupling links, which are designed to replace Integrated Cluster Bus 4 (ICB-4), and to complement 1x InfiniBand and ISC-3 on a zEnterprise server. InfiniBand coupling can provide significantly improved service times compared to ISC-3s for distances up to 150 meters. You can read about InfiniBand coupling links in *IBM System z Connectivity Handbook* (SG24-5444).
 - The zEnterprise servers cannot be connected to a Sysplex Timer (9037-002). The Server Time Protocol (STP) feature is the follow-on to the Sysplex Timer. STP is designed to allow multiple

servers and coupling facilities to maintain time synchronization with each other without requiring a Sysplex Timer. STP is a hardware feature of the zEnterprise, z10 EC, z10 BC, z9 EC, z9 BC, z990, and z890 servers. To implement STP, see the STP web site and the publications and other resources listed there. The STP web site is at <http://www.ibm.com/systems/z/advantages/pso/stp.html>.

The STP design introduced a concept called Coordinated Timing Network (CTN). A CTN is a collection of servers and coupling facilities that are time-synchronized to a time value called Coordinated Server Time. A CTN can be configured in two ways:

- STP-only CTN, which does not require a Sysplex Timer.
- Mixed-CTN (External Time Reference and STP), which does require a Sysplex Timer.

The Sysplex Timer provides the timekeeping information in a Mixed-CTN. Even though the zEnterprise servers do not support attachment to a Sysplex Timer, they can participate in a Mixed-CTN that has either a z10 or z9 server synchronized to the Sysplex Timer. This maintains the capability for enterprises to concurrently migrate from an existing External Time Reference (ETR) to a Mixed-CTN and from a Mixed-CTN to an STP-only CTN.

3. **Unsupported hardware features.** The following hardware features that were available on System z10 (and some earlier) servers cannot be ordered (and cannot be carried forward on an upgrade to a z114) server with zEnterprise servers. You must migrate to the newer technology available on zEnterprise servers.

- FICON Express
- FICON Express2
- Crypto Express2
- OSA-Express2 10 GbE LR

The following hardware features are not orderable on z196 servers. If they are installed on your existing server at the time of an upgrade to a z196 server, they may be retained.

- FICON Express4 10KM LX
- FICON Express4 SX
- FICON Express4 4KM LX
- OSA-Express2 GbE LX
- OSA-Express2 GbE SX
- OSA-Express2 1000BASE-T

The following hardware features are not orderable on z114 servers. If they are installed on your existing server at the time of an upgrade to a z114 server, they may be retained.

- FICON Express4 10KM LX
- FICON Express4 SX
- FICON Express4 4KM LX
- FICON Express4-2C 4KM LX
- FICON Express4-2C SX
- OSA-Express2 GbE LX
- OSA-Express2 GbE SX
- OSA-Express2 1000BASE-T

Actions you can take before you order a z196 and z114 server

You can perform the following migration actions before you order or install a z196 or z114 server:

1. **Review the sysplex configuration in which the z196 or z114 server will participate.** See “Restrictions for a z196 or z114 server” on page 76 for a description of the limitations when using IBM zEnterprise EC12 servers with zEnterprise z196 or z114 servers or with other earlier servers in a Parallel Sysplex.
2. **Implement STP (or a Mixed-CTN) timing network.** This action is needed because Sysplex Timers (9037-002) are not supported on zEnterprise servers.
3. **Migrate from ICB-4 to InfiniBand coupling links.** This action is needed because ICB-4 links are not supported on zEnterprise servers. If desired, you can take this action after you order a zEnterprise server, as you upgrade to the new server.

General migration actions: Hardware

4. **Migrate from unsupported hardware features to newer technology.** This action is needed because FICON Express, FICON Express2, Crypto Express2, and OSA-Express2 10 GbE LR are not supported on zEnterprise servers.
5. **Install the necessary z/OS service, as indicated in PSP buckets.** For a zEnterprise 196 CPC, PTFs are identified in the 2817DEVICE PSP bucket (Subset 2817/ZOS). For a zEnterprise 114 CPC, PTFs are identified in the 2818DEVICE PSP bucket (Subset 2818/ZOS). For an IBM zEnterprise BladeCenter Extension (zBX) attached to your z196 CPC or to your z114 CPC, the PTFs are identified in the 2458DEVICE PSP bucket (Subset 2458/ZOS). In each PSP bucket, the content is dependent on the z/OS release you will run on the zEnterprise server. If you reviewed the PSP buckets some time ago, review them again to ensure that any newly identified z/OS service has been installed. To assist you in determining if you have the recommended service (identified in these PSP buckets) installed on your system, you can use the SMP/E REPORT MISSINGFIX command in conjunction with the FIXCAT type of HOLDDATA, as follows:
 - a. Acquire and RECEIVE the latest HOLDDATA onto your z/OS system(s). Use your normal service acquisition portals or download the two (2) year HOLDDATA directly from <http://service.software.ibm.com/holdata/390holddata.html>. Ensure you select **Full** from the Download NOW column (last 730 days) to receive the FIXCAT HOLDDATA, as the other files do not contain FIXCAT HOLDDATA.
 - b. Run the SMP/E REPORT MISSINGFIX command on your z/OS systems and specify one or more of the following Fix Categories (FIXCAT):
 - IBM.Device.Server.z196-2817
 - IBM.Device.Server.z196-2817.ParallelSysplexInfiniBandCoupling
 - IBM.Device.Server.z196-2817.ServerTimeProtocol
 - IBM.Device.Server.z196-2817.zHighPerformanceFICON
 - IBM.Device.Server.z114-2818
 - IBM.Device.Server.z114-2818.ParallelSysplexInfiniBandCoupling
 - IBM.Device.Server.z114-2818.ServerTimeProtocol
 - IBM.Device.Server.z114-2818.zHighPerformanceFICON
 - IBM.Device.Server.z114-2818.UnifiedResourceManager
 - IBM.Device.Server.zBX-2458
 - IBM.Device.Server.zBX-2458.ISAOPTThe report will identify any missing coexistence and fallback PTFs for that system. For complete information about the REPORT MISSINGFIX command, see *SMP/E for z/OS Commands*.
 - c. Periodically, you might want to acquire the latest HOLDDATA and rerun the REPORT MISSINGFIX command to find out if there are any new PTFs recommended for the zEnterprise servers.

Note:

- a. You can also use the Service Link PSP Service Extraction tool.
 - b. Because the Enhanced PSP Tool (EPSPT) was removed the end of 2010, you can no longer use that tool to identify missing PSP bucket service. You should use SMP/E's Fix Category support, which is fully integrated into SMP/E procedures and IBM product and service deliverables.
6. **Run the CFSIZER and Sizer tools.** If you are moving your coupling facilities and the coupling facility structures will be on higher CFCC levels than they were previously, run the Coupling Facility Structure Sizer (CFSIZER) tool to find out if you have to increase coupling facility structure sizes. Run the Sizer utility, an authorized z/OS program that you can download, to evaluate structure size changes. The Sizer utility is distinct from CFSizer, and should be run after the new hardware (CFLEVEL) is installed but before any CF LPAR on the new hardware is populated with structures. z196 or z114 servers are initially shipped with CFCC Level 17; prepare to make the necessary changes as indicated by the tool. You can find the CFSIZER tool at Coupling Facility sizer (www.ibm.com/systems/support/z/cfsizer).

7. **Plan for the fixed HSA enhancement on a zEnterprise server.** On zEnterprise (and z10) servers, preplanning requirements are minimized by offering a fixed HSA and introduction of the ability to seamlessly include such events as creation of LPARs, inclusion of logical subsystems, changing logical processor definitions in an LPAR, and introduction of cryptography into an LPAR.
8. **Decide on the steps to take for your migration to a z196 or z114 server.** As a guide, see “Recommended migration steps for a z196 and z114 server” on page 80. Also, note the following:
 - You should compare the cryptographic support you currently have installed with the support required for the functions you plan to use on the zEnterprise z196 and z114 server. Several cryptographic support web deliverables have been made available for various z/OS releases. The newer cryptographic web deliverables include the previous function (when applicable) for that particular z/OS level. Note that you can use the newer cryptographic web deliverables on servers before the zEnterprise servers, that is, on z10 and z9 (or earlier) servers.
 - The level of function provided for cryptographic support differs by z/OS release and the ICSF web deliverable that is installed. For z/OS V1R12 and later, exploitation of zEnterprise z196 and z114 cryptographic support is provided by Cryptographic Support for z/OS V1R11-V1R13 (FMID HCR7790) web deliverable. Note that this level of ICSF is not integrated in z/OS V1R13 and must be downloaded and installed even after ordering a z/OS V1R13 ServerPac.
9. **Review the new mnemonics introduced for the z196 or z114 server.** The new mnemonics might collide with (be identical to) the names of assembler macro instructions you use or provide. In the event of such collisions, the HLASM’s default opcode table (UNI) will treat specification of these names as instructions when APAR PK97799 is installed. This will probably cause assembler error messages and possibly cause generation of incorrect object code. For a tool to help in identifying mnemonic conflicts, see *Techdoc PRS5289* at the IBM Techdocs website.

If you write programs in assembler language, you should compare the list provided in *z/Architecture Principles of Operation, SA22-7832*, to the names of assembler macro instructions you use or provide, to identify any such conflicts or collisions that would occur following installation of HLASM APAR PK97799. If a conflict is identified, take one of the following actions:

- Change the name of your macro instruction.
- Specify PARM=’...OPTABLE(YOP)...’ (or some other earlier opcode table).
- Specify a separate ASMAOPT file containing assembler options, such as in the previous method (this method requires no changes to source code or JCL).
- Add, as the first statement of your source program, *PROCESS OPTABLE(YOP).
- Specify the PROFILE option either in JCL or the ASMAOPT file, and the specified or default member of the SYSLIB data set is copied into the front of the source program.
- If you must use both a new instruction and a macro with the same name in an assembly, you can use the following technique (where XXX is a sample mnemonic):

```
Assume the default OPTABLE(UNI) is in effect
  XXX  a,b      new instruction
  PUSH ACONTROL save current optable definition
  ACONTROL OPTABLE(YOP) switch optable dynamically
  XXX  r,s,t    macro invocation
  POP  ACONTROL restore previous definition
  XXX  c,d      new instruction
```

For more information about the HLASM opcode table, see *HLASM Programmer’s Guide*.

Actions you can take after you order a z196 and z114 server

After you order, but before you install your zEnterprise server, do the following:

1. **Use the CHPID Mapping Tool.** As you might have done with your z10 EC, z10 BC, z9 EC or z9 BC servers, use the CHPID Mapping Tool to map logical CHPIDs to physical channels (PCHIDs) and create input to HCD/IOCP for your zEnterprise server. The tool is a workstation-based Java application available from the Resource Link[®] web site (<http://www.ibm.com/servers/resourcelink>). For more information about this tool, refer to the web site.

General migration actions: Hardware

2. **Define an Ensemble.** If you are running z/OS V1R10 or later, you can define an Ensemble and exploit the IBM zEnterprise Unified Resource Manager. See *System z Ensemble Planning and Configuration Guide (GC27-2608)* for the steps required to define an Ensemble.

Recommended migration steps for a z196 and z114 server

This topic suggests the steps for migrating your same z/OS release level from your current server to a zEnterprise server. The steps are based on the assumption that you want to minimize the amount of change (and therefore risk) and the amount of work required to perform the migration.

The migration steps follow:

1. If necessary, migrate to an STP-only or Mixed-CTN timing network.
2. Ensure that you have installed the z196, z114, z10 EC (or z10 BC), and z9 EC (or z9 BC) required service, as indicated in the respective PSP buckets. See "Install the necessary z/OS service, as indicated in PSP buckets" in "Actions you can take before you order a z196 and z114 server" on page 77 for information about how to identify, acquire, and install any missing required service.
3. Ensure you have the required service, and any required ICSF web deliverable installed for the cryptographic functions that you have decided to use.
4. Upgrade your hardware to zEnterprise system. If necessary convert to InfiniBand Coupling Links from ICB-4 links.
5. Update configuration setting to exploit zEnterprise functions.

Migration and exploitation considerations for z196 and z114 server functions

This topic provides migration and exploitation considerations for zEnterprise server functions.

The following zEnterprise functions are available on z/OS V1R12 and later releases:

- **InfiniBand Coupling.** Each system can use, or not use, InfiniBand coupling links independently of what other systems are doing, and do so in conjunction with other link types. InfiniBand Coupling connectivity can only be performed with other systems that also support InfiniBand Coupling.
- **HiperDispatch.** The existing HIPERDISPATCH=YES|NO parameter in IEAOPTxx member of parmlib, and on the SET OPT=xx command to control whether HiperDispatch is enabled or disabled for the system, can be changed dynamically.

A WLM goal adjustment might be required when using HiperDispatch. Review and update your WLM policies as necessary.

- **HiperDispatch cache and affinity node changes.** This function is enhanced to exploit zEnterprise architecture and now allows three physical CPUs from same chip to form affinity node. A z10 uses HiperDispatch book cache support and four physical CPUs from same book.

To realize the benefits of HiperDispatch, z/OS has been changed to force HiperDispatch=YES for LPARs with greater than 64 CPUs. On LPARs with greater than 64 CPUs defined on a zEnterprise server with IEAOPTxx specifying HIPERDISPATCH=NO during IPL (or SET OPT=xx after IPL), the system generates a message but continues to run with HIPERDISPATCH=YES. The new message is IRA865I HIPERDISPATCH=YES FORCED DUE TO GREATER THAN 64 LPS DEFINED.

On LPARs in which HIPERDISPATCH=NO is specified with less than 64 CPUs, you can dynamically add more CPUs and continue to run in HIPERDISPATCH=NO. However, you may see the new message ISN012E HIPERDISPATCH MUST BE ENABLED TO CONFIGURE CPU IDS GREATER THAN 3F ONLINE.

Any attempt to configure CPUs greater than 64 CPUs online in HIPERDISPATCH=NO will be rejected with message IEE241I CPU(x) NOT RECONFIGURED ONLINE - REQUIRES HIPERDISPATCH ENABLED.

An LPAR with greater than 64 CPUs that dynamically changed to HIPERDISPATCH=YES cannot go back to HIPERDISPATCH=NO. It will be treated as if it was IPLed with HIPERDISPATCH=YES after HIPERDISPATCH=YES is activated.

To assist with warning when you are getting close to 64 CPUs and running with HIPERDISPATCH=NO, the IBM Health Checker for z/OS check, SUP_HiperDispatchCPUConfig, was

added in z/OS V1R12. The check always succeeds for LPAR in HIPERDISPATCH=YES (all CPU configurations supported). When an LPAR is running with HIPERDISPATCH=NO, the check raises an exception when the number of CPUs is close to forcing the LPAR to IPL with HIPERDISPATCH=YES. The CPUSLEFTB4NEEDHD parameter indicates the minimum number of CPUs that can be installed and activated on an LPAR running in HIPERDISPATCH=NO. When CPUSLEFTB4NEEDHD=0, the check always succeeds. The default is 8, with values 0-63 accepted. To assist with warning when you are getting close to 64 CPUs and running with HIPERDISPATCH=NO, use IBM Health Checker for z/OS check, SUP_HiperDispatchCPUConfig. Possible IBM Health Checker for z/OS messages:

- IEAVEH080I CPU configuration supported with HiperDispatch *curstate*
- IEAVEH081E CPU configuration supported with HiperDispatch disabled. *numcpus* more CPU(s) can be added with HiperDispatch disabled.
- **CFCC Level 17.** If you are moving your coupling facilities and the coupling facility structures will be on higher CFCC levels than they were previously, run the Coupling Facility Structure Sizer (CFSIZER) tool to find out if you have to increase coupling facility structure sizes. zEnterprise servers initially shipped with CFCC Level 17. Prepare to make the necessary changes as indicated by the tool. You can find the CFSIZER tool at Coupling Facility sizer (www.ibm.com/systems/support/z/cfsizer).

Note: The PTFs to support CFCC Level 17 have coexistence (or sysplex preconditioning) PTFs that require installation throughout your sysplex before implementing CFCC Level 17.

- **Third Subchannel Set.** You now have the ability to extend the amount of addressable storage capacity to help facilitate storage growth with the introduction of a third subchannel set, an additional 64K devices, to help complement other functions such as "large" or extended addressing volumes and HyperPAV. This may also help to facilitate consistent device address definitions, simplifying addressing schemes for congruous devices.

The first subchannel set (SS 0) allows definitions of any type of device, such as bases, aliases, secondaries, and those other than disk that do not implement the concept of associated aliases or secondaries. The second and third subchannel sets (SS1 and SS2) can now both be designated for use for disk alias devices (of both primary and secondary devices), or Metro Mirror secondary devices only. The third subchannel set applies ESCON, FICON and zHPF protocols. Definitions for the third subchannel set are similar to those for the second subchannel set and can be made with HCD.

The IODF statement of LOADxx allows users to indicate which devices to use during IPL (that is, devices that are connected to subchannel set 0, 1 or 2). This specification is done on the IODF statement (column 36). For more information, see *z/OS MVS Initialization and Tuning Reference*.

- **IPL from alternate subchannel set.** This function allows you to IPL from subchannel set 1 (SS1) or subchannel set 2 (SS2), in addition to subchannel set 0. Devices used early during IPL processing can now be accessed using subchannel set 1 or subchannel set 2. This is intended to allow users of Metro Mirror (PPRC) secondary devices defined using the same device number and a new device type in an alternate subchannel set to be used for IPL, IODF, and standalone dump volumes when needed. IPL from an alternate subchannel set is supported by z/OS V1R13 and later, and applies to the FICON and zHPF protocols (CHPID type FC).

To IPL from an alternate subchannel set, you need to specify a 5 digit load address on the LPAR image profile on the HMC, and have the appropriate specification on the IODF statement column 36 in LOADxx. This capability is available for z196 as of September 2011 (GA2) and later and for z114. z114 supports only SS0 and SS1, so you cannot IPL from subchannel set 2 (SS2).

Tip: Column 36 of the IODF statement in LOADxx is the subchannel set indicator. This field indicates which subchannel set should be used as the primary volume during IPL. You can now specify an asterisk "*" for this value in the field to indicate that the subchannel set of the IPL volume should be used as the subchannel set for the primary volumes. APAR OA35135 for z/OS V1R11 and V1R12 added this new function to specify an asterisk '*' in column 36 of the IODF statement in LOADxx parmlib member.

- **IBM zEnterprise Unified Resource Manager for enabling management and virtualization of heterogeneous workloads.** The Unified Resource Manager manages the deployment of heterogeneous hardware resources based on individual workload requirements:

General migration actions: Hardware

- Performance management
- Integrated private data network

See *System z Ensemble Planning and Configuration Guide* (GC27-2608) for the steps that are required.

- **Power save mode.** This function is available only on z196 servers. There is a new SMFPRMxx parmlib option, MAXEVENTINTRECS, that allows governing the number of event interval records to be collected when the processor capacity changes. The default is zero. This function is available only on z196 servers; it is not available on z114 servers.

If you are using the CPU Measurement Facility (Hardware Instrumentation Services), there is a new parameter on the MODIFY *hisproc* command. You can use this parameter, STATECHANGE, to override the default action to take when a CPU speed change is detected within the HIS component.

- **zHPF performance improvements for FICON Express8S.** FICON Express8S contains a new IBM ASIC which is designed to support the 8 Gbps (gigabytes per second) PCIe interface to the PCIe I/O drawer and increased start I/Os. In addition, a hardware data router has been added in support of the zHPF and FCP protocols for path length reduction and increased throughput. FICON Express8S supports a link data rate of 2, 4, or 8 Gbps autonegotiated. With these changes FICON Express8S, when supporting the zHPF or FCP protocols, has been designed to achieve full duplex line speed (8 Gbps) in each direction. The performance of the FICON protocol remains unchanged from FICON Express8. To use zHPF performance improvements for FICON Express8S, you need to specify the ZHPF=YES | NO parameter in the IECIOSxx member of PARMLIB and use FICON Express8S.
- **Additional Crypto exploitation.** The following enhancements have been added to the Common Cryptographic Architecture support, which is used in the Crypto Express3 feature when it is configured as a coprocessor:
 - ANSI X9.8 Pin security
 - Enhanced Common Cryptographic Architecture (CCA), 64bit, CP Assist for Cryptographic Function (CPACF) enhancements
 - Secure Keyed-Hash Message Authentication Code (HMAC)
 - CKDS Constraint Relief
 - PCI Audit, Elliptical Curve Cryptography (ECC) Digital Signature Algorithm
 - CBC Key Wrap
 - PKA RSA OEAP with SHA-256
 - Expanded support for AES algorithm
 - Enhanced ANSI TR-31 Secure Key Exchange
 - PIN block decimalization table protection
 - PKA RSA OAEP with SHA-256 algorithm, additional Elliptic Curve Cryptography (ECC) functions.

- **z/OS Discovery and AutoConfiguration (zDAC) for FICON channels.** With a zEnterprise CPC and z/OS, a new function, z/OS Discovery and AutoConfiguration (zDAC), is designed to automatically perform a number of I/O configuration definition tasks for new and changed disk and tape controllers through FICON channels. Starting with z/OS V2R1 FICON point-to-point paths are also included in the discovery process whether or not they are connected to a switch or director when attached to a FICON channel. When new controllers are added to an I/O configuration, or changes are made to existing controllers, the system is designed to discover them and propose configuration changes based on a policy you define in the Hardware Configuration Definition (HCD) dialog. Your policy can include preferences for availability and bandwidth including parallel access volume (PAV) definitions, control unit numbers, and device number ranges.

zDAC is designed to perform discovery for all systems in a sysplex that support the function. The proposed configuration will incorporate the current contents of the I/O definition file (IODF) with additions for newly installed and changed control units and devices. zDAC is designed to help simplify I/O configuration on CPC running z/OS and reduce complexity and setup time. zDAC applies to all FICON features supported on zEnterprise servers when configured as CHPID type FC, and is supported by z/OS V1R12 and later.

To use zDAC, you must first establish a policy for the discovery operation. This is done through HCD or HCM. You can limit the scope of the discovery, limit the proposal information, indicate the desired number of paths to discovered logical control units, and indicate the method used for device and

control unit numbering. After controllers and devices are discovered, you can select which controllers to be defined and accept or override the proposed values for control units and devices.

- **OSA-Express3 and OSA-Express4S Inbound Workload Queuing (IWQ).** Inbound workload queuing for Enterprise Extender is supported by the OSA-Express4S and OSA-Express3 features when defined as CHPID types OSD or OSX. It is exclusive to the z196 and z114 servers, and is supported by z/OS and by z/VM for guest exploitation. OSA-Express3 introduces inbound workload queuing (IWQ), which creates multiple input queues and allows OSA to differentiate workloads “off the wire” and then assign work to a specific input queue (per device) to z/OS. With each input queue representing a unique type of workload, each having unique service and processing requirements, the IWQ function allows z/OS to preassign the appropriate processing resources for each input queue. This approach allows multiple concurrent z/OS processing threads to then process each unique input queue (workload), avoiding traditional resource contention. In a heavily mixed workload environment, this “off the wire” network traffic separation provided by OSA-Express3 IWQ reduces the conventional z/OS processing required to identify and separate unique workloads, which results in improved overall system performance and scalability. The types of z/OS workloads that are identified and assigned to unique input queues are:
 - z/OS Sysplex Distributor traffic: Network traffic that is associated with a distributed Virtual Internet Protocol Address (VIPA) is assigned a unique input queue allowing the Sysplex Distributor traffic to be immediately distributed to the target host.
 - z/OS bulk data traffic: Network traffic that is dynamically associated with a streaming (bulk data) TCP connection is assigned to a unique input queue allowing the bulk data processing to be assigned the appropriate resources and isolated from critical interactive workloads.

IWQ is supported on zEnterprise CPC and System z10, and is exclusive to OSA-Express3 CHPID types OSD and OSX (exclusive to zEnterprise CPC). There are some Communications Server configuration settings required to enable multiple inbound data queues.

- **Display OSAINFO.** OSA-Express3 introduces the capability for the operating system to directly query and display the current OSA configuration information (similar to OSA/SF). z/OS exploits this new OSA capability by introducing a new TCP/IP operator command, Display OSAINFO. Display OSAINFO allows the operator to monitor and verify the current OSA configuration, which helps to improve the overall management, serviceability, and usability of OSA-Express3. The Display OSAINFO command is exclusive to OSA-Express3 CHPID types OSD, OSM, and OSX (on z196, z114, and z10 servers).
- **XL C/C++ ARCH(9) and TUNE(9) options.** The ARCHITECTURE XL C/C++ compiler option selects the minimum level of machine architecture on which your program can run. Certain features provided by the compiler require a minimum architecture level. ARCH(9) exploits instructions available on zEnterprise servers. For more information, refer to the ARCHITECTURE compiler option in *z/OS XL C/C++ User's Guide*. The TUNE compiler option allows you to optimize your application for specific machine architecture. The TUNE level has to be at the ARCH level, at a minimum. If the TUNE level is earlier than the specified ARCH level, the compiler forces TUNE to match the ARCH level, or uses the default TUNE level, whichever is greater. For more information about the ARCHITECTURE and TUNE compiler options refer to *z/OS XL C/C++ User's Guide*.

Exploitation restriction. When programs exploit the ARCH(9) or TUNE(9) option, those programs can only run on zEnterprise servers, or an operation exception will occur. This is a consideration for programs that will run on different server levels (z10 and z9 servers) during development, test, and production, as well as during fallback or disaster recovery.

The following zEnterprise functions are only available on z/OS V1R13 and later releases. See *z/OS Introduction and Release Guide* for restrictions, dependencies, and steps to take to use these new hardware functions:

- **OSA-Express4S checksum offload for LPAR-to-LPAR traffic for IPv4 and IPv6 packets (CHPID type OSD).** Checksum offload for LPAR-to-LPAR traffic is included in the OSA-Express4S design. The checksum function has been moved from the PCIe adapter to the OSA-Express4S hardware to help reduce CPU utilization.

General migration actions: Hardware

- **OSA-Express4S large send for IPv6 packets (CHPID types OSD and OSX).** Large send (also referred to as TCP segmentation offload) is designed to improve performance by offloading outbound TCP segmentation processing from the host to an OSA-Express4S feature by employing a more efficient memory transfer into OSA-Express4. Large send support for IPv6 packets applies to the OSA-Express4S features (CHPID type OSD and OSX), and is exclusive to z196 and z114.
- **Inbound workload queuing for Enterprise Extender.** Inbound workload queuing (IWQ) for the OSA-Express4S features has been enhanced to differentiate and separate inbound Enterprise Extender traffic to a new input queue. The Enterprise Extender separation and processing associated with the Enterprise Extender input queue provides improved scalability and performance for Enterprise Extender.

Reference information

See *z/OS Communications Server: IP Configuration Guide* for more information about the following functions:

- OSA-Express4S checksum offload for LPAR-to-LPAR traffic for IPv4 and IPv6 packets (CHPID type OSD)
- OSA-Express4S large send for IPv6 packets (CHPID types OSD and OSX)
- Inbound workload queuing for Enterprise Extender.

Accommodate functions for the z196 and z114 servers to be discontinued on future servers

Description

The following changes in hardware support could affect your environment. Make the appropriate changes as needed.

- **ISC-3 features (#0217, #0218, #0219).** The IBM zEnterprise zEC12 is planned to be the last high-end System z server to offer support of the InterSystem Channel-3 (ISC-3) for Parallel Sysplex environments at extended distances. ISC-3 will not be supported on future high-end System z servers as carry forward on an upgrade. Previously it was announced that the IBM zEnterprise 196 (z196) and IBM zEnterprise 114 (z114) servers were the last to offer ordering of ISC-3. Enterprises should continue migrating from ISC-3 features (#0217, #0218, #0219) to 12x InfiniBand (#0171 - HCA3-O fanout) or 1x InfiniBand (#0170 - HCA3-O LR fanout) coupling links.
- **Power Sequence Controller (PSC feature #6501).** The last zEnterprise server machines to support PSC (feature #6501) are the z196 (machine type 2817) and z114 (machine type 2818). PSC features cannot be ordered and cannot be carried forward on an upgrade to the zEC12 server. The optional PSC feature is used to turn on or off specific control units from the central processor complex (CPC).
- **ESCON channels.** The last zEnterprise server to support ESCON channels are the z196 (machine type 2817) and z114 (machine type 2818). In addition, ESCON channels cannot be carried forward on an upgrade to the zEC12 server. This applies to channel path identifier (CHPID) types CNC, CTC, CVC, and CBY and to feature numbers 2323 and 2324. You should be migrating from ESCON to FICON and eliminating ESCON channels from the mainframe wherever possible. Alternate solutions are available for connectivity to ESCON devices. IBM Global Technology Services offers an ESCON to FICON migration solution, Offering ID #6948-97D, to help facilitate migration from ESCON to FICON. This offering can help you to simplify and manage a single physical and operational environment.
- **OSA-Express2 features.** The z196 is the last high-end server, and the z114 is the last mid-range server, to support OSA-Express2 features. OSA-Express2 features are not supported on future servers. You should begin migrating from OSA-Express2 features (#3364, #3365, #3366) to OSA-Express3 1000BaseT and OSA-Express4S features.
- **Dial-up modems.** The z196 is the last high-end server, and the z114 is the last mid-range server, to support dial-up modems for use with the Remote Support Facility (RSF), and the External Time Source (ETS) option of Server Time Protocol (STP). These features are not supported on future servers. The currently available Network Time Protocol (NTP) server option for ETS, as well as Internet time

services available using broadband connections, can be used to provide the same degree of accuracy as dial-up time services. You should begin migrating from dial-up modems to broadband for RSF connections.

Note: IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Table 39 provides more details about this migration action. Use this information to plan your changes to the system.

Table 39. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	<ul style="list-style-type: none"> • 12 July 2011 in U.S. Announcement Letter 211-252. • 15 February 2011 in U.S. Announcement Letter 111-012. • 22 July 2010 in U.S. Announcement letter 110-170.
Applies to migration from:	z/OS V2R2, z/OS V2R1, and z/OS V1R13.
Timing:	Before migrating to a z114 or z196 server.
Is the migration action required?	Yes.
Target system hardware requirements:	See "Description" on page 84.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Take into account the statements in "Description" on page 84 as you plan for the future.

Reference information

None.

Ensure that you are running on supported servers and storage controllers

Description

z/OS V2R2 runs on the following IBM System z servers:

- IBM z Systems z13 (z13).
- IBM zEnterprise EC12 (zEC12).
- IBM zEnterprise BC12 (zBC12).
- IBM zEnterprise 196 (z196), which is withdrawn from marketing.
- IBM zEnterprise 114 (z114), which is withdrawn from marketing.
- IBM System z10[®] (z10 EC, z10 BC), which is withdrawn from marketing.

General migration actions: Hardware

In addition, z/OS V2R2 supports these and later IBM storage control units:

- 3990 Model 3 and 3990 Model 6
- 9393
- 2105
- 2107
- 2421
- 2422
- 2423
- 2424

The following IBM servers are no longer supported to run z/OS V2R2:

- IBM System z9[®] (z9 BC, z9 EC)
- IBM eServer zSeries 990 (z990)
- IBM eServer zSeries 890 (z890)
- IBM eServer zSeries 900 (z900)
- IBM eServer zSeries 800 (z800)

Note that running z/OS V2R2 as a z/VM[®] guest has the same requirements as running natively in an LPAR.

Table 40 provides more details about this migration action. Use this information to plan your changes to the system.

Table 40. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS VR13.
Timing:	Anytime
Is the migration action required?	Yes, if you use any of the servers or controllers that are no longer supported to run with z/OS V2R2.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.

Table 40. Information about this migration action (continued)

System impacts:	<ul style="list-style-type: none"> During IPL/NIP processing, if you try to use an unsupported control unit for z/OS V2R2, you receive the following error condition for devices under the control unit . IEA434I (nnnn) ONLINE IS NOT ALLOWED, INVALID CONTROL UNIT MODEL During VARY ONLINE command processing after IPL/NIP, you receive the following error condition for devices under the unsupported control unit: IEA434I DEVICE ONLINE IS NOT ALLOWED, INVALID CONTROL UNIT MODEL If you IPL z/OS V2R2 on a server that it does not support, you might receive wait state 07B-1E (decimal 30). Note: The number of IEA434I messages is limited to 32 during IPL/NIP to avoid exhausting initial ESQA. An IEA444I message will be reported one time during IPL/NIP to indicate that additional IEA434I messages have been suppressed: IEA444I NUMBER OF IEA434I MESSAGES EXCEEDS NIP MAXIMUM
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Determine whether the servers and control units that you use are supported for z/OS V2R2. If you have a question about support for any devices not listed, contact your IBM representative.
- Install replacement servers and control units. Detach unsupported servers and control units from the system and delete their corresponding definitions from the input/output definition file (IODF).

Reference information

For more information, see *Release memorandum - RFA 58183 - 04/15/13 (IBM Guide 27.10)*.

Replace unsupported devices

Description

You should remove and replace devices that were supported by earlier releases but cannot be used with the current release of z/OS because they are no longer supported.

Table 41 provides more details about this migration action. Use this information to plan your changes to the system.

Table 41. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.

General migration actions: Hardware

Table 41. Information about this migration action (continued)

Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Anytime.
Is the migration action required?	Yes, if you use any of the devices that are no longer supported.
Target system hardware requirements:	Replacement devices as necessary.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Determine whether the devices you use are supported. A list of supported I/O devices is in the topic about identifying I/O device requirements in *z/OS Planning for Installation*. If you have a question about support for any devices not listed, contact your IBM representative.
2. Install replacement devices. Move data that is stored on unsupported devices to the supported devices. Detach unsupported devices from the system and delete their corresponding device definitions from the input/output definition file (IODF).

Reference information

For more information, see the following references:

- For a list of I/O devices that are supported, see the topic about identifying I/O device requirements in *z/OS Planning for Installation*.
- For information about deleting device definitions from the IODF, see *z/OS HCD User's Guide*.

Provide for new device installations

Description

The hardware configuration of your processors and I/O devices determines how many devices you can attach to your system. z/OS supports attachment of up to 65,280 devices, each with up to eight access paths.

Table 42 provides more details about this migration action. Use this information to plan your changes to the system.

Table 42. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Anytime.
Is the migration action required?	Yes, if you are going to use new devices with z/OS V2R2 and later.
Target system hardware requirements:	Dependent upon the new devices used.
Target system software requirements:	None.

Table 42. Information about this migration action (continued)

Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

The following are general considerations related to I/O device support.

- *Attaching devices through HCD.* You can define, or attach, new devices to your system through the interactive panels of the Hardware Configuration Definition (HCD) base element. HCD has dynamic I/O capabilities, changing hardware definitions without the need for an IPL or hard power-on reset. Any time you make changes to your I/O configuration, you need to use HCD to modify your system's I/O definition file (IODF). You should also update the input/output configuration data set (IOCDS) when you run HCD to ensure that the configuration information is consistent across the software and microcode.
- *Operating modes.* Most devices attached to z/OS operate in full function mode, that is, all features on the device are compatible with, and usable on, the operating system. Some of these features include:
 - For DASD devices: dynamic path reconnection, extended count-key-data operation, and caching and cache-related facilities
 - For tape devices: cartridge stack loading and data compaction
 Some devices also operate in compatibility mode, which allows you to simulate the function of another device or model. Compatibility mode causes the device to function like a different device of the same type, ignoring some or all of the additional features the device might have. This allows you to migrate between devices with minimal impact on programs that have device dependencies.
- *UCB virtual storage constraint relief.* Each device attached to the system has one or more UCBs associated with it. You have the option to define UCBs either above or below the 16 MB line by specifying the LOCANY parameter on the Hardware Configuration Definition (HCD) panel. The system programmer should review the contents of the link pack area (LPA) list to determine whether to remove or move libraries to gain virtual storage constraint relief.
- *Hardware maintenance.* Some devices require a specific level of hardware maintenance to operate properly on a z/OS system. DFSMS software support for new hardware devices might also require the installation of PTFs.

Reference information

For more information, see the following references:

- For a summary of the most commonly-used I/O devices supported by z/OS that are also directly supported by DFSMS functions, see the topic about identifying I/O devices in *z/OS Planning for Installation*. If you have a question about support for a device that is not listed, contact your IBM representative.
- For more information about HCD, see *z/OS HCD Planning*.
- For information about working with IODFs, see *z/OS HCD User's Guide*.

Update your CFRM policy with coupling facility structure size changes

Description

If you are migrating to a new level of coupling facility control code (CFCC), you have to make appropriate coupling facility structure size updates in the z/OS coupling facility resource management (CFRM) policy.

General migration actions: Hardware

Table 43 provides more details about this migration action. Use this information to plan your changes to the system.

Table 43. Information about this migration action

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Anytime.
Is the migration action required?	Yes, if you are migrating to a new CFCC level.
Target system hardware requirements:	See http://www.ibm.com/systems/z/advantages/pso/cftable.html .
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you are migrating to a new CFCC level, do the following:

1. Run the Coupling Facility Structure Sizer (CFSizer) tool. This tool sizes structures, taking into account the amount of space needed for the current CFCC levels. The tool sizes for the most currently available level; you might find that the results are oversized if you use an earlier CFCC level. You can find the tool at Coupling Facility sizer (www.ibm.com/systems/support/z/cfsizer).
Alternatively, you can run an as-is batch utility program called SIZER after you have brought a new CFLEVEL coupling facility into use in your configuration. SIZER examines your currently allocated coupling facility structures and recalculates the size that should be used for them with the new later-CFLEVEL coupling facility. The as-is SIZER utility is available as a zipped package that you can download from <http://www.ibm.com/systems/support/z/cfsizer/altsize.html>.
2. Update the CFRM policy with the size modifications that are needed.
3. Activate the updated CFRM policy so that it becomes the active policy governing structure allocation in the sysplex.

Reference information

For more information about coupling facility code levels and the processors that support those levels, see <http://www.ibm.com/systems/z/advantages/pso/cftable.html>.

Chapter 3. Migration from z/OS V2R1

Chapter 3 describes those actions for anyone who is migrating from z/OS V2R1.

Sysplex migration actions

This topic summarizes actions for you to take if you are migrating systems that are members of a base sysplex or Parallel Sysplex configuration.

Sysplex actions related to hardware upgrades

Title of migration action	Page or topic
"Migrate to an IBM z13 or IBM z13s server" on page 43	"Migrate to an IBM z13 or IBM z13s server" on page 43
"Migrate to an IBM zEnterprise EC12 or IBM zEnterprise BC12 server" on page 60	"Migrate to an IBM zEnterprise EC12 or IBM zEnterprise BC12 server" on page 60
"Migrate to an IBM zEnterprise z196 or z114 server" on page 72	"Migrate to an IBM zEnterprise z196 or z114 server" on page 72
"Update your CFRM policy with coupling facility structure size changes" on page 89	"Update your CFRM policy with coupling facility structure size changes" on page 89
"Relocate Cross System Extended Services (XES) component trace buffers" on page 113	"Relocate Cross System Extended Services (XES) component trace buffers" on page 113
"Consider the new COUPLExx CFRMTAKEOVERCF(NO) default" on page 128	"Consider the new COUPLExx CFRMTAKEOVERCF(NO) default" on page 128

Sysplex actions to perform before installing z/OS V2R2

Element or feature	Title of migration action	Page or topic
Multiple	"Install coexistence and fallback PTFs" on page 6	"Install coexistence and fallback PTFs" on page 6
BCP	"Use LOGR Couple Data Set at format level HBB7705" on page 95	"Use LOGR Couple Data Set at format level HBB7705" on page 95
DFSMSdfp	"DFSMSdfp: Back up SMS control data sets" on page 168	"DFSMSdfp: Back up SMS control data sets" on page 168

Migration actions from z/OS V2R1: Sysplex

Sysplex actions to perform before the first IPL of z/OS V2R2

Element or feature	Title of migration action	Page or topic
BCP	"Format the ARM couple data set for long symbol table support" on page 105	"Format the ARM couple data set for long symbol table support" on page 105
BCP	"Relocate Cross System Extended Services (XES) component trace buffers" on page 113	"Relocate Cross System Extended Services (XES) component trace buffers" on page 113
BCP	"Consider the new COUPLExx CFRMTAKEOVERCF(NO) default" on page 128	"Consider the new COUPLExx CFRMTAKEOVERCF(NO) default" on page 128

Sysplex actions to perform after the first IPL of z/OS V2R2

None.

BCP migration actions

This topic describes migration actions for the base element BCP (Base Control Program).

BCP actions to perform before installing z/OS V2R2

This topic describes BCP migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Evaluate your stand-alone dump data set allocations and your IPCS processing of them

Description

As your applications grow in size and use greater amounts of storage, you should evaluate whether the DASD allocated for your stand-alone dump data continues to be adequate.

In z/OS V1R6, support was introduced for extended-format sequential data sets, a form of data set that is SMS-managed and can occupy more than 64 K tracks per volume. In z/OS V1R7, this support was supplemented with support for large format sequential data sets (DSNTYPE=LARGE), a form of data set that is essentially the same as conventional sequential data sets except that more than 64 K tracks may be spanned per volume. If your stand-alone dump data sets are spread over more volumes than you want, both types of support can help you gain better control over the number of volumes used for each stand-alone dump data set.

Table 44 provides more details about the migration action. Use this information to plan your changes to the system.

Table 44. Information about this migration action

Element or feature:	BCP.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.

Table 44. Information about this migration action (continued)

Is the migration action required?	No, but recommended because of changes that have been made to stand-alone dump processing (that reorder dump records with the intent of recording more important data early), and especially recommended if you deploy any LPARs with significantly more main storage than previously used.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Use multivolume stand-alone dump data sets. Adjust the number of volumes and their separation to achieve tolerable stand-alone dump capture times.
- Use extended-format sequential data sets or large format sequential data sets. Copy their contents to an extended-format, compressed, striped data set using the IPCS COPYDUMP subcommand before analysis. Use the same or a larger striping factor than you used for your stand-alone dump data sets. Dump data sets to which stand-alone dump can write may be neither compressed nor striped, but both attributes are advantageous for the target of the copy operation. Starting with z/OS V1R12, stand-alone dump data sets can be placed in track-managed space as well as cylinder-managed space on Extended Address Volumes (EAV).
- Use a large CISIZE and striping for IPCS dump directories, and use blocking, striping, and compression for the stand-alone dump data set. Very large stand-alone dumps might require that you define your directory with the extended addressing attribute, allowing it to hold more than 4 GB.

Tip: Control interval sizes less than 24K have been shown to be more vulnerable to fragmentation when used as IPCS dump directories, and IPCS performance can be degraded when such fragmentation occurs. In this background, warning message BLS21110I will be issued and you might recreate the DDIR by using the CLIST BLSCDDIR.

BLS21110I CISIZE(cisize) is less than 24K. It may degrade IPCS performance

Reference information

For more information, see the following references:

- For information about dump data set allocation, extended format sequential data sets, large format sequential data sets, and multivolume dump data sets, see *z/OS MVS Diagnosis: Tools and Service Aids*.
- For stand-alone dump procedures, see *z/OS V2R2 Problem Management*.

AMBLIST uses the system-determined block size for SYSPRINT Description

With APAR OA46441 applied, the AMBLIST utility uses the system determined block size when it creates the SYSPRINT data set. Before APAR OA46441, AMBLIST used (by default) a block size equal to the record length for allocating the SYSPRINT data set, if the block size was not specified or was specified as 0.

Migration actions from z/OS V2R1: BCP

Table 45 provides more details about this migration action. Use this information to plan your changes to the system.

Table 45. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V2R1 and z/OS V1R13, both with APAR OA46441 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA46441.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you expect the SYSPRINT data set that is created by AMBLIST to have a block size other than the system determined block size.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	If a program opens the SYSPRINT data set created by AMBLIST with DCB RECFM=FA or RECFM=FA, LRECL=121 parameters, the program is abended with message IEC141I 013-60.
Related IBM Health Checker for z/OS checks:	None.

Steps to take

Check for JCL and programs that use the AMBLIST utility to write SYSPRINT output to a sequential data set, and ensure that block sizes are specified explicitly where appropriate. For example, suppose that a program that refers to the SYSPRINT data set expects a new SYSPRINT data set to have a block size of 121 (BLKSIZE=121). If so, you must specify this value explicitly in the SYSPRINT DD statement when you run the AMBLIST utility. For any programs that open the SYSPRINT data set with the DCB parameters RECFM=FA or RECFM=FA, LRECL=121, remove the RECFM and LRECL parameter from the DCB macro. Or, change the record format value to FBA (RECFM=FBA).

Reference information

For more information about the AMBLIST utility, see *z/OS MVS Diagnosis: Tools and Service Aids*.

Plan to move from SHARED mode to DISTRIBUTED mode for consoles

Description

z/OS V2R2 is the last release in which the SHARED console mode is supported. You must migrate to DISTRIBUTED mode, which was introduced in z/OS V1R10.

Table 46 provides more details about the migration action. Use this information to plan your changes to the system.

Table 46. Information about this migration action

Element or feature:	BCP
When change was introduced:	See <i>Statement of direction: IBM z/OS IBM United States Software Announcement 212-086 April 11, 2012</i>
Applies to migration from:	z/OS V2R1 and z/OS V1R13.

Table 46. Information about this migration action (continued)

Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended if you are using SHARED console mode. When shared mode is removed, you are required to move to DISTRIBUTED mode.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	Fallback considerations exist; see topic on migration and fallback considerations in <i>z/OS MVS Planning: Operations</i> .
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	Use check IBM CNZ,CNZ_CONSOLE_OPERATING_MODE to determine whether your installation is operating in the DISTRIBUTED console mode, which is preferred.

Steps to take

Move from SHARED mode to DISTRIBUTED mode for your console environment. Note that the default changed from SHARED to DISTRIBUTED mode in z/OS V1R13.

Tip: You can check the current mode by using the command **DISPLAY OPDATA,MODE**.

Reference information

For more information, see the following references:

- *Statement of direction: IBM z/OS IBM United States Software Announcement 212-086 April 11, 2012.*
- For DISTRIBUTED mode, see *z/OS MVS Planning: Operations*

Use LOGR Couple Data Set at format level HBB7705

Description

IBM recommends that you use the highest format level LOGR couple data set (CDS) that can be used by the lowest system release level in your sysplex. This will allow for the latest system logger features to be available, given the sysplex configuration. Currently, the highest LOGR CDS format level is HBB7705 (introduced in z/OS V1R2). This format level is established by providing the ITEM NAME(SMDUPLEX) NUMBER(1) specification in the IXCL1DSU couple data set format utility program.

Table 47 provides more details about the migration action. Use this information to plan your changes to the system.

Table 47. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V1R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended to allow for the latest system logger features to be available, given the sysplex configuration. If your LOGR couple data sets are already at HBB7705 level, this migration action does not apply to you.

Migration actions from z/OS V2R1: BCP

Table 47. Information about this migration action (continued)

Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	System Logger does not allow the introduction of an alternate LOGR CDS that is formatted at a lower-level than the primary.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Determine your current LOGR couple data set level. Use the **D XCF,C,TYPE=LOGR** command. If your LOGR couple data sets are at level HBB7705, you do not need to perform this migration action.
2. Use the IXCL1DSU (format couple data set utility) and include the ITEM NAME(SMDUPLEX) NUMBER(1) specification to obtain at least two LOGR CDSs at the HBB7705 format level, with:
 - LOGR CDS *primarydsname* on volume *primaryvolume*
 - LOGR CDS *alternatedsname* on volume *alternatevolume*

Note: SMDUPLEX item NUMBER(1) is the default value when you run the IXCL1DSU utility on z/OS V2R2.

3. After you create the HBB7705 format-level LOGR CDSs, you can dynamically bring them into your existing sysplex with these SETXCF commands:
 - SETXCF COUPLE,TYPE=LOGR,ACOUPLE=(*primarydsname,primaryvolume*)
 - SETXCF COUPLE,TYPE=LOGR,PSWITCH
 - SETXCF COUPLE,TYPE=LOGR,ACOUPLE=(*alternatedsname,alternatevolume*)
4. Remember to also specify, in your COUPLExx member of SYS1.PARMLIB, these two LOGR CDSs as the primary and alternate for any future sysplex IPLs:

```
DATA
TYPE(LOGR)
PCOUPLE(primarydsname,primaryvolume)
ACOUPLE(alternatedsname,alternatevolume)
```

Note: If you did not bring the newly formatted HBB7705 LOGR CDSs into the sysplex (with the SETXCF commands in the Step 3) prior to the first z/OS system that IPLs into the sysplex using the COUPLExx member identifying the newly formatted LOGR CDSs, then there will be no persistent logger data from before the IPL. Therefore, no log stream data exists when this first system IPLs.

Reference information

For more information, see the following references:

- For information about using the IXCL1DSU format couple data set utility for system logger, see the "LOGR parameters for format utility" section of *z/OS MVS Setting Up a Sysplex*.
- For considerations on the system logger functions that are supported using the different LOGR CDS format levels, see the "LOGR couple data set versioning - new format levels" section of *z/OS MVS Setting Up a Sysplex*.
- For details on the SETXCF command, see *z/OS MVS System Commands*.
- For information about the COUPLExx SYS1.PARMLIB member, see *z/OS MVS Initialization and Tuning Reference*.

Update Capacity Provisioning Manager parameters to use CIM Client for Java Version 2

Description

z/OS V2R1 was the last release to include Version 1 of the Standards Based Linux Instrumentation for Manageability (SBLIM) CIM client for Java. Version 1 support for SourceForge open source project was discontinued in 2010. Version 2 of the SBLIM client, which is designed to be a JSR48-compliant implementation, was included in z/OS V1R13 and z/OS V2R1. Users of SBLIM Version 1 must convert to Version 2.

Table 48 provides more details about the migration action. Use this information to plan your changes to the system.

Table 48. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use SBLIM Version 1.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. The Provisioning Manager user CPOSRV needs READ access to CIM Client for Java Version 2 **sblim-cim-client.jar**. This access usually by default should be sufficient. If it is not, you must set the "other" READ access file permissions using the z/OS UNIX command **chmod** (for example, `chmod o+r/usr/lpp/wbem/jclicent/sblim-cim-client2.jar`). Note that this command must be issued by a user with the appropriate authorization.
2. If your CIM installation directory is not at the default location, you need to add the location of the CIM Client for Java Version 2 **slim-cim-client2.jar** to the CLASSPATH entry., If you have already specified the location of a previous version of the CIM Client Java, you need to add the location of CIM Client for Java Version 2 before the location of the previous version of CIM Client for Java. the CLASSPATH is specified in the ENV member of the Provisioning Manager runtime environment data set with prefix.PARM. The prefix for the data set name is the high-level qualifier of the Capacity Provisioning Manager parameters data set and the name of the domain managed by the Capacity Provisioning Manager. For example, with default values, the data set name is CPO.DOMAIN1.PARM.

Reference information

For more information, see *z/OS MVS Capacity Provisioning User's Guide*.

Migration actions from z/OS V2R1: BCP

Update a Capacity Provisioning Manager parameter to avoid a defined capacity WTOR

Description

In z/OS V2R2, the Provisioning Manager can detect when a manual change to defined capacity or group capacity would interfere significantly with Capacity Provisioning management. In such cases, the Provisioning Manager suspends its management of defined capacity or group capacity and issues one of the following write-to-operator-with-reply (WTOR) messages:

CPO4218I

New DC for *systemName/sysplexName*. Previous base *previousLimit* MSU. Enter 1 to set base to *currentLimit* or 2 to set to *newLimit* MSU

CPO4219I

New GC for *groupName/CPCname*. Previous base *previousLimit* MSU. Enter 1 to set base to *currentLimit* or 2 to set to *newLimit* MSU.

In response, the operator can choose to reinitialize the capacity management by setting the management base to the new capacity value and its managed capacity to 0, or continue the capacity management by adapting the management base to the manual change.

If you want the Provisioning Manager to continue managing the defined capacity or group capacity, regardless of manual changes, you can suppress the WTOR by setting the key

DefinedCapacity.BaseToleration to 100 in the Capacity Provisioning Manager parameter file.

In z/OS V2R2, the default value of this key is 15, meaning that while Capacity Provisioning is managing a defined capacity, any concurrent manual reduction in defined capacity by more than 15% causes the WTOR to be issued.

Table 49 provides more details about the migration action. Use this information to plan your changes to the system.

Table 49. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use Capacity Provisioning for managing defined capacity or group capacity and you want to avoid a WTOR for large manual reductions of defined capacity or group capacity.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Add the entry `DefinedCapacity.BaseToleration=100` to the Capacity Provisioning parameter file.

By default, the parameter file is named CPO.DOMAIN1.PARM(PARM).

Reference information

For information about how to define the new key to the Capacity Provisioning Manager parameters, see *z/OS MVS Capacity Provisioning User's Guide*.

BCP actions to perform before the first IPL of z/OS V2R2

This topic describes BCP migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Create IPL text

Description

IPL text is bootstrap information required for IPL, such as the location of the nucleus library. You must create IPL text by running ICKDSF against the system residence volume.

Table 50 provides more details about the migration action. Use this information to plan your changes to the system.

Table 50. Information about this migration action

Element or feature:	BCP.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Update and run the IPLTEXT job to write a new copy of the IPL text. If you install z/OS with a ServerPac, an installation dialog job is provided to perform this action. If you install z/OS with a CBPDO, instructions to perform this action are provided in *z/OS Program Directory* at the z/OS installation related information website.

Tip: With ICKDSF R17 APAR PM42057, a new parameter called REMOVEIPLTXT has been added to the REFORMAT command that allows you to remove IPL text from the volume.

Note: When the IPLTXTEXIST parameter (which was introduced by ICKDSF R17 APAR PK16403) is specified with the REFORMAT command using the IPLDD parameter, WTOR message ICK21836D is suppressed if IPL text already exists.

Migration actions from z/OS V2R1: BCP

Reference information

For a sample IPLTEXT job, see *z/OS Program Directory* at the z/OS installation related information website. ServerPac provides a similar job for accomplishing this task; see *ServerPac: Installing Your Order*.

Review the list of WTORs in parmlib member AUTOR00

Description

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.

Table 51 provides more details about the migration action. Use this information to plan your changes to the system.

Table 51. Information about this migration action

Element or feature:	BCP.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use the auto reply facility of z/OS, which is enabled by default when the AUTOR00 member is found in the parmlib concatenation, as of z/OS V1R12.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- 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.

Note: The IBM-shipped data set SYS1.IBM.PARMLIB contains the AUTOR00 member. So, if you specify it within the PARMLIB concatenation and will not intend to activate the auto reply functionality, you need to specify AUTOR=OFF in the IEASYSxx parmlib member.

Reference information

For more information, see the following references:

- For more information about the AUTORxx and IEASYSy parmlib members, see *z/OS MVS Initialization and Tuning Reference*
- For the contents of AUTOR00, see *z/OS MVS Planning: Operations*.

Reassemble the stand-alone dump program

Description

The stand-alone dump program produces a dump of storage that is occupied by a system that failed or a stand-alone dump program that failed. You must reassemble the stand-alone dump program each release. When the stand-alone dump program is properly created on a DASD residence volume, it resides in the SYS1.PAGEDUMP.Vvolser data set.

Table 52 provides more details about the migration action. Use this information to plan your changes to the system.

Table 52. Information about this migration action

Element or feature:	BCP.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Reassemble the stand-alone dump program. If you install z/OS with a ServerPac, an installation dialog job is provided to perform this action. If you install z/OS with a CBPDO, instructions to perform this action are provided in *z/OS MVS Diagnosis: Tools and Service Aids*.

Reference information

For more information, see the following references:

- *ServerPac: Installing Your Order*
- *z/OS MVS Diagnosis: Tools and Service Aids*

Plan for HWIREXX helper program restriction for z/OS BCPii

Description

Starting with z/OS V2R1, users of the z/OS BCPii System REXX helper program HWIREXX are required to have at least READ authority to the FACILITY class resource HWI.HWIREXX.execname as defined in the security product. This function is provided in APAR OA45932 with PTF UA75120.

Table 53 provides more details about the migration action. Use this information to plan your changes to the system.

Table 53. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R1 with APAR OA45932.

Migration actions from z/OS V2R1: BCP

Table 53. Information about this migration action (continued)

Applies to migration from:	z/OS V2R1 without APAR OA45932 applied, and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use the BCPii helper program HWIREXX.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	The security product definitions as described need to be implemented to restrict use of the HWIREXX helper program.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- To allow you to run your BCPii System REXX exec using the HWIREXX helper program, you must have at least READ authority to the FACILITY class resource HWI.HWIREXX.*execname*, where *execname* specifies a 1 to 8 character System REXX exec to be executed by the HWIREXX helper application. Also, BCPii requires the FACILITY class to be RACLIST-specified.

The RACF syntax is as follows:

```
RDEFINE FACILITY HWI.HWIREXX.execname UACC(NONE)
PERMIT HWI.HWIREXX.execname CLASS(FACILITY) ID(userid) ACCESS(READ)
SETROPTS RACLIST(FACILITY) REFRESH
```

If the caller does not have sufficient SAF authorization to run the HWIREXX program, HWIREXX return code 112 (in decimal) is returned.

Reference information

For more information, see *z/OS MVS Programming: Callable Services for High-Level Languages*.

Adjust parameters to start IOSHMCTL in TPC-R Basic Hyperswap environment Description

With APAR OA40866 applied (with one of the following PTFs: UA71220 for z/OS V2R1, or UA71219 for z/OS V1R13), parameters supplied in the JCL to start PGM=IOSHMCTL may be rejected. APAR OA40866 introduced new function which caused JCL parameter checking to now be enforced. As a result, unsupported parameters will be rejected and IOSHMCTL will not start due to JCL failures.

For example:

```
ASA101I SYNTAX ERROR: MODE=EXT, WAS SEEN, WHERE ONE OF
(SOCKPORT=)
WOULD BE CORRECT.
DETECTING MODULE IS IOSHMCTL
```

Prior to APAR OA40866, unsupported parameters would be ignored and IOSHMCTL would start without any JCL failures.

Note: This problem is a documentation error where some examples of JCL to start the Basic HyperSwap address space used incorrect parameters. At this time with Basic HyperSwap Sockets Server APAR OA40866 applied, the only parameter allowed to the IOSHMCTL program is 'SOCKPORT=*port_num*'. Any other parameters are rejected.

Table 54 provides more details about the migration action. Use this information to plan your changes to the system.

Table 54. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R1 and z/OS V1R13, both with APAR OA40866 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA40866 applied.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have unsupported parameters specified to start the Basic HyperSwap address space.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- When applying the PTF for APAR OA40866, make sure that any HSIB procedures to start IOSHMCTL do not include unsupported parameters. For example, the following JCL may be used:

```
//HSIB JOB MSGLEVEL=(1,1),TIME=NOLIMIT,REGION=0M
//IEFPROC EXEC PGM=IOSHMCTL
```

Tip: Some older publications, including Redpapers, might have documented incorrect parameters on the PARM statement used in the examples of suggested procedures for starting IOSHMCTL. It is best to refer to the latest TPC-R publications for current supported parameters.

Reference information

For more information, see APAR OA46189, which describes the potential JCL failures after installing PTFs for APAR OA40866.

Accommodate system symbol names that contain underscores

Description

z/OS V2R2 enhances the use of system symbols in the following ways:

- Longer system symbol names (up to 16 characters) and longer symbol substitution values
- Underscores (_) can be specified in any character position other than the first one.

System symbols are typically used in started procedures and jobs, parmlib members, and other objects. Information about using system symbols is provided in *z/OS MVS Initialization and Tuning Reference*.

Migration actions from z/OS V2R1: BCP

For objects that undergo system symbol substitution, be aware that the use of underscores in symbol names can result in an incompatibility if a symbol reference is followed immediately by an underscore (that is, without a symbol-delimiting period). For example, in previous releases, specifying &SYM_A in a file would match the symbol &SYM and add "_A". In z/OS V2R2, this specification can match the symbol &SYM or the symbol &SYM_A. Here, a match is attempted first for &SYM_A (with the underscore). If no match is found, an attempt is made to match &SYM.

Note: As of z/OS z/OS 2.1, underscores can be specified in JES symbol names. Thus, this migration action does not apply to JES symbol names.

Table 55 provides more details about the migration action. Use this information to plan your changes to the system.

Table 55. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have situations in which a symbol name might be followed immediately by an underscore.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	In a sysplex of mixed releases of z/OS systems, if you use symbol names with underscores, you must ensure that earlier systems can handle the symbol names. Install the toleration PTF for APAR OA46739 on the earlier systems. The PTFs for this APAR are identified with the SMP/E FIXCAT IBM.Coexistence.z/OS.V2R2.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

In z/OS V2R2, IBM provides a REXX exec, ASASYMUN, to help you locate data that might encounter unexpected results if symbol names have underscores. You can run the exec on z/OS V2R2 and older systems.

ASASYMUN scans a PDS or PDSE for situations where a symbol name that contains an underscore might cause different results than expected. For example, it checks for a symbol (an ampersand followed by other characters) followed immediately by an underscore with no delimiting period. Change these lines to add a period before the underscore to delimit the symbol.

ASASYMUN is supplied by IBM in the SBLSCLI0 data set. To use ASASYMUN, you must invoke it from an ISPF environment.

Follow these steps:

1. From the ISPF command line, run the exec as follows:

```
TSO EXEC execdsn(ASASYMUN) 'scandsn'
```

Where:

execdsn

is the cataloged data set containing the ASASYMUN exec. Use 'execdsn(ASASYMUN)' if the data set name is fully qualified. You can use alternative forms of execdsn(ASASYMUN) if the data set is in the SYSEXEC or SYSPROC concatenation of the user. For example, you might be able to specify just (ASASYMUN).

scandsn

is the PDS or PDSE you want to scan. Specify a data set contain statements subject to symbol substitution, like JCL or parmlib statements. If the data set name is fully qualified, double the quotations around the name in addition to the single quotation marks that surround the parameter. For example, specify '''fully.qual.dsn''' for a fully qualified data set.

- For any references you find that were intended to be resolved by a symbol, add a period before the underscore to delimit the symbol. For example:

```
&SYM._A
```

Reference information

For information about specifying system symbols, see *z/OS MVS Initialization and Tuning Reference*.

Format the ARM couple data set for long symbol table support**Description**

z/OS V2R2 systems require an ARM couple data set (CDS) that is formatted for long symbol table support. Otherwise, V2R2 systems can join the sysplex, but are not ARM-capable. You can establish this format level by using the z/OS V2R2 level of the IXCL1DSU format utility (either from a z/OS V2R2 system or with a STEPLIB to a z/OS V2R2 MIGLIB) to format the CDS.

Table 56 provides more details about the migration action. Use this information to plan your changes to the system.

Table 56. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if systems are intended to use ARM functions.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None required. Systems at lower-level releases can use an ARM CDS formatted for long symbol-table support. However, a DISPLAY XCF,COUPLE,TYPE=ARM command from a down-level system cannot indicate that the HBB77A0 level of symbol table is in use unless you apply the PTFs for OA46977. With the PTFs for OA46977 applied, the response message IXC358I contains the text HBB77A0 SYMBOL TABLE SUPPORT.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

Migration actions from z/OS V2R1: BCP

1. Use the IXCL1DSU (format couple data set utility) at the z/OS V2R2 level to obtain at least two ARM CDSs at the HBB77A0 format level, with:
 - ARM CDS *primarydsname* on volume *primaryvolume*
 - ARM CDS *alternatedsname* on volume *alternatevolume*
2. After you create the HBB77A0 format-level ARM CDSs, you can dynamically bring them into your existing sysplex with these SETXCF commands:
 - SETXCF COUPLE,TYPE=ARM,ACOUPL=(*primarydsname,primaryvolume*)
 - SETXCF COUPLE,TYPE=ARM,PSWITCH
 - SETXCF COUPLE,TYPE=ARM,ACOUPL=(*alternatedsname,alternatevolume*)
3. Remember to also specify, in your COUPLExx member of SYS1.PARMLIB, these two ARM CDSs as the primary and alternate for any future sysplex IPLs :

```
DATA
TYPE(ARM)
PCOUPLE(primarydsname,primaryvolume)
ACOUPLE(alternatedsname,alternatevolume)
```

Reference information

For more information, see the following references:

- For information about the SETXCF command, see *z/OS MVS System Commands*.
- For information about the COUPLExx SYS1.PARMLIB member, see *z/OS MVS Initialization and Tuning Reference*.

Ensure that PARMDD or REGIONX are not used as job statement symbols

Description

z/OS V2R1 adds PARMDD and z/OS V2R2 adds REGIONX as new keywords on the JCL EXEC statement and PROC statement. Because JCL keyword names are reserved, you must ensure that your jobs do not use symbols with these same names. That is, if a job contains the symbolic parameter name PARMDD or REGIONX on the EXEC or PROC statement, you must edit the job to use an alternatively named symbol. Otherwise, the job can fail with a JCL error.

Table 57 provides more details about the migration action. Use this information to plan your changes to the system.

Table 57. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V2R2 (REGIONX) and z/OS V2R1 (PARMDD).
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you used symbol names REGIONX or PARMDD on EXEC or PROC statements in jobs.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Jobs that use PARMDD or REGIONX as an EXEC or PROC statement symbol name will fail with a JCL error.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Search for a symbol named PARMDD or REGIONX in all libraries that contain JCL, such as procedure libraries. Specifically, search for the following occurrences:

- PROC statements that contain a symbolic parameter named PARMDD or REGIONX.

Examples:

```
//PROC1 PROC PARMDD=ABC
//PROC1 PROC REGIONX=ABC
```

- EXEC statements that contain a symbolic parameter named PARMDD or REGIONX.

Examples:

```
//JSTEP1 EXEC PROC1,PARMDD=ABC
//JSTEP1 EXEC PROC1,REGIONX=ABC
```

- EXEC statements that contain a '®IONX' PARM or '&PARMDD' parameter value string.

Examples:

```
//STEP1 EXEC PGM=MYPROG,PARM='&PARMDD'
//STEP1 EXEC PGM=MYPROG,PARM='&REGIONX'
```

For any occurrences that you find, change the PROC or EXEC statement to refer to another symbolic parameter name.

Reference information

For information about JCL statements, see *z/OS MVS JCL Reference*.

Examine your IEFUSI exit routine for possible changes

Description

z/OS V2R2 includes a number of functional enhancements to support improved region management, including:

REGIONX keyword

New JCL keyword for the JOB and EXEC statements. JCL programmers can use REGIONX to explicitly request precise below-the-line and above-the-line storage amounts.

SMFLIMxx parmlib member

New parmlib member. Your installation can use SMFLIMxx to set rules for the REGION and MEMLIMIT values in job steps, or cancel job steps that violate the rules.

These changes include new parameter input fields for the IEFUSI exit routine. If your installation uses an IEFUSI exit routine to control job region size, it is recommended that you examine the routine for possible changes that you might need to make.

Note the following changes in the exit input parameter list:

- If the REGIONX keyword is used, the "region requested" value in sub-word 2 (as pointed to by word 5) is updated to contain a value based on the two values that were supplied on the REGIONX keyword. This change allows an existing exit routine to continue to receive the total amount of storage that was requested by the job step. Specifically, the value now contains either of the following values:
 - A value of 0 when the REGIONX second parameter is 0M, 0K, or 0G
 - The larger of the specified values when the REGIONX second parameter is not 0M, 0K, or 0G
 If the REGIONX keyword is not used, the IEFUSI input parameter list contains one "region requested" value in sub-word 2. This behavior is the same as in previous releases of z/OS.
- For job steps that include the REGIONX keyword, sub-word 1, bit 3 (as pointed to by word 5), indicates that separate values are also available. Here, two more words are provided, sub-word 7 and 8 (as pointed to by word 5), which provide the below-the-line and above-the-line values on the REGIONX keyword.

Migration actions from z/OS V2R1: BCP

If the total size indicated in sub-word 2 is not specific enough for your purposes, you can have your exit routine use the values in sub-word 7 and 8 to set the existing below- and above-the-line output fields in sub-words 2, 3, 4, and 5, as pointed to by word 5 of the input parameter list.

No additions or changes to the output parameter list are needed for REGIONX-related processing. The output parameter list allows for specifying separate above- and below-the-line values, as in previous releases of z/OS.

After the IEFUSI exit routine runs, the system checks the SMFLIMxx member for rules that might override region limits. This processing allows the existing IEFUSI exit to continue to set region and MEMLIMIT values for its various functions, including functions that are not supported by SMFLIMxx, such as setting limits on data space blocks. The SMFLIMxx member can be used to set values for new work or to override IEFUSI values for changes to existing work, thus reducing the need for more IEFUSI exit code changes.

In some cases, however, your installation might require that the IEFUSI exit routine make the final determination. If so, the exit routine can set a new flag (sub-word 1, bit 4, as pointed to by word 5) to bypass the SMFLIMxx rules. This bit essentially disables the SMFLIMxx processing for the current job step.

Note: A sample IEFUSI exit routine is provided in SYS1.SAMPLIB in member IEEUSI. For more information about changes that might be needed, see the commented sections in the sample IEFUSI exit routine.

Table 58 provides more details about the migration action. Use this information to plan your changes to the system.

Table 58. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	No, but recommended to ensure that users who specify a REGIONX value in their JCL receive the correct storage allocation, according to your installation's requirements.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- If your installation uses an IEFUSI exit routine, examine it to determine whether changes are required for the REGIONX keyword and SMFLIMxx member processing.

It is possible that no action is needed, if the decisions made by the exit routine are generic, such as setting the region above-the-line value 128 MB for all job steps. If the exit sets storage values using sub-word 2 (as pointed to by word 5) and a job uses REGIONX, the exit continues to set the desired value. Here, the REGIONX value is ignored and the IEFUSI selected storage value is used.

SMFLIMxx processing, if activated by specifying SMFLIM= as part of IPL parameters or through the SET SMFLIM= operator command, overrides the IEFUSI exit-returned values, if environmental conditions match the job step's current environment.

- If you determine that your IEFUSI exit routine requires updating, you can modify your routine by using the new values in the input parameter list. For example, you can have your exit routine do the following:
 - Use the new REGIONX values for below- and above-the-line storage for region size determinations. These values are provided in sub-word 7 and 8 (as pointed to by word 5), when sub-word 1, bit 3 is set to 1.
 - Bypass SMFLIMxx processing for certain jobs by setting sub-word 1, bit 4 (as pointed to by word 5).
- Or, you can remove all region and MEMLIMIT processing from your routine, and create SMFLIMxx statements to limit the REGION and MEMLIMIT values. Here, you might retain your routine to perform other types of processing, such as setting limits on data space blocks.

Reference information

For more information, see *z/OS MVS Installation Exits*.

Assess the use of the INCLUDE1MAFC keyword on the LFAREA parameter in IEASYSxx

Description

Prior to z/OS V2R2, the default was for RSM not to include 1 M fixed frames in the available frame count (RCEAFC). APAR OA41968 added the INCLUDE1MAFC keyword on the LFAREA parameter in the IEASYSxx member of parmlib to cause RSM to include 1 M fixed frames in the available frame count. This results in the following system behavior:

- RSM performs less paging when there is an abundance of available 1 M fixed frames in the system.
- RSM is more likely to break up 1 M fixed frames to satisfy 4 K page demand. Although RSM attempts to coalesce broken up 1 M fixed frames when there is fixed 1 M page demand, there is no guarantee that coalescing will be successful, especially if any of the 4 K frames making up the fixed 1 M page is fixed long term.

Starting with z/OS V2R2, RSM includes 1 M fixed frames in the available frame count by default; you no longer need to specify INCLUDE1MAFC to do this. Furthermore, the syntax of the INCLUDE1MAFC keyword has been extended to include a YES or NO option. The former INCLUDE1MAFC keyword syntax is still valid and can now also be specified as INCLUDE1MAFC(YES).

IBM recommends that you accept the default (or specify INCLUDE1MAFC or INCLUDE1MAFC(YES)). However, if you have a need to retain the old default behavior (that is, to exclude 1 M fixed frames from the available frame count), you must specify INCLUDE1MAFC(NO).

Table 59 provides more details about the migration action. Use this information to plan your changes to the system.

Table 59. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you did not specify the INCLUDE1MAFC keyword on the LFAREA parameter in IEASYSxx prior to z/OS V2R2 and you want to continue excluding 1 M fixed frames from the available frame count.

Migration actions from z/OS V2R1: BCP

Table 59. Information about this migration action (continued)

Target system hardware requirements:	None.
Target system software requirements:	RMF APAR OA42066 for z/OS V2R1 RMF APAR OA42510 for z/OS V1R13
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Check the LFAREA parameter specification in the IEASYSxx member on your pre-z/OS V2R2 system.
 - If you specified the INCLUDE1MAFC keyword on the LFAREA parameter after APAR OA41968, and you want to continue with that setting on your z/OS V2R2 system, you can do any of these things:
 - Leave the INCLUDE1MAFC keyword as it is.
 - Remove the INCLUDE1MAFC keyword, as it is now the default.
 - Change INCLUDE1MAFC to INCLUDE1MAFC(YES).
 - If you did not specify the INCLUDE1MAFC keyword on the LFAREA parameter and you want to retain the old default behavior, you must now specify INCLUDE1MAFC(NO).
- Check any application programs that use the STGTEST SYSEVENT to determine if any changes need to be made. The STGTEST event returns information about the amount of storage available in the system, which includes the LFAREA when INCLUDE1MAFC(YES) is specified or defaulted. Application programs can check the RCEINCLUDE1MAFC bit to determine the setting of INCLUDE1MAFC in the LFAREA specification.

Reference information

For information about the LFAREA parameter and the INCLUDE1MAFC keyword in IEASYSxx, see *z/OS MVS Initialization and Tuning Guide*.

Plan for the use of freemained frames

Description

To enhance system performance on the IBM z13, there might be cases where the system does not free the real frame that is backing a virtual page following a FREEMAIN, that is, when the page no longer contains any GETMAIN-assigned storage ranges. If so, the system will clear or “dirty” the frame to ensure that sensitive information is removed. Such a frame is referred to as a *freemained frame*. Freemained frames do not cause the count of frames owned by the address space (RAXFMCT) to be decremented (as they would have previously), nor do they cause the count of available frames within the system (RCEAFC) to be incremented (as they would have previously). Instead, the system uses a new counter, RAX_FREEMAINEDFRAMES, to keep track of the number of frames backing freemained pages in the address space with which the RAX is associated.

This feature is active by default on the IBM z13 and only applies to region private “low” storage (below 2GB), which is defined as subpools 0-127, 129-132, 240, 244, 250-252. Storage subpools define the characteristics of virtual storage below 2 GB and are discussed in detail in *z/OS MVS Diagnosis: Reference*.

The SYSEVENT STGTEST API reports on the current usage of real storage, returning a three-word value:

Word 1

Use of this number affects system performance very little, if at all.

Word 2

Use of this number affects performance to some degree.

Word 3

Use of this number may substantially affect performance.

To maintain compatibility with prior releases, SYSEVENT STGTEST will include most of Rce_FreemainedFrames in word 1 and all of it in words 2 and 3 for z/OS V2R1 (HBB7790) and z/OS V1R13 (JBB778H). For z/OS V2R2 (HBB77A0), SYSEVENT STGTEST is changed to exclude Rce_FreemainedFrames from word 1.

Programs that reference or issue TPROT instructions against region private storage that is not GETMAIN assigned might not experience an 0C4 system abend nor get a non-zero condition code where they previously would have. This applies to the subpools listed earlier.

The following new parameters in the DIAGxx member of parmlib allow you to disable this feature, if necessary:

FREEMAINEDFRAMES(NO)

Disables the freemained frames feature on a system-wide basis.

FREEMAINEDFRAMES(YES) [EXCLUDEJOBLIST(job1[,job2,...])]

Enables the freemained frames feature, except for the specified jobs. Up to eight job names may be specified. The job names may include the * and ? wildcard characters, where the * character is allowed in any position.

Reissuing the SET DIAG command with different EXCLUDEJOBLIST values will *not* increase the total number of excluded jobs; the last EXCLUDEJOBLIST specification overrides any previous specifications.

Disabling this feature for selected jobs will cause performance degradation for the entire system, not just for the specified jobs.

You can use the DISPLAY DIAG command to verify that the system is using the requested FREEMAINEDFRAMES statement.

Note: The DISPLAY DIAG command does not report the default value. The FREEMAINEDFRAMES statement only appears in the IGV007I message when it has been specified in the DIAGxx member. Therefore, you can use the DISPLAY DIAG command to verify that the system is using the specified FREEMAINEDFRAMES statement.

Table 60 provides more details about the migration action. Use this information to plan your changes to the system.

Table 60. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2. z/OS V2R1 and z/OS V1R13 (with the RSM web deliverable), both with APAR OA46291 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13 (with the RSM web deliverable).
Timing:	Before the first IPL of z/OS V2R2.

Migration actions from z/OS V2R1: BCP

Table 60. Information about this migration action (continued)

Is the migration action required?	<p>Yes, unless you disable this feature. Otherwise, installations that use software tools that monitor real storage usage must install updates to accommodate the advent of freemained frames.</p> <p>Applications that invoke the TPROT instruction to determine whether pages of region private storage have been GETMAIN assigned should change to use the VSMLOC or VSMLIST services. The IARQDUMP service may also be applicable in some cases.</p> <p>If none of these services meet the performance requirements of the application, then the application should use the new IARBRVER and IARBRVEA services provided with APAR OA46291 and z/OS V2R2.</p>
Target system hardware requirements:	IBM z13.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	<ul style="list-style-type: none">• Address spaces may appear to be using more storage than before the feature is enabled or by default.• The system may appear to have less available storage than before the feature is enabled or by default.• References to non-GETMAIN assigned storage may not result in a 0C4 system abend.• The TPROT instruction may not return a condition code of 3 in cases where it previously would have done so.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Verify that the value of RceOA46291Applied is B'1' before using any other new fields in the RCE or RAX data areas, as the new fields are not guaranteed to be initialized otherwise.
- Programs that reference RAXFMCT can subtract Rax_FreemainedFrames to determine how much real storage the address space is currently using.
- Programs that reference RCEAFC can add RCE_FreemainedFrames to determine how much storage is not currently in use. If an application is referencing RCEAFC to determine how much storage is available to be used by the application, a better solution is to use SYSEVENT STGTEST.
- If an application needs to determine whether a virtual address range is GETMAIN assigned, it should use the VSMLOC or VSMLIST services, instead of using the LLAG or TPROT assembly language instructions. These services are documented in *z/OS MVS Programming: Authorized Assembler Services Reference SET-WTO* and can be invoked regardless of whether the caller is running in a cross-memory environment (although they would only be applicable to the primary address space).

The IARQDUMP callable service can be used to determine whether there is some virtual storage backing a given page and is documented in *z/OS MVS Programming: Authorized Assembler Services Guide*.

If neither of these approaches are feasible, perhaps due to concerns about performance, the following new callable services provide the same results as the TPROT instruction while also taking freemained frames into account:

- IARBRVER takes in general purpose register (GPR) 1 the virtual address of the page and returns one of the following codes in GPR 15:

Code Meaning

- 0 Caller has write access to the data.
- 1 Caller has Read-only access (no write access) to the data.
- 2 Caller has neither read nor write access to the data.
- 3 The page either cannot be translated or is backed by a freemained frame.

- IARBRVEA is similar to IARBRVER except that it is invoked in AR mode and access register (AR) 1 contains the ALET associated with the virtual address to be tested. This entry should be used when the page to be tested does not reside in the primary address space.

These services are available when the value of RceOA46291Applied is B'1' and can be invoked on all supported hardware, not just the z13.

Reference information

The documentation updates for APAR OA46291 are described in the file, OA46291.PDF, which is available at: <http://publibz.boulder.ibm.com/zoslib/pdf/OA46291.pdf> .

The following table provides a list of references for various aspects of the freemained frames feature.

Table 61. Reference information for freemained frames

For information about...	See...
User region private storage and the freemained frames feature	<i>z/OS MVS Initialization and Tuning Guide</i>
The FREEMAINEDFRAMES parameter in DIAGxx	<i>z/OS MVS Initialization and Tuning Reference</i>
The IARQDUMP service	<i>z/OS MVS Programming: Authorized Assembler Services Guide</i>
The IARBRVEA and IARBRVER services	<i>z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG</i>
The VSMLOC and VSMLIST services	<i>z/OS MVS Programming: Authorized Assembler Services Reference SET-WTO</i>
The PVT, RAX, and RCE data areas	<i>z/OS MVS Data Areas in the z/OS Internet library</i> (www.ibm.com/systems/z/os/zos/library/bkserv)

Relocate Cross System Extended Services (XES) component trace buffers Description

In z/OS V2R2, the Cross System Extended Services (XES) buffers for component tracing are moved from a common area data space (CADS) to a 4 GB memory object in 64-bit common high virtual (HVCOMMON) storage. During system initialization, XES obtains a 4 GB memory object and manages the virtual storage for global and connection CTRACE buffers. This change allows the GLOBAL trace buffer to be increased from 16 MB to 32 MB (fixed), which reduces the possibility of buffer wrapping. It also increases the available address range for connector trace buffers, which decreases the possibility of a connector running without component tracing.

In previous releases, the XES CTRACE buffers resided in a CADS object named IXLTCAD, which limited the buffers to a 2 GB range of addresses. In z/OS V2R2, XES no longer creates the IXLTCAD object.

Notes:

1. The 4 GB memory object is a fixed size area that is obtained by XES; the size cannot be modified.
2. The IXLBCAD object is not affected by this migration action.

Migration actions from z/OS V2R1: BCP

Table 62 provides more details about the migration action. Use this information to plan your changes to the system.

Table 62. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use coupling facilities in your sysplex or have references to the XES CTRACE CADS ('IXLCTCAD') on the DSPNAME parameter of the DUMP and SLIP commands or in automated parse routines.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Eliminating the XES CADS decreases the number of common area data spaces that are created in the system.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Ensure that enough 64-bit common storage (HVCOMMON) storage is allocated by the system, so that the additional 4 GB request by XES does not cause shortages for other components and elements. The amount of 64-bit common storage is controlled by the HVCOMMON parameter in the IEASYSxx parmlib member. Review the value that is specified on the HVCOMMON parameter to determine whether it must be increased. You can use the MVS operator command **D VIRTSTOR,HVCOMMON** to display information about the current use of the HVCOMMON storage on your system.

For example:

```
IAR019I 06.55.51 DISPLAY VIRTSTOR
SOURCE = DEFAULT
TOTAL 64-BIT COMMON = 66G
64-BIT COMMON RANGE = 1982G-2048G
64-BIT COMMON ALLOCATED = 4171M
```

- To accommodate the allocation of a 4 GB XES CTRACE buffer, add 4 gigabytes (4G) to the HVCOMMON value in the IEASYSxx parmlib member.
- Check for references to the IXLCTCAD object, which is no longer created in z/OS V2R2. Specifically, check for references to 'IXLCTCAD' on the DSPNAME parameter of the **DUMP** and **SLIP** commands (that is, DSPNAME=('XCFAS'.IXLCTCAD)) and on any automated parse routines.
- Ensure that SDATA=XESDATA is specified on any **DUMP** or **SLIP** commands where the IXLCTCAD name was removed. This setting causes the XES CTRACE 64-bit common storage to be included in an SVC dump.

Failure to remove the IXLCTCAD references can result in an error message, such as ASA104. This error, however, does not stop the running process.

If XES cannot obtain a 4 GB memory object, message IXL017I is issued. The system continues to process XES requests normally, but SYSXES CTRACE data is not be available in dumps for analysis under IPCS.

Reference information

For more information, see the following references:

- For information about the HVCOMMON system parameter, see *z/OS MVS Initialization and Tuning Reference*.
- For information about CTRACE, see *z/OS MVS Diagnosis: Tools and Service Aids*.

MVS SLIP command change for MODE=HOME

Description

When a **SLIP** command is issued for a PER trap with **MODE=HOME** specified, but without **JOBNAME** and **ASID** specified, the system issues message IEE088D to prompt the operator for a reply (continue or cancel).

The **JOBNAME**, **ASID**, and **MODE** parameters for a **SLIP** command work together to control the cross memory environment for a PER interrupt. Specifying **MODE=HOME** indicates that the SLIP trap matches only when the command is running in the home address space. When **MODE=HOME** is specified, more processing is used to monitor for the correct environment. When **MODE=HOME** is specified with the **JOBNAME** or **ASID** parameter, this monitoring is limited to the specified address spaces.

However, if **MODE=HOME** is specified without **JOBNAME** and **ASID**, the monitoring occurs for every address space on the system, which can impact performance significantly. As a warning, the system issues message IEE088D with either of the following text strings:

```
IEE088D SLIP COMMAND SPECIFIES MODE=HOME WITHOUT JOBNAME AND ASID. SPECIFY 'OK' OR 'CANCEL'
IEE088D SLIP ID=xxxx SPECIFIES MODE=HOME WITHOUT JOBNAME AND ASID. SPECIFY 'OK' OR 'CANCEL'
```

Note: When this capability was introduced in z/OS V2R1 with APAR OA45297 and even after APAR OA45912, you enabled it by specifying the option TRAPS NAME(IeaSlipConfirm) in the DIAGxx parmlib member. However, in z/OS V2R2, this capability is enabled automatically; you no longer need to specify it explicitly. If you do so in z/OS V2R2, the explicit specification is ignored without an error.

Table 63 provides more details about the migration action. Use this information to plan your changes to the system.

Table 63. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use any IEASLPxx parmlib member or program that issues a SLIP command for a PER trap with MODE=HOME specified, but without JOBNAME and ASID specified.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Migration actions from z/OS V2R1: BCP

Steps to take

For any IEASLPxx parmlib member or program that issues a **SLIP** command for a PER trap with **MODE=HOME** specified, but without **JOBNAME** and **ASID** specified, verify your use of **MODE=HOME** to determine whether changes are needed.

Follow these steps:

- If a **SLIP** command includes **MODE=HOME**, ensure that it also includes **JOBNAME** or **ASID**, or both. Or, if you require the SLIP trap to be set this way, include the **OK** parameter to avoid message IEE088D.
- If you already include the **OK** parameter on the **SLIP** command for another purpose, verify that the **MODE=HOME** parameter is required. Previously, you might have specified the **OK** parameter to avoid receiving the following message:

```
IEE831D SLIP TRAP ID=0001 PER RANGE (00000000_00000000,00000000_01000000)
EXCEEDS 1M OR WRAPS. SPECIFY 'OK' OR 'CANCEL'
```

For example, if you have a SLIP trap that is defined as follows, verify that **MODE=HOME** is required:

```
SLIP SET,IF,RA=(0,1000000),MODE=HOME,OK,END
```

Reference information

For more information, see the following references:

- For the SLIP command, see *z/OS MVS System Commands*.
- For the IEE088D message, see *z/OS MVS System Messages, Vol 7 (IEB-IEE)*.

Define a SAF profile for the log stream subsystem exits

Description

As of APAR OA51174, a log stream subsystem exit routine name is used only when it is one of the IBM-defined names, or the exit name is allowed through a SAF profile. Otherwise, z/OS does not invoke the exit routine name. Instead, z/OS issues message IXG507I and returns a failure indication to the log stream subsystem function (either converter or allocation).

Currently, log stream users can specify a log stream subsystem exit routine name to receive control for reading log data. Users can use either of the following methods to specify the exit routine names:

- On the JCL DDNAME statement, on the keyword SUBSYS=(LOGR,*exit_routine_name*,...)
- On a dynamic allocation request that includes a text unit value for key DALSSPRM (*exit_routine_name*)

With APAR OA51174, this behavior is changed. To continue to specify an exit routine name as described here, your installation must protect the resource IXGLOGR.SUBSYS.LSEXIT.*exit_routine_name*, where *exit_routine_name* identifies the name of the log stream subsystem exit routine.

If your installation uses RACF as its security management product, your security administrator can protect the resource by defining a profile in the FACILITY class. If your installation uses a security management product other than RACF, your security administrator can refer to this topic for reference when creating an equivalent protection in the security management product on your system.

The exception to this requirement is if your installation uses the following IBM-defined names for the exit routines. If so, you have no migration action to perform.

- IXGSEXIT
- IFASEXIT
- IFBSEXIT
- DFHLGCNV

This table provides more details about the migration action. Use this information to plan your changes to the system.

Element or feature:	BCP
---------------------	-----

This table provides more details about the migration action. Use this information to plan your changes to the system.

When change was introduced:	z/OS V2R2, z/OS V2R1, and z/OS V1R13, all with PTFs for APAR OA51174 applied.
Applies to migration from:	z/OS V2R2, z/OS V2R1, and z/OS V1R13, all without PTFs for APAR OA51174 applied.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if both of the following conditions are true: <ul style="list-style-type: none"> Your installation has a log stream subsystem exit routine that is specified through the SUBSYS=(LOGR,...) keyword on a DDNAME JCL statement or on a dynamic allocation request that includes a text unit value for key DALSSPRM Exit routine name is not one of the following IBM-defined names: IXGSEXIT, IFASEXIT, IFBSEXIT, or DFHLGCNV.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Jobs or dynamic allocation requests that specify a log stream exit routine name might fail with an authorization error.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If your installation does not use any log stream subsystem exit routines, or if your installation uses only the IBM-defined names for the log stream subsystem exit routine names, you have no migration action to perform.

Otherwise, if your installation uses or plans to use log stream subsystem exit routine names other than the IBM-defined names, you must perform the following steps:

- Define a discrete profile IXGLOGR.SUBSYS.LSEXIT.*exit_routine_name* for the FACILITY class, where *exit_routine_name* is the name of the log stream subsystem exit routine. Your security administrator can use this profile to audit access failures and grant users READ access. For example:

```
RDEFINE FACILITY IXGLOGR.SUBSYS.LSEXIT.exit_routine_name UACC(READ) AUDIT(FAILURES(READ))
```

- If you need to allow for exit routine names that might not be explicitly known on your system, consider also defining the generic profile IXGLOGR.SUBSYS.LSEXIT.* in the FACILITY class. Include the WARNING attribute in the profile definition (to issue a warning message, but allow access). This profile protects resources that are associated with the log stream subsystem exit routines. For example:

```
RDEFINE FACILITY IXGLOGR.SUBSYS.LSEXIT.* UACC(NONE) WARNING
```

When this generic profile is used to cover the authorization check for the resource IXGLOGR.SUBSYS.LSEXIT.*exit_routine_name*, if the check fails, RACF issues the appropriate warning message to the user, logs the access attempt, and allows the user to access the resource.

Using a generic profile is recommended only as a temporary means for gathering information on the possible exit routine names on your system that require protection. When the exit routine names are identified, you can define the appropriate discrete profiles. After you protect the known exit routine names with discrete profiles, delete the generic profile.

Migration actions from z/OS V2R1: BCP

Note: If you do not define profiles as described here, but instead, define a generic profile that protects the resource IXGLOGR.SUBSYS.LSEXIT.*exit_routine_name*, the generic profile attributes are used to determine the following behaviors:

- Outcome of the authorization checking
- Logging
- Whether the exit routine is invoked.

Reference information

For information about defining RACF profiles in the FACILITY class, see *z/OS Security Server RACF Security Administrator's Guide*.

Update Capacity Provisioning to use Java 7.1 or higher Description

Starting with z/OS V2R2, the Provisioning Manager component of Capacity Provisioning supports Java V7.1. If the references in the ENV member of the Provisioning Manager parameters data set specify the location of an earlier version of Java, you must update the LIBPATH environment variable.

Table 64 provides more details about the migration action. Use this information to plan your changes to the system.

Table 64. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use Capacity Provisioning.
Target system hardware requirements:	IBM 31-bit SDK for z/OS, Java Technology Edition, V7.1 (5655-W43).
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	Levels prior to z/OS V2R2 Capacity Provisioning Manager are not compatible with IBM 31-bit SDK for z/OS V7.1, Java Technology Edition. The support for Java V7.1 is found in z/OS V2R2 Capacity Provisioning Manager. Thus, you cannot use Java V7.1 with pre-z/OS V2R2 Capacity Provisioning Manager levels.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Install IBM 31-bit SDK for z/OS, Java Technology Edition, V7.1 (5655-W43).
- Change the LIBPATH variable in the ENV member of your Provisioning Manager PARM data set to refer to the installation directories of your Java V7 installation. For example:
`LIBPATH=/usr/lpp/cpo/lib:/usr/lib:/usr/lpp/java/a71/J7.1/bin:/usr/`

Reference information

For information about how to adapt the Provisioning Manager parameters, see *z/OS MVS Capacity Provisioning User's Guide*.

Modify the UPDATE statement for the PFA date change

Description

Before z/OS V2R2, Predictive Failure Analysis (PFA) checks had a **DATE** value that reflected the current parameters and values.

Beginning with z/OS V2R2, the **DATE** value in each PFA check changed because new parameters are added to all checks. The existing **UPDATE** statements in HZSPRMxx parmlib members fail unless the **DATE** parameter is set to use ('20140313') or later.

New parameters are added to all PFA checks. If you want to use the new PFA enhancements, or you want to use a value other than the default, you must create an HZSPRMxx parmlib member or modify the existing one.

Table 65 provides more details about this migration action. Use this information to plan your changes to the system.

Table 65. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have updated PFA checks in HZSPRMxx.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Determine whether you are using an HZSPRMxx parmlib member that contains the **UPDATE** statements for one or more PFA checks.
2. If you have an **UPDATE** statement for any PFA check, the **DATE** parameter must be changed to **DATE('20140313')** or later, or the **UPDATE** fails.
3. Determine whether you want to change the value of any of the new parameters. If you want to change the values, add the parameters and new values to the **UPDATE** command.
4. If you do not want to change any of the other parameter values, PFA uses the value that was last set. When a value is never set, PFA uses the default.
5. If you specify WTOTYPE for the PFA_COMMON_STORAGE_USAGE check and want to use the new enhancement for dynamic severity for that check, remove WTOTYPE from the **UPDATE** statement.

For example, the following **UPDATE** statement changes for the PFA_JES_SPOOL_USAGE check changes:

- **DATE** to ('20140313').

Migration actions from z/OS V2R1: BCP

- EXCDIRDAYS to 30 days.
- FORCEMODEL time to 5:00 A.M.
- COLLUPTIME to 3 hours.

```
UPDATE CHECK(IBMPFA,PFA_JES_SPOOL_USAGE)
ACTIVE
SEVERITY(MEDIUM)
INTERVAL(ONETIME)
PARMS=('COLLECTINT(5)', 'MODELINT(720)', 'STDDEV(3)', 'DEBUG(0)', 'COLLECTINACTIVE(1)'
, 'EXCEPTIONMIN(10)', 'EXCDIRDAYS(30)', 'FORCEMODEL(5:00)', 'COLLUPTIME(180)')
DATE(20140313)
REASON('To detect a damaged address space by comparing the amount of
change in the size of the JES spool to the expected value.')
```

Reference information

For more information about PFA, see *z/OS V2R2 Problem Management*.

Review PFA check values

Description

Before z/OS V2R2, Predictive Failure Analysis (PFA) defined the following default values for the checks listed:

- TRACKEDMIN(3) for PFA_SMF_ARRIVAL_RATE and PFA_MESSAGE_ARRIVAL_RATE.
- STDDEVLOW(4) in PFA_ENQUEUE_REQUEST_RATE.

In z/OS V2R2, changes were made to the algorithm that PFA uses, and to the default PFA check values, to work more accurately with the algorithm changes. The changes are intended to accomplish the following goals:

- Increase the accuracy of the PFA checks
- Reduce false positives while still issuing valid exceptions.
- Choose which address spaces to track more accurately.

Table 66 provides more details about this migration action. Use this information to plan your changes to the system.

Table 66. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you are using PFA and not satisfied with the results.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Determine whether you are using a HZSPRMxx parmlib member that contains one or more of the following checks, or if you manually change the parameters for these PFA checks by using the **MODIFY** command supplied by IBM Health Checker for z/OS:
 - PFA_ENQUEUE_REQUEST_RATE
 - PFA_SMF_ARRIVAL_RATE
 - PFA_MESSAGE_ARRIVAL_RATE.
2. If you are changing values for any or all of the checks, determine whether the following parameters are being set for the checks in your HZSPRMxx parmlib member, and if the value set is anything other than the following value:
 - PFA_ENQUEUE_REQUEST_RATE: STDDEVLOW(8)
 - PFA_MESSAGE_ARRIVAL_RATE: TRACKEDMIN(2)
 - PFA_SMF_ARRIVAL_RATE: TRACKEDMIN(2)
3. If yes, remove the change to those values from the HZSPRMxx parmlib member. Do not change them using the **MODIFY** command.
4. Restart PFA to begin by using the new default values.
5. After PFA runs for more than a week, if the current default values are not sufficient for your installation, consider changing them based on the results from that period.

Reference information

For more information about the checks, see *z/OS V2R2 Problem Management*.

Ensure that PFA finds the configuration file

Description

Before z/OS V2R2, Predictive Failure Analysis (PFA) required that you run the install script, AIRSHREP.sh, to create the new directory structure, copy the ini file, and create the default EXCLUDED_JOBS file. Beginning with z/OS V2R2, there is no need to run the install script. Everything previously done by the install script is now done when PFA starts. Also, the only ini file that PFA uses is the /etc/PFA/ini file. The install of PFA requires that any values in the /etc/PFA/ini file are correct.

Table 67 provides more details about this migration action. Use this information to plan your changes to the system.

Table 67. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the /etc/PFA/ini file does not exist or if the values for JAVAPATH , PATH , and LIBPATH are not correct.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Migration actions from z/OS V2R1: BCP

Steps to take

Before you begin, ensure that the PFA user has READ access to the /etc/PFA/ini file. Also, the operator must have proper authority to read or update the files, as needed.

When PFA is started, PFA attempts to use the values in the /etc/PFA/ini file.

Follow these steps:

1. If the /etc/PFA/ini file already exists, PFA uses the existing **JAVAPATH**, **PATH**, and **LIBPATH** that are in the file. Update the values as necessary.
2. If the /etc/PFA/ini file does not exist, PFA attempts to create the /etc/PFA/ini file from an existing check, or it uses the values defined in the /usr/lpp/bcp/samples/PFA/ini file. To ensure that the **JAVAPATH**, **PATH**, and **LIBPATH** values are correct for your installation before PFA starts, copy /usr/lpp/bcp/samples/PFA/ini into /etc/PFA/ini and update the values as necessary.

For example, check the values for the **JAVAPATH**, **PATH**, and **LIBPATH** to be certain they are at the correct level for PFA. In z/OS V2R2, PFA uses a minimum level of Java 7.1 (31-bit) as in the following examples for the **PATH** and **LIBPATH**:

```
PATH= /usr/lpp/java/J7.1/lib/s390/classic:/usr/lpp/java/J7.1/lib/s390
```

```
LIBPATH=/usr/lpp/java/J7.1/lib/s390:/usr/lpp/java/J7.1/lib/s390/classic:/lib:/usr/lib:
```

If the values are not correct, PFA either fails to start or can have processing errors.

Reference information

For information about installing PFA, see *z/OS V2R2 Problem Management*.

Update PFA to use Java 7.1 or higher Description

Before z/OS V2R2, Predictive Failure Analysis (PFA) used a minimum level of IBM 31-bit SDK for z/OS Java Technology Edition version 6.0.0. Beginning with z/OS V2R2, PFA uses a minimum level of IBM 31-bit SDK for z/OS Java Technology Edition version 7.1.0 or later.

Table 68 provides more details about this migration action. Use this information to plan your changes to the system.

Table 68. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you are using PFA.
Target system hardware requirements:	None.
Target system software requirements:	IBM 31-bit SDK for z/OS Java Technology Edition version 7.1.0 or later.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Before you begin, ensure that the PFA user must have READ access to the `/etc/PFA/ini` file. When PFA is started, PFA attempts to use the values in the `/etc/PFA/ini` file.

Follow these steps:

1. If the `/etc/PFA/ini` exists, update the **PATH=** and **LIBPATH=** statements to point to IBM 31-bit SDK for z/OS Java Technology Edition version 7.1.0 or higher.
2. If the `/etc/PFA/ini` file does not exist, copy it from `/usr/lpp/bcp/samples/PFA/ini`. If the path to the JDK for your installation is not the same as the path in the ini file, update it so that both the **PATH=** and **LIBPATH=** statements point to IBM 31-bit SDK for z/OS Java Technology Edition version 7.1.0 or higher.
3. If the `/etc/PFA/ini` file does not exist and you do not copy the sample file, when PFA starts, it attempts to copy the ini file from an existing PFA check directory. If no ini files exists in any of the PFA check directories, PFA copies the sample file that specifies the default path for Java 7.1. If the path to the JDK for your installation is the same as the default, PFA starts. If the path to the JDK for your installation is not the same as the default, PFA issues a message, and then either fails to start or can have processing errors.

The following example is the default **PATH** and **LIBPATH** for PFA:

```
PATH= /usr/lpp/java/J7.1/lib/s390/classic:/usr/lpp/java/J7.1/lib/s390
LIBPATH=/usr/lpp/java/J7.1/lib/s390:/usr/lpp/java/J7.1/lib/s390/classic:/lib:/usr/lib:
```

Reference information

For more information about PFA, see *z/OS V2R2 Problem Management*.

Ensure that the IWM4HLTH service is used properly

Description

As of z/OS V2R2, the minimum authorization requirements for callers of the Workload Management service, IWM4HLTH (setting the server health indicator), are changed. Problem state with any PSW key is sufficient only for setting the health indicator for the home address space of the calling application.

To set the health indicator for another address space, the caller must have at least one of the following authorizations:

- Supervisor state
- Program key mask (PKM) with at least one of the keys 0 - 7
- UPDATE authority to the resource IWM.SERVER.HEALTH in the FACILITY class.

Also, callers of the IWM4HLTH service are recommended to avoid setting the health value to less than 100 for any purposes other than for server health. In z/OS V2R2, a server health value of less than 100 can result in false positives, as follows:

- Runtime Diagnostics creates a diagnostic event for each address space with a server health value less than 100, regardless of the reason. Events that are created for reasons other than server health might be considered as false events by the user of Runtime Diagnostics.
- Predictive Failure Analysis (PFA) issues exceptions for Runtime Diagnostics events that are received for server health values less than 100. PFA exceptions that are issued for these events might be considered as false positive exceptions by the user of PFA.

Table 69 provides more details about this migration action. Use this information to plan your changes to the system.

Table 69. Information about this migration action

Element or feature:	BCP.
---------------------	------

Migration actions from z/OS V2R1: BCP

Table 69. Information about this migration action (continued)

When change was introduced:	z/OS V2R2, z/OS V2R1, and z/OS V1R13, all with APAR OA46280.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA46280.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have <ul style="list-style-type: none">• Unauthorized applications that call this service• Callers that set health values of less than 100 for reasons other than server health
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

To identify unauthorized callers of the IWM4HLTH service who set the health indicator for an address space other than the caller's home address space, you can temporarily define the resource profile IWM.SERVER.HEALTH with the parameter WARNING. After the first IPL of z/OS V2R2, RACF issues the following warning message for callers of the service with insufficient authorization:

```
ICH408I USER(user) IWM.SERVER.HEALTH CL(FACILITY)
WARNING: INSUFFICIENT AUTHORITY - TEMPORARY ACCESS ALLOWED
```

Take one of the following steps for unauthorized callers:

- Change the program so that it no longer calls the IWM4HLTH service or no longer runs the program.
- Change the caller authorization to supervisor state or PKM, with at least one of the keys 0-7.
- Give the user ID associated with the program UPDATE authority to the resource profile IWM.SERVER.HEALTH or an appropriate generic profile when generic profile checking is active.

After the necessary steps are taken, modify the resource profile and specify NOWARNING. Or, if there are no unauthorized callers of the IWM4HLTH service, delete the profile.

Also, ensure that callers of the IWM4HLTH service do not set health values of less than 100 for reasons other than server health.

Reference information

For more information, For more information, see *z/OS MVS Programming: Workload Management Services*.

Identify unauthorized callers of the IWMSRDRS and IWMSRSRG services Description

With z/OS V2R2, the minimum authorization requirements for the callers of Workload Management services IWMSRDRS (Deregister a server for sysplex routing) and IWMSRSRG (Register a server for sysplex routing) are changed.

- Problem state with any PSW key if the server address space to be registered or deregistered is the home address space. If resource BPX.WLMSEVER is defined in the FACILITY class, an unauthorized caller requires access authority to this resource or the IWM.SERVER.REGISTER resource in the FACILITY class.
- If the server to be registered or deregistered is not the home address, one of the following:
 - Supervisor state
 - Program key mask (PKM) allowing at least one of the keys 0-7
 - The caller has at least READ authority to the resource IWM.SERVER.REGISTER in the FACILITY class. If this resource is not defined, READ authority to the FACILITY class resource BPX.WLMSEVER is required.

Table 70 provides more details about this migration action. Use this information to plan your changes to the system.

Table 70. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V2R2, z/OS V2R1, and z/OS V1R13, all with APAR OA46405.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA46405.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have unauthorized applications that invoke one of these services and resource BPX.WLMSEVER in the FACILITY class is not defined.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If RACF resource BPX.WLMSEVER is defined in the FACILITY class, unauthorized callers of WLM services IWMSRDRS and IWMSRSRG already have access authority and no further steps are necessary.

If the resource is not defined, it is recommended that you identify unauthorized callers that use the IWMSRDRS and IWMSRSRG services to register or deregister an address space other than the caller's home address space. To do so, you can temporarily define the IWM.SERVER.REGISTER resource profile with the WARNING parameter. After the first IPL of z/OS V2R2, RACF issues the following warning message for callers of the macro with insufficient authorization:

```
ICH408I USER(user) IWM.SERVER.REGISTER CL(FACILITY)
WARNING: INSUFFICIENT AUTHORITY - TEMPORARY ACCESS ALLOWED
```

For unauthorized callers, take one of the following steps:

- Change the program so that it no longer calls the IWMSRDRS or IWMSRSRG macro or no longer runs the program.
- Change the caller's authorization to supervisor state or PKM allowing at least one of the keys 0-7.
- Give the user ID associated with the program access authority to the resource profile IWM.SERVER.REGISTER or an appropriate generic profile when generic profile checking is active.

Migration actions from z/OS V2R1: BCP

After all necessary steps have been taken, modify the resource profile and specify NOWARNING. Or, delete the resource profile if there are no unauthorized callers of the IWMSRDRS or IWMSRSRG macro.

Reference information

For more information, see *z/OS MVS Programming: Workload Management Services*.

Ensure that authorizations are correct for callers of WLM services

Description

With z/OS V2R2, the minimum authorization requirements for the callers of following Workload Management services are changed:

- IWMDEXTR – Extract WLM service definition
- IWMDINST – Install a service definition
- IWMPACT – Activate service policy.

Resource MVSADMIN.WLM.POLICY in the FACILITY class is mandatory. Callers of IWMDEXTR must have READ access and callers of IWMDINST and IWMPACT must have UPDATE authority. Appropriate access authorities are also required when using the WLM ISPF Application to install or extract a service definition or activate a service policy.

In previous releases, MVSADMIN.WLM.POLICY was optional. If you did not define this resource (or a generic one), any user could invoke IWMDEXTR, IWMDINST, and IWMPACT.

Table 71 provides more details about this migration action. Use this information to plan your changes to the system.

Table 71. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the resource MVSADMIN.WLM.POLICY in the FACILITY class is not already defined.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Define resource MVSADMIN.WLM.POLICY in the FACILITY class. Then, provide read access or update authority to users according to their needs.

Reference information

For more information, see the following references:

- *z/OS MVS Programming: Workload Management Services*
- *z/OS MVS Planning: Workload Management*

BCP actions to perform after the first IPL of z/OS V2R2

This topic describes BCP migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

Plan for the new default format level of HBB7705 in the IXCL1DSU utility Description

Starting in z/OS V2R2, system logger uses a new default NUMBER() value for the SMDUPLEX item when using the XCF couple data set format utility (IXCL1DSU) to format a LOGR CDS.

The SMDUPLEX item NUMBER(1) is now the default value when running the IXCL1DSU utility on a z/OS V2R2 or higher release level and results in a LOGR CDS format level of HBB7705.

The LOGR CDS format level is managed as follows:

HBB7705

Indicates that the LOGR CDS was formatted at one of the following sets of release level ranges and options:

- z/OS V2R2 or later when the ITEM NAME(SMDUPLEX) specification is not provided
- z/OS V1R2 or later with option NUMBER(1) specified for item name SMDUPLEX

HBB6603

Indicates that the LOGR CDS was formatted at one of the following sets of release level ranges and options:

- OS/390 V1R3 or later, through OS/390 V2R10 and z/OS V1R1
- z/OS V1R2 or later, through z/OS V2R1, without option NUMBER(1) for item name SMDUPLEX
- z/OS V1R2 or later with option NUMBER(0) specified for item name SMDUPLEX

HBB5520

Indicates that the LOGR CDS was formatted at a release level before OS/390 V1R3.

Table 72 provides more details about this migration action. Use this information to plan your changes to the system.

Table 72. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you intend on using the IXCL1DSU format couple data set utility on any z/OS V2R2 level systems.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Plan to make use of the default HBB7705 LOGR CDS format level or take steps to format a different LOGR CDS level.

Migration actions from z/OS V2R1: BCP

Reference information

For more information, see the following references:

- For information about using the IXCL1DSU format couple data set utility for system logger, see the "LOGR parameters for format utility" section of *z/OS MVS Setting Up a Sysplex*.
- For considerations on the system logger functions that are supported using the different LOGR CDS format levels, see the "LOGR couple data set versioning - new format levels" section of *z/OS MVS Setting Up a Sysplex*.

Consider the new COUPLExx CFRMTAKEOVERCF(NO) default

Description

z/OS V2R2 introduces a new COUPLExx parmlib member keyword: CFRMTAKEOVERCF. Specifying CFRMTAKEOVERCF(NO) enables CF gain ownership processing enhancements that might prevent a sysplex outage by avoiding operator errors. CFRMTAKEOVERCF(NO) is also the default for z/OS V2R2. To have your z/OS V2R2 system to prompt the operator as it did in prior releases, specify CFRMTAKEOVERCF(PROMPT).

When CFRMOWNEDCFPROMPT(YES) is specified by the COUPLExx parmlib member of a down-level system (prior to z/OS V2R2), the z/OS V2R2 default of CFRMTAKEOVERCF(NO) is not compatible with the configuration.

When CFRMOWNEDCFPROMPT(YES) is used by a down-level system, that system clears the CF authorities saved in the CFRM CDS during CFRM and sysplex initialization (that is, a sysplex-wide IPL). When that occurs, an up-level system (z/OS V2R2) rejects the use of any CF that has a non-zero authority. However, CFRMTAKEOVERCF(NO) is not intended to reject the use of the CF when the old CF authority in the CFRM CDS matches the CF authority in the CF. If a down-level system is no longer in the sysplex, no system will perform the desired prompting.

When CFRMOWNEDCFPROMPT(NO) is specified (or defaulted) by the COUPLExx parmlib member of a down-level system, the z/OS V2R2 default of CFRMTAKEOVERCF(NO) is compatible with the configuration.

Table 73 provides more details about the migration action. Use this information to plan your changes to the system.

Table 73. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you are currently using CFRMOWNEDCFPROMPT(YES) or if, for some reason, the new behavior of CFRMTAKEOVERCF(NO) is not desirable.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you specify CFRMOWNEDCFPROMPT(YES) in the COUPLExx parmlib member, follow these steps:

- Create a COUPLExx parmlib member for z/OS V2R2 systems with CFRMOWNEDCFPROMPT(YES) CFRMTAKEOVERCF(PROMPT) to obtain the old default behavior. After all of the systems are on z/OS V2R2, the COUPLExx parmlib member can be changed to CFRMOWNEDCFPROMPT(YES) CFRMTAKEOVERCF(NO) if the enhanced CF gain ownership processing of CFRMTAKEOVERCF(NO) is desired.
- To have your z/OS V2R2 system prompt the operator as it did in prior releases:
 - Copy the existing COUPLExx parmlib member into a new COUPLExx parmlib member.
 - Add the new CFRMTAKEOVERCF(PROMPT) statement after the COUPLE statement in the new COUPLExx parmlib member.
 - Ensure that the new COUPLExx parmlib member is used when you IPL z/OS V2R2.

If you specify or default to CFRMOWNEDCFPROMPT(NO), you have no migration action to perform.

Reference information

For more information, see the following reference:

- For the COUPLExx (cross-system coupling facility (XCF)) parmlib parameters, see *z/OS MVS Initialization and Tuning Reference*.

Evaluate the stand-alone dump default for large memory objects

Description

Before APAR OA47439, large memory objects were included in stand-alone dumps, which contributed to longer stand-alone dump times. With the PTF for APAR OA47439 applied, this default behavior is changed to improve stand-alone dump processing time.

As part of this support, a new keyword, `SADMP=DEFAULT|YES|NO`, is added to the IARV64 macro. This keyword is used to specify whether a memory object is to be included in a stand-alone dump by default.

The SADMP keyword is added to the IARV64 macro for the following options:

- IARV64 REQUEST=GETSTOR
- IARV64 REQUEST=GETCOMMON
- IARV64 REQUEST=GETSHARED

SADMP=NO is the default when PAGEFRAMESIZE=2G is specified on the IARV64 REQUEST=GETSTOR macro invocation. Previously, the default behavior was equivalent to specifying SADMP=YES. The new default behavior can help to reduce stand-alone dump capture times by avoiding the inclusion of large memory objects and their associated real storage in the dump. To have this type of memory object included in a stand-alone dump, you must allow it explicitly by specifying SADMP=YES.

Table 74 provides more details about the migration action. Use this information to plan your changes to the system.

Table 74. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2, and z/OS V2R1 with APAR OA47439 applied.
Applies to migration from:	z/OS V2R1 (without APAR OA47439 applied) and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.

Migration actions from z/OS V2R1: BCP

Table 74. Information about this migration action (continued)

Is the migration action required?	Yes, if you want to continue capturing memory objects that are backed by 2G frames in stand-alone dumps.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	By default, not including memory objects in stand-alone dumps is expected to result in faster stand-alone dumps. If memory objects are included in stand-alone dumps, you can expect lengthened stand-alone dump times. The performance of stand-alone dump might be noticeably lengthened for z/OS systems that have a large amount of real memory (1 TB or greater) when memory objects are included.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Check for the IARV64 REQUEST=GETSTOR macro invocation with the PAGEFRAMESIZE=2G option specified.
2. For memory objects that should not be included in a stand-alone dump, add SADMP=NO to the macro invocation (or accept the default).
3. Otherwise, for memory objects that contain data that should be captured in a stand-alone dump, add SADMP=YES to the IARV64 REQUEST=GETSTOR macro invocation, if PAGEFRAMESIZE=2G is specified.

Note: SADMP APAR OA44443 for z/OS V2R2 and V2R1 introduces the SADMPNO keyword, which can be used to capture memory objects that are created with the SADMP=NO attribute in specified address spaces.

Reference information

For information about creating large memory objects with the IARV64 macro, see *z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG*.

BookManager BUILD migration actions

This topic describes migration actions for optional feature BookManager BUILD.

BookManager BUILD actions to perform before installing z/OS V2R2

This topic describes BookManager BUILD migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Accommodate the removal of BookManager BUILD Description

z/OS V2R1 is the last release that supported the optional feature BookManager BUILD of z/OS. As of z/OS V2R2, this optional feature has been removed.

Table 75 provides more details about this migration action. Use this information to plan your changes to the system.

Table 75. Information about this migration action

Element or feature:	BookManager BUILD
When change was introduced:	z/OS V2R1
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use the optional feature BookManager BUILD.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Remove any usage of BookManager BUILD. Note that the z/OS base element BookManager READ is still available for reading existing BookManager books.

Reference information

None.

BookManager BUILD actions to perform before the first IPL of z/OS V2R2

This topic describes BookManager BUILD migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

None.

BookManager BUILD actions to perform after the first IPL of z/OS V2R2

This topic describes BookManager BUILD migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

CIM migration actions

This topic describes migration actions for the base element Common Information Model (CIM).

CIM actions to perform before installing z/OS V2R2

This topic describes CIM migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Migration actions from z/OS V2R1: CIM

Prepare for the removal of the CIM Java Managed Provider Interface (JMPI)

Description

z/OS V2R2 is planned to be the last release to support the Java Managed Provider Interface (JMPI) in Common Information Model (CIM). If your installation is using JMPI, IBM recommends that you migrate to a supported provider interface, such as the Common Manageability Programming Interface (CMPI).

Table 76 provides more details about this migration action. Use this information to plan your changes to the system.

Table 76. Information about this migration action

Element or feature:	z/OS Common Information Model
When change was introduced:	See IBM United States Software Announcement 215-267 "IBM z/OS Version 2 Release 2—Fueling the new digital enterprise," dated July 28, 2015.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you are using the JMPI function.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Identify any provider that is using the JMPI function, and convert it to use a supported provider interface. Equivalent function is available through the Common Manageability Programming Interface (CMPI), which is a C language interface. Using the CMPI requires that the CIM provider be written in the C language.

Reference information

For information about CIM providers, see *z/OS Common Information Model User's Guide* .

CIM actions to perform before the first IPL of z/OS V2R2

This topic describes CIM migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

None.

CIM actions to perform after the first IPL of z/OS V2R2

This topic describes CIM migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

Update to SBLIM CIM Client for Java Version 2

Description

z/OS V2R1 is the last release to include Version 1 of the Standards Based Linux Instrumentation for Manageability (SBLIM) CIM client for Java. Version 1 support for the SourceForge open source project was discontinued after 2010. Version 2 of the SBLIM client, which is designed to be a JSR48- compliant implementation, is included in z/OS. Users of SBLIM Version 1 must convert to Version 2.

If you are using SBLIM Version 1, convert to Version 2, which has been included in z/OS since V1R13.

Table 77 provides more details about this migration action. Use this information to plan your changes to the system.

Table 77. Information about this migration action

Element or feature:	z/OS Common Information Model
When change was introduced:	IBM United States Software Announcement 213-013, dated February 5, 2013. The removal occurs in z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you used SBLIM CIM Client for Java Version 1.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Identify any non-IBM application that is using the SBLIM CIM Client for Java Version 1 (**sblimCIMClient.jar**) and contact the owner of the application to convert it to use SBLIM CIM Client for Java Version 2 (**sblim-cim-client2.jar**).

Reference information

For more information about the CIM client for Java, see *z/OS Common Information Model User's Guide* .

Communications Server migration actions

This topic describes migration actions for base element Communications Server.

Communications Server actions to perform before installing z/OS V2R2

This topic describes Communications Server migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Migration actions from z/OS V2R1: Communications Server

IP Services: Replace configuration of TCP/IP legacy device types

Description

Support for the DEVICE and LINK profile statements for the following TCP/IP legacy device types are removed from IBM Communications Server in z/OS V2R2:

- ATM
- CDLC
- CLAW
- HYPERchannel
- SNALINK (LU0 and LU6.2)
- X.25

Because support will be eliminated for the ATM device type, the following associated TCP/IP profile statements will no longer be supported:

- ATMARPSV
- ATMLIS
- ATMPVC
- TRANSLATE NSAP

Because support will be eliminated for the CDLC, SNALINK (both LU0 and LU6.2), and X.25 device types, the following server applications will no longer be supported:

- NCPROUTE
- SNALINK LU0
- SNALINK LU6.2
- X.25 NPSI

Because support will be eliminated for the CLAW and HCH device types, the following TCP/IP profile statement parameters will no longer be supported:

- IPCONFIG CLAWUSEDODUBLENOP and STOPONCLAWERROR
- TRANSLATE HCH

If you are using these legacy device type profile statements, migrate to a later interface type, such as OSA-Express QDIO or HiperSockets.

Note: This only affects device types that are configured to the TCP/IP stack.

As of z/OS V2R2, ZOSMIGV2R1_CS_LEGACYDEVICE migration health check is removed.

Table 78 provides more details about this migration action. Use this information to plan your changes to the system.

Table 78. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R2. This change was also announced in the Statement of direction: IBM zEnterprise System, z/OS, and z/VM enhancements shorten time to value, deliver enhanced security, and improve data access 114-009 February 24, 2014.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you are using any of these legacy device types, you must migrate from these device types to more recent types, such as OSA-Express QDIO and HiperSockets.
Target system hardware requirements:	None.

Table 78. Information about this migration action (continued)

Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	TCP/IP configuration error messages are issued if any of the affected profile statements are configured to the TCP/IP stack.
Related IBM Health Checker for z/OS check:	<p>The ZOSMIGV2R1_CS_LEGACYDEVICE migration health check determines whether you are using any legacy device statements in your TCP/IP profile. This check is available on the following releases:</p> <ul style="list-style-type: none"> • z/OS V1R13 with APARs PI12977 and OA44669 applied. • z/OS V2R1 with APARs PI12981 and OA44671 applied. <p>If any of these device type profile statements are processed, warning message EZZ0717I is issued.</p>

Steps to take

- | If your current configuration includes functions for which support has been eliminated, perform the following steps:
 1. Migrate to a later TCP/IP interface type, such as OSA-Express QDIO or HiperSockets.
 2. Review your TCP/IP IPCONFIG and TRANSLATE profile statements for unsupported parameters.
 3. Verify you are not using the unsupported server applications.
- | You should also remove any customization for the ZOSMIGV2R1_CS_LEGACYDEVICE health check in your IBM Health Checker for z/OS HZSPRMxx parmlib member.

Reference information

For information about configuring OSA-Express QDIO and HiperSockets interfaces, see Considerations for networking hardware attachment in *z/OS Communications Server: IP Configuration Guide*.

IP Services: Replace GATEWAY statements in the TCP/IP profile Description

As of z/OS V2R2, support for the GATEWAY statement in the TCP/IP profile is removed. You must migrate your static route configuration to the equivalent BEGINROUTES statements.

Also, the migration health check ZOSMIGV2R1_CS_GATEWAY is removed in z/OS V2R2.

Table 79 provides more details about this migration action. Use this information to plan your changes to the system.

Table 79. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you have defined static routes by using GATEWAY statements, you must migrate to the BEGINROUTES statements.

Migration actions from z/OS V2R1: Communications Server

Table 79. Information about this migration action (continued)

Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	TCP/IP configuration error messages are issued if a GATEWAY statement is configured to the TCP/IP stack.
Related IBM Health Checker for z/OS check:	ZOSMIGV2R1_CS_GATEWAY can help you determine if you are using any GATEWAY statements in your TCP/IP profile. This check is provided in z/OS V1R13 via VTAM APAR OA43345 and TCP/IP APAR PM96813. If the GATEWAY statement is processed, warning message EZZ0717I is issued.

Steps to take

You must migrate your static route configuration from GATEWAY statements to BEGINROUTES statements.

Follow these steps:

1. Obtain a dump of the TCP/IP stack address space from your z/OS V2R1 or V1R13 system.
2. Use the TCPIP CS PROFILE command against the dump. The command formats all configured static routes as BEGINROUTES profile statements.
3. Use the BEGINROUTES profile statements from the TCPIP CS PROFILE command output to replace the GATEWAY statements in your TCP/IP stack profile.

Remove any customization for the ZOSMIGV2R1_CS_GATEWAY health check in your HZSPRMxx parmlib member.

Reference information

For more information, see the following references:

- For more information about the TCP/IP profile BEGINROUTES statement, see BEGINROUTES statement in *z/OS Communications Server: IP Configuration Reference*.
- For more information on health check customization, see *IBM Health Checker for z/OS User's Guide*

SMTP: Prepare for the removal of SMTPD NJE Mail Gateway and Sendmail Description

z/OS V2R2 is the last release in which the Simple Mail Transport Protocol Network Job Entry (SMTPD NJE) Mail Gateway and Sendmail mail transports are planned to be supported. If you use the SMTPD NJE Gateway to send mail, IBM recommends that you use the CSSMTP SMTP NJE Mail Gateway instead. CSSMTP provides functional and performance improvements, and is designed so that application programming changes are not required.

No replacement functions are planned for the SMTPD or Sendmail listener support; these functions allow for receiving mail for delivery to local TSO/E or z/OS UNIX System Services user mailboxes, or for forwarding mail to other destinations.

Table 80 on page 137 provides more details about this migration action. Use this information to plan your changes to the system.

Table 80. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	24 February 2014 in U.S. Announcement Letter 114-009.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended if you are using the SMTPD NJE Gateway function.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS checks:	<ul style="list-style-type: none"> • ZOSMIGV2R2_Next_CS_SENDMAILDAEMN • ZOSMIGV2R2_Next_CS_SENDMAILCLIEN • ZOSMIGV2R2_Next_CS_SENDMAILMTA • ZOSMIGV2R2_Next_CS_SENDMAILMSA • ZOSMIGV2R2_Next_CS_SMTPDDAEMON • ZOSMIGV2R2_Next_CS_SMTPDMTA

Steps to take

If you are using the SMTPD NJE Gateway, migrate to the existing CSSMTP SMTP NJE Mail Gateway.

Reference information

For more information, see the following references:

- See *Statement of direction: IBM zEnterprise System, z/OS, and z/VM enhancements shorten time to value, deliver enhanced security, and improve data access 114-009 February 24, 2014.*
- For information about the functions supported by CSSMTP, see the Communications Server SMTP server chapter of *z/OS Communications Server: IP Configuration Reference* and the Mail on z/OS chapter of *z/OS Communications Server: IP Configuration Guide*.

IP Services: Verify that the changed DHGroup default is acceptable Description

In z/OS V2R2, the default value for the DHGroup parameter on the KeyExchangeOffer statement in the IPSec policy is changed from Group1 to Group2. If you have an IPSec policy, determine whether this change effects your policy. If you use the IBM Configuration Assistant for z/OS Communications Server to configure your IPSec policy, an explicit DHGroup value is generated on every KeyExchangeOffer statement. A default value is not used.

Table 81 provides more details about this migration action. Use this information to plan your changes to the system.

Table 81. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R2 and z/OS V2R1, both with APAR PI43832. z/OS V1R13 with APAR PI43833.
Applies to migration from:	z/OS V2R1 without APAR PI43832. z/OS V1R13 without APAR PI43833.

Migration actions from z/OS V2R1: Communications Server

Table 81. Information about this migration action (continued)

Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use an IPSec policy.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS checks:	None.

Steps to take

If your policy is not generated by IBM Configuration Assistant for z/OS Communications Server, search your IPSec policy files for any KeyExchangeOffer statements that do not specify a DHGroup parameter. If you find such a KeyExchangeOffer statement, your policy is effected. If you require the DHGroup value to continue to use the previous default of Group1, update your policy to explicitly set the DHGroup parameter to Group1. If you want to use the new default, you need to coordinate with the owners of each remote IKE peer that is associated with the z/OS policy changes to ensure that the remote peer's policy is compatible with the z/OS changes. If the z/OS policy changes so that it is incompatible with the remote peer's policy, the IKE daemons will no longer be able to successfully negotiate IPSec tunnels.

Note: Diffie-Hellman group 1 is considered a weak algorithm and is not recommended.

Reference information

For more information about the KeyExchangeOffer statement in the IPSec policy, see *z/OS Communications Server: IP Configuration Reference*.

IP Services: Replace configuration of additional z/OS legacy device types

Description

TCP/IP DEVICE and LINK profile statements for the following legacy device types will not be supported in a future release of IBM z/OS Communications Server:

- FDDI and Token Ring (LCS with LINKs FDDI and IBMTR)
- Token Ring (MPCIPA with LINK IPAQTR)
- Ethernet and FDDI (MPCOSA with LINKs OSAENET and OSAFDDI)

If you are currently using these profile statements, migrate to a supported interface type, such as OSA-Express QDIO or HiperSockets. For more information about using OSA-Express QDIO or HiperSockets interfaces, see Considerations for networking hardware attachment in z/OS Communications Server: IP Configuration Guide.

Table 82 provides more details about this migration action. Use this information to plan your changes to the system.

Table 82. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	This change was announced in IBM United States Hardware Announcement 215-267 dated July 28, 2015.
Applies to migration from:	z/OS V1R13 and z/OS V2R1.

Migration actions from z/OS V2R1: Communications Server

Table 82. Information about this migration action (continued)

Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended because these TCP/IP device types will not be supported in a future release of IBM z/OS Communications Server.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	ZOSMIGV2R2_NEXT_CS_LEGACYDEVICE can help you determine whether you are using any legacy device statements in your TCP/IP profile. This check is provided in z/OS V2R1 and V2R2 with TCP/IP APAR PI49962 and SNA APAR OA49071 applied.

Steps to take

Use a supported TCP/IP interface type, such as OSA-Express QDIO or HiperSockets.

Reference information

For information about configuring OSA-Express QDIO and HiperSockets interfaces, see Considerations for networking hardware attachment in *z/OS Communications Server: IP Configuration Guide*.

IP Services: Prepare for the removal of the TFTPDP function

Description

z/OS V2R2 is planned to be the last release to include the Trivial File Transfer Protocol Daemon (TFTPDP) function in z/OS Communications Server. If you are using the TFTPDP function, IBM recommends that you migrate to a supported file transfer protocol, such as FTP.

Table 83 provides more details about this migration action. Use this information to plan your changes to the system.

Table 83. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	See IBM United States Software Announcement 215-267 "IBM z/OS Version 2 Release 2—Fueling the new digital enterprise," dated July 28, 2015.
Applies to migration from:	z/OS V1R13 and z/OS V2R1.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended if you are using the TFTPDP function.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Migration actions from z/OS V2R1: Communications Server

Steps to take

If you are using the TFTP function, IBM recommends that you migrate to a supported file transfer protocol, such as FTP.

Reference information

For information about the trivial file transfer protocol (TFTP) and the TFTP daemon, see *z/OS Communications Server: IP Configuration Reference*.

Communications Server actions to perform before the first IPL of z/OS V2R2

This topic describes Communications Server migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

IP Services: Modify GLOBALCONFIG SMCR PFID definitions Description

In z/OS V2R1 Communications Server, VTAM provided physical function services for IBM 10GbE RoCE Express features used for Shared Memory Communications via Remote Direct Memory Access (SMC-R) processing. This allowed multiple TCP/IP stacks operating in the same logical partition (LPAR) to share a RoCE Express feature by configuring and activating the same Peripheral Component Interconnect Express (PCIe) function ID (PFID) representation of the feature. Starting with z/OS V2R2 on a z13 server, each TCP/IP stack must have unique PFID values to represent the RoCE Express feature.

Table 84 provides more details about this migration action. Use this information to plan your changes to the system.

Table 84. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if all the following conditions are true: <ul style="list-style-type: none">• You used Shared Memory Communications – RDMA in z/OS V2R1 Communications Server.• The 10GbE RoCE Express features operated in a dedicated RoCE environment.• You are running on a z13 server.
Target system hardware requirements:	Only applicable to a z13 server. If you are running on a server before z13, this migration action does not apply to you.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Before starting your TCP/IP stacks that activate 10GbE RoCE Express features, perform the following steps:

1. Use the hardware configuration definition (HCD) to define a unique FID value for each TCP/IP stack that will be activating the 10GbE RoCE Express feature. You must also assign a virtual function number (VFN) for each potential user of the 10GbE RoCE Express feature.
2. Modify the GLOBALCONFIG SMCR statement in the TCP/IP profile to specify the PFID values that are assigned for this stack. Update the GLOBALCONFIG statements for all TCP/IP stacks that activate a given 10GbE RoCE Express before starting any of the TCP/IP stacks. The PFID values should correspond to the FID values you defined in the HCD.

Reference information

For more information, see *z/OS Communications Server: IP Configuration Guide*.

IP Services: Make changes for Netstat enhancements

Description

The Netstat command displays the status of a local host. In each release of z/OS, the Netstat reports can change in ways that can affect automation or front-end programs.

Table 85 provides more details about this migration action. Use this information to plan your changes to the system.

Table 85. Information about this migration action

Element or feature:	Communications Server
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the changed or removed settings affect either automation that uses the Netstat report output or front-end programs that invoke the Netstat command.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Accommodate the Netstat changes in your automation and front-end programs. You can begin by reviewing the ways in which the displays are updated in each release. For details about the changes for each Netstat report, see *z/OS Summary of Message and Interface Changes*. However, you must run the commands to know with certainty what changes to make after IPL on a z/OS V2R2 system.

Reference information

For more information, see the following references:

Migration actions from z/OS V2R1: Communications Server

- For information about using the Netstat command, see *z/OS Communications Server: IP System Administrator's Commands*
- For information about the Netstat report changes, see *z/OS Summary of Message and Interface Changes*.

IP Services: Update /etc configuration files

Description

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.

Table 86 provides more details about this migration action. Use this information to plan your changes to the system.

Table 86. Information about this migration action

Element or feature:	Communications Server.
When change was introduced:	Various releases. See Table 87.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have customized a configuration file (listed in Table 87) that IBM has changed.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you added installation-dependent customization to any of the IBM-provided configuration files listed in Table 87, make the same changes in the new versions of the files by copying the IBM-provided samples to the files shown in the table and then customizing the files.

Table 87. Changed Communications Server configuration files

Utility	IBM-provided sample file	Target location	What changed and when
Communications Server z/OS UNIX applications	SEZAINST(SERVICES)	/etc/services	In z/OS V2R2, the NCPROUT entry is removed because NCPROUTE is no longer supported. If you update /etc/services, ensure that you also update the ETC.SERVICES data set.

Migration actions from z/OS V2R1: Communications Server

Table 87. Changed Communications Server configuration files (continued)

Utility	IBM-provided sample file	Target location	What changed and when
DCAS	No sample provided	/etc/dcas.conf	In z/OS V2R2, a new TLSV1ONLY keyword is provided to configure SSLv3 protocol for connections secured using the DCAS SSL support.
File Transfer Protocol Daemon (FTPD)	SEZAINST(FTPDATA)	/etc/ftp.data	In z/OS V2R1, a configuration statement was provided to specify that a type 119 SMF record of subtype 71 is collected for the FTP daemon configuration information when the FTP daemon starts.
FTP Server and Client	SEZAINST(FTCDATA) for the client and (FTPDATA) for the server	/etc/ftp.data	In z/OS V2R2, a new SSLV3 keyword is provided to configure SSLv3 protocol for connections secured using the FTP TLS support.
Internet Key Exchange Daemon(IKED)	/usr/lpp/tcpip/samples/iked.conf	/etc/security/iked.conf	In z/OS V2R2, a new log level is added for the IKE daemon.
Policy agent	/usr/lpp/tcpip/samples/pagent.conf	/etc/pagent.conf	In z/OS V2R2, a new ServerSSLV3 keyword is provided to configure SSLv3 protocol for the policy client connecting to the server.
Sendmail	/usr/lpp/tcpip/samples/sendmail/cf/zOS.cf	/etc/mail/zOS.cf	In z/OS V2R2, a new SSLV3 keyword is provided to configure SSLv3 protocol for connections secured using System SSL.
SNMP agent	/usr/lpp/tcpip/samples/osnmpd.data	/etc/osnmpd.data	Every release, the value of the sysName MIB object is updated to the current release.
SNMP agent	/usr/lpp/tcpip/samples/snmpd.conf	/etc/snmpd.conf	In z/OS V2R2, a new privacy protocol value AESCFB128 can be specified on a USM_USER statement to request AES 128-bit encryption.
z/OS UNIX snmp command	/usr/lpp/tcpip/samples/snmpv2.conf	/etc/osnmp.conf	In z/OS V2R2, a new privacy protocol value AESCFB128 can be specified on a statement for an SNMPv3 user to request AES 128-bit encryption.

Reference information

For more information about Communications Server configuration files, see *z/OS Communications Server: IP Configuration Guide*.

Migration actions from z/OS V2R1: Communications Server

IP Services: Verify z/OS UNIX file permission settings

Description

As of z/OS V2R2, z/OS UNIX file security is enhanced to include additional restrictions for some of the z/OS UNIX files that belong to z/OS Communications Server functions. Table 89 lists the affected z/OS UNIX files. For any existing file that does not comply with the restrictions, take the following steps:

- If the file is not a symbolic link or hard link, delete the file.
- If the file is a symbolic link or hard link, change the incorrect permissions of the file or directory, and the owning information if any.

Table 88 provides more details about this migration action. Use this information to plan your changes to the system.

Table 88. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R1 with APAR PI16886, and z/OS V1R13 with APAR PI17084.
Applies to migration from:	z/OS V2R1 without APAR PI16886, and z/OS V1R13 without APAR PI17084.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if any files you have are affected by the restrictions in Table 89.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Verify whether the z/OS UNIX files in Table 89 comply with the restrictions. To conform with the restrictions, correct any discrepancies that are found.

Table 89. Affected z/OS UNIX files.

Function	File name	Restrictions
DCAS	/tmp/dcas.tcpname_or_INET.pid	1,2,3
IKED	/var/ike/iked.pid	1,2,3
Network SLAPM2 subagent	/tmp/nslapm2.tcpname.pid	1,2,3
Policy Agent	<ul style="list-style-type: none">• /tmp/tcpname.Pagent.tmp• /tmp/pagent.pid	1,2,3
Popper	user bulletin and maildrop files in directory /usr/mail	1,2
RSVP	/tmp/rsvpd.pid.imagename	1,2,3
SNTP	/etc/sntpd.pid	1,2,3
Syslog	<ul style="list-style-type: none">• /etc/syslog.pid• /etc/syslog_net.pid	1,2,3

Migration actions from z/OS V2R1: Communications Server

Table 89. Affected z/OS UNIX files (continued).

Function	File name	Restrictions
TCP/IP stack	/tmp/tcpname.Pagent.tmp	1,2

Restrictions:

1. If the file is a symbolic link, it must have an owning UID or GID that matches the EUID or EGID that is assigned to the listed function.
2. If the file is a hard link or the target of a hard link, users that are outside the owner or group of the directory in which the file is stored cannot have write access to the directory.
3. Additionally, write access to the file must be limited to the owning UID or group, for example, `--w--w----` permissions.

Reference information

None.

IP Services: Enable SSLv3 for z/OS components if required

Description

In z/OS V2R2, Communications Server changed its default protocol support for components that use SSL/TLS natively or through AT-TLS. SSLv3 is now disabled by default, which can affect the usage of AT-TLS, the FTP client and server, the TN3270 server, the DCAS server, Policy Agent, and sendmail. For any exploiters (installations and applications) that must continue to use SSLv3, you can explicitly enable this protocol.

Table 90 provides more details about this migration action. Use this information to plan your changes to the system.

Table 90. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R1 with APAR PI28679, and z/OS V1R13 with APAR PI28678.
Applies to migration from:	z/OS V2R1 without APAR PI28679 and z/OS V1R13 without APAR PI28678.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have applications that use SSLv3.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Review each of the Communications Server components that follow to determine whether you are affected. Make changes as directed. For applications that are protected by AT-TLS and that require SSLV3, evaluate their usage and change them to use TLS protocols, if possible. TLS addresses many security deficiencies that exist in the prior SSLv2 and SSLv3 protocols. For applications that must continue to use SSLv3, you can explicitly enable this protocol, as described in the sections that follow.

Migration actions from z/OS V2R1: Communications Server

AT-TLS

AT-TLS is modified to disable SSLv3 by default. Any applications that are protected by AT-TLS default to SSLv3 Off.

If SSLv3 is explicitly enabled in your policy, no action is required. However, it is recommended that you evaluate whether applications can be updated to use a more secure protocol version, such as TLSv1, TLSv1.1, or TLSv1.2.

Applications that require SSLv3, and for which this protocol is not explicitly enabled in the policy, rely on AT-TLS defaults. For these applications, you can enable SSLv3 at the environment or connection level by specifying the parameter SSLv3 on the relevant TTLSEnvironmentAdvancedParms or TLSConnectionAdvancedParms policy statement with a value of ON. For Configuration Assistant users, you can enable SSLv3 in the **name** tab of the Modify Security Level dialog under the AT-TLS perspective.

FTP client and server

The FTP client and FTP server are modified to disable SSLv3 by default when TLSMECHANISM FTP is specified. In this mode, the FTP client or server uses System SSL APIs natively for SSL/TLS protection, rather than AT-TLS.

Because the z/OS FTP client and server enabled SSLv3 by default, evaluate whether either of the following conditions are true:

- Your server is supporting clients that require SSLv3
- Your client is connecting to a server that requires SSLv3

If so, you can enable SSLv3 by specifying the new parameter SSLV3 in the relevant FTP configuration data set FTP.DATA with a value of TRUE.

If TLSMECHANISM ATTLS is specified, the FTP client or server is protected by AT-TLS; the changes that are described for the AT-TLS function apply.

TN3270 server

The TN3270 server is modified to disable SSLv3 by default when SECUREPORT is specified. In this mode, the TN3270 server uses System SSL APIs natively for SSL/TLS protection, rather than AT-TLS.

Because the TN3270 server enabled SSLv3 by default, determine whether your server is supporting clients that require SSLv3. If so, you can enable SSLv3 by specifying the new statement SSLV3 in the relevant TN3270 profile data set and refreshing the configuration by using the command **VARY TCPIP, tnproc, OBEYFILE**.

If TTLSPORT is specified, the TN3270 server is protected by AT-TLS; the changes that are described for the AT-TLS function apply.

DCAS server

The DCAS server is modified to disable SSLv2 and SSLv3 by default when TLSMECHANISM DCAS is specified. In this mode, the DCAS server uses System SSL APIs natively for its SSL/TLS protection, rather than AT-TLS.

Because the DCAS server enabled SSLv2 and SSLv3 by default, evaluate whether your server is supporting clients that require SSLv2 or SSLv3. If so, you can enable SSLv2 and SSLv3 by specifying the new parameter TLV10ONLY in your DCAS configuration file with a value of FALSE and restarting DCAS.

If TLSMECHANISM ATTLS is specified, the DCAS server is protected by AT-TLS; the changes that are described for the AT-TLS function apply.

Policy Agent

The Policy agent, when it operates as a policy client, is modified to disable SSLv3 by default. Because the policy client enabled SSLv3 by default, evaluate whether your policy server supports SSLv3 only. If so, you can enable SSLv3 by specifying the new parameter ServerSSLv3 on the ServerSSL

substatement of the ServerConnection statement with a value of ON in the policy agent main configuration file. Then, update the policy agent configuration by using the command **MODIFY pagent,UPDATE**.

Sendmail

Sendmail, which operates as both a client and server, is modified to disable SSLv3 by default. Because the z/OS sendmail program enabled SSLv3 by default, evaluate whether either of the following conditions is true:

- Your server is supporting clients that require SSLv3
- Your client is connecting to a server that requires SSLv3

If so, you can enable SSLv3 by specifying the parameter SSLV3 in the zOS.cf configuration file with a value of TRUE and restarting sendmail.

Reference information

None.

IP Services: Verify the new default for the QUEUEDRTT parameter

Description

In z/OS V2R2, enhancements were made to the Communications Server outbound serialization function, which is controlled by the QUEUEDRTT parameter on the TCPCONFIG profile statement. The default value for this parameter is changed. Previously, the default setting for QUEUEDRTT was 20, meaning that only TCP/IP connections with a *round-trip time* (RTT) value of 20 milliseconds or more are eligible to use outbound serialization. In z/OS V2R2, the default value for QUEUEDRTT is changed to 0, meaning that all TCP/IP connections are eligible to use outbound serialization.

Table 91 provides more details about this migration action. Use this information to plan your changes to the system.

Table 91. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you do not specify the QUEUEDRTT parameter on the TCPCONFIG profile statement.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	The new default value allows more connections to be eligible for outbound serialization. This performance optimization might result in higher CPU costs at the sending host, but these costs are offset by the CPU savings on the receiving host.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you do not currently specify the QUEUEDRTT parameter on the TCPCONFIG profile statement, but you want to continue using a value of 20 milliseconds as the threshold to enable a TCP/IP connection to

Migration actions from z/OS V2R1: Communications Server

use outbound serialization, you must specify `QUEUEDRTT 20` on the `TCPCONFIG` profile statement.

Reference information

For more information, see the following references:

- See the `QUEUEDRTT` parameter description in `TCPCONFIG` statement in *z/OS Communications Server: IP Configuration Reference*.
- See *Outbound Serialization* in *z/OS Communications Server: IP Configuration Guide*.

IP Services: Use the new maximum segment size adjustments if required

Description

New function is introduced in z/OS V2R2 to automatically adjust the Maximum Segment Size (MSS) that is used on a TCP connection to avoid fragmentation. This function is turned on by default. If you need to continue using your existing setting for the MSS, see “Steps to take.”

Table 92 provides more details about this migration action. Use this information to plan your changes to the system.

Table 92. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you do not want the automatic reduction of MSS.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	A performance degradation can result if the MSS is not configured to avoid fragmentation.
Related IBM Health Checker for z/OS check:	None.

Steps to take

To disable the auto-adjusting function and continue using your existing setting for the MSS from the prior release, specify the subparameter `ADJUSTDVIPAMSS NONE` on the parameter `GLOBALCONFIG`.

Reference information

For more information, see *z/OS Communications Server: IP Configuration Reference*.

IP Services: Check code that automates on IKE daemon syslogd messages

Description

Scalability enhancements in z/OS V2R2 Communications Server introduce a new internal thread pool to the Internet Key Exchange (IKE) daemon. As part of this change, all of the IKED messages that are written through syslogd will contain the thread identifier in the syslogd header, which precedes the message identifier. In addition, messages from different IKED threads might be interleaved. These changes might affect the automation code that parses these IKED messages:

Migration actions from z/OS V2R1: Communications Server

- If the automation code parses individual IKED messages in syslogd destinations based on any sort of position-based logic (for example, counting blanks delimiters, relying on a specific column), you need to update to account for the new thread id field.
- If the automation code parses individual IKED messages based on message content (for example, searching the string for specific message identifiers), no change is needed.
- If the automation code depends on the order of the IKED messages, you might need to update to take the thread id field into account so that the code ignores messages from other threads that are interleaved with the messages of interest.

IKED messages are those in the ranges EZD0902I - EZD1160I, EZD1751I - EZD1800I, and EZD1901I - EZD1925I as well as EZD2017I, EZD2019I, EZD2025I and EZD2027I.

The following example shows a small excerpt of messages from z/OS V2R1 and the equivalent messages from z/OS V2R2 with the imbedded thread identifiers:

V2R1:

```
Jul 28 11:39:26 mvs046 IKE: EZD1061I IKE connecting to PAGENT
Jul 28 11:39:26 mvs046 IKE: EZD1062A IKE retrying connection to PAGENT
Jul 28 11:39:34 mvs046 IKE: EZD0923I IKE has received the STOP command
Jul 28 11:39:34 mvs046 IKE: Message instance 0: EZD0967I IKE release
CS V2R1 Service Level CS130924 Created on Sep 24 2013
Jul 28 11:39:34 mvs046 IKE: Message instance 14: EZD1116I IKE detected
an NAPT in front of the remote security endpoint while initiating a new
phase 1 tunnel
```

V2R2:

```
Jul 28 15:10:47 mvs046 IKE: (00000001) EZD1061I IKE connecting to PAGENT
Jul 28 15:10:47 mvs046 IKE: (00000001) EZD1062A IKE retrying connection
to PAGENT
Jul 28 15:11:06 mvs046 IKE: (00000003) EZD0923I IKE has received the STOP command
Jul 28 15:11:06 mvs046 IKE: Message instance 0: (00000001) EZD0967I IKE release
CS V2R2 Service Level CS140728 Created on Jul 28 2014
Jul 28 15:11:06 mvs046 IKE: Message instance 14: (00000007) EZD1116I IKE detected
an NAPT in front of the remote security endpoint while initiating a new
phase 1 tunnel
```

Table 93 provides more details about this migration action. Use this information to plan your changes to the system.

Table 93. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use the z/OS IKE daemon and you have code that automates on IKED messages written through syslogd.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Migration actions from z/OS V2R1: Communications Server

Steps to take

Change the code that automates on IKED messages written through syslogd to account for the thread identifier that is added to the header area preceding the IKED message number.

Reference information

None.

IP Services: Decide whether to accept the new FIXED CSM default Description

In z/OS V2R2, the default amount for communications storage manager (CSM) fixed storage for buffers is increased from 100 MB to 200 MB. Your installation can specify a value for the CSM fixed storage amount on the FIXED statement in the IVTPRM00 parmlib member.

Table 94 provides more details about this migration action. Use this information to plan your changes to the system.

Table 94. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use the default CSM FIXED MAX value of 100M and you do not want to use the new default of 200M.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you did not previously code a value for FIXED in IVTPRM00 and you do not want the new default, specify FIXED MAX(100M) 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.

Reference information

For information about the IVTPRM00 parmlib member, see the IVTPRM00 parmlib member in *z/OS Communications Server: New Function Summary*.

SNA Services: Update TIBUF pool size and T1BUF pool size Description

z/OS V2R2 reduces the number of buffers per page of storage for the following buffer pools:

TIBUF pool bufsize change

The TIBUF pool contains control information to support HPDT services for HPR or IP. It is used to contain the HPR headers and the media, IP, and UDP headers for an Enterprise Extender connection. It is also used to contain data for APPC conversations.

T1BUF pool bufsize change

The T1BUF pool contains control information to support HPDT services for HPR or IP. It is similar to the TIBUF pool, but larger. It is used as a packing buffer by HiperSockets accelerator and QDIO. It is also used to contain the HPR headers and the media, IP, and UDP headers for an Enterprise Extender connection.

Table 95 provides more details about this migration action. Use this information to plan your changes to the system.

Table 95. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have modified the buffer pool values for the TIBUF pool or the T1BUF pool, and you might want to revisit your settings.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Enterprise Extender performance degradation can result from poorly tuned buffers.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you have tuned your systems to require a specific number of pages of TIBUF or T1BUF buffer storage, you might need to recalculate the number of pages required. For information, see *Tuning Enterprise Extender specific buffer pools in z/OS Communications Server: SNA Network Implementation Guide*.

Reference information

For information about how to adjust the value, see *Tuning Enterprise Extender specific buffer pools in z/OS Communications Server: SNA Network Implementation Guide*.

For more information, see the following references:

- *z/OS Communications Server: SNA Resource Definition Reference*
- *z/OS Communications Server: SNA Operation*

Communications Server actions to perform after the first IPL of z/OS V2R2

This topic describes Communications Server migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

Cryptographic Services migration actions

This topic describes migration actions for base element Cryptographic Services. Included are the components Integrated Cryptographic Service Facility (ICSF), Open Cryptographic Services Facility (OCSF), PKI Services, and System Secure Sockets Layer (SSL).

Cryptographic Services actions to perform before installing z/OS V2R2

This topic describes Cryptographic Services migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

ICSF: Detect any coprocessor that will not become active when HCR77A1 or later is started

Description

For ICSF FMIDS HCR7780, HCR7790, and HCR77A0, the activation procedure was designed to maximize the number of active coprocessors by selecting the set of master keys that are available on the majority of coprocessors. A DES master key is no longer required in order for a coprocessor to become active. Instead, any one of four master keys – the DES master key, the AES master key, the RSA master key (which in earlier releases was called the asymmetric master key), or the ECC master key – is enough for a coprocessor to become active. However, because the goal is to select the combination of master keys that will maximize the number of active coprocessors, if a certain master key is not set on all the same coprocessors, that master key support will not be available.

Starting with FMID HCR77A1, the activation procedure now uses the master key verification patterns (MKVP) in the header record of the CKDS and PKDS to determine which coprocessors become active. If the MKVP of a master key is in the CKDS or PKDS, that master key must be loaded and the verification pattern of the current master key register must match the MKVP in the CKDS or PKDS. If all of the MKVPs in the CKDS and PKDS match the current master key registers, the coprocessor will become active. Otherwise, the status is master keys incorrect. This applies to all master keys that the coprocessor supports. When there is a MKVP in the CKDS or PKDS and the coprocessor does not support that master key, it is ignored. When a MKVP is not in the CKDS or PKDS, the master key is ignored.

If there are no MKVPs in the CKDS and PKDS, the coprocessor will be active. If the CKDS is initialized without any MKVPs, the CKDS cannot be used on a system that has cryptographic features installed.

Table 96 provides more details about this migration action. Use this information to plan your changes to the system.

Table 96. Information about this migration action

Element or feature:	Cryptographic Services
When change was introduced:	Cryptographic Support for z/OS V1R13 - z/OS V2R1 web deliverable (FMID HCR77A1), which installs on z/OS V1R13 or z/OS V2R1.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without the Cryptographic Support for z/OS V1R13 - z/OS V2R1 web deliverable (FMID HCR77A1) or a later ICSF web deliverable installed.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you are affected by the change in the way master keys are processed to determine which coprocessors become active.
Target system hardware requirements:	None.
Target system software requirements:	None.

Migration actions from z/OS V2R1: Cryptographic Services

Table 96. Information about this migration action (continued)

Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	Use check ICSFMIG77A1_COPROCESSOR_ACTIVE to determine which coprocessors will not become active when Cryptographic Support for z/OS V1R13 - z/OS V2R1 Web Deliverable (FMID HCR77A1) is started. This check is delivered in APAR OA42011 available for ICSF FMIDs HCR7770, HCR7780, HCR7790 and HCR77A0.

Steps to take

Run the migration check ICSFMIG77A1_COPROCESSOR_ACTIVE to find any coprocessors that will not become active when you start HCR77A1 or a later ICSF web deliverable.

Reference information

For more information, see the following references:

- See the chapter on migration in *z/OS Cryptographic Services ICSF System Programmer's Guide*
- For information about IBM Health Checker, see *IBM Health Checker for z/OS User's Guide*.

ICSF: Detect TKDS objects that are too large for the new record format in HCR77A1

Description

In ICSF FMID HCR77A1, ICSF is introducing a common key data set record format for CCA key tokens and PKCS #11 tokens and objects. This new record format adds new fields for key utilization and metadata. Because of the size of the new fields, some existing PKCS #11 objects in the TKDS might cause ICSF to fail. If you do not have a Token Data Set (TKDS) with PKDS #11 objects in it, there is no need to run this check.

The problem exists for TKDS object records with large objects. The User data field in the existing record will cause the TKDS not be to loaded if the object size is greater than 32,520 bytes. The TKDSREC_LEN field in the record has the size of the object. If the User data field is not empty and the size of the object is greater than 32,520 bytes, the TKDS cannot be loaded.

Note that ICSF does not provide any interface to modify the User data field in the TKDS object record. A field can be created using IDCAMS. Check the contents of the User data field and determine if the information in the field is valuable. If you want to preserve the data, consider how the information can be stored other than in the object record. The field can only be modified by editing the record. For information about the TKDS object record, see *z/OS Cryptographic Services ICSF System Programmer's Guide*. The IBM Health Checker migration check, ICSFMIG77A1_TKDS_OBJECT detects any TKDS object that is too large to allow the TKDS is read into storage during ICSF initialization starting with ICSF FMID HCR77A1. This migration check is available for HCR7770, HR7780, HCR7790, and HCR77A0 through APAR OA42011

Table 97 provides more details about this migration action. Use this information to plan your changes to the system.

Table 97. Information about this migration action

Element or feature:	Cryptographic Services
---------------------	------------------------

Migration actions from z/OS V2R1: Cryptographic Services

Table 97. Information about this migration action (continued)

When change was introduced:	Cryptographic Support for z/OS V1R13 – z/OS V2R1 web deliverable (FMID HCR77A1), which installs on z/OS V1R12, z/OS V1R13 or z/OS V2R1.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without the Cryptographic Support for z/OS V1R13 - z/OS V2R1 web deliverable (FMID HCR77A1) installed.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you affected by the record format changes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	Use the IBM Health Checker migration check ICSFMIG77A1_TKDS_OBJECT to detect any TKDS object with a value in the User data field that is too large to preserve in the User data field of the new format record. This migration check is available for HCR7770, HR7780, HCR7790, and HCR77A0 through APAR OA42011.

Steps to take

Run the migration check ICSFMIG77A1_TKDS_OBJECT to detect if TKDS objects are too large for the new record format in HCR77A1.

Note: ICSF does not provide any interface to modify the User data field in the TKDS object record. A flat file can be created using IDCAMS. Check the contents of the User data field and determine if the information in the field is valuable. If you want to preserve the data, consider how the information can be stored other than in the object record. The field can only be modified by editing the record. For information about the TKDS object record, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.

Reference information

For more information, see the following references:

- For information about TKDS, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.
- For information about IBM Health Checker, see *IBM Health Checker for z/OS User's Guide*.

Cryptographic Services actions to perform before the first IPL of z/OS V2R2

This topic describes Cryptographic Services migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

ICSF: Determine if applications using hash services have archived hashes of long data

Description

Due to service introduced by APAR OA43937, new Hash Method Rule keywords for the ICSF One-Way Hash Generate (CSNBOWH or CSNBOWH1 and CSNEOWH or CSNEOWH1) and PKCS11 One-Way

Migration actions from z/OS V2R1: Cryptographic Services

Hash Services (CSFPOWH and CSFPOWH6) will support generation of legacy hash values for verification of archived hash values generated from pre-OA43937 releases of HCR7770 and higher.

Note: This correction of hashing function does not apply to the case where the sum of the length of hashed text over a series of chained calls exceeds 256 megabytes (or 512, as described further in this topic), but no single invocation supplies an input *text_length* that exceeds 256 (or 512) megabytes. Correct hashes are created when no single invocation of the callable services exceeds the described limit prior to (and after) application of the PTFs for OA43937.

Applications that wish to verify archived hash values created by pre-OA43937 HCR7770 and higher releases of ICSF callable services One-Way Hash Generate and PKCS11 One-Way Hash may need to invoke these callable services with new rule array keywords that support the creation of legacy hash values. The hash generated using the new rule array keywords must be used to verify the archived hash values.

The ICSF Callable Services One-Way Hash Generate and PKCS11 One-Way Hash, sign, or verify have corrected the way they create hash values when the length of the text on a single invocation of one of these services supplies an input *text_length* that equals or exceeds 256 megabytes (512 megabytes on z990/z890 or later hardware on HCR7770). The hashing services are corrected with the application of the PTFs for OA43937.

Table 98 provides more details about this migration action. Use this information to plan your changes to the system.

Table 98. Information about this migration action

Element or feature:	Cryptographic Services.
When change was introduced:	PTFs for OA43937, which are applicable to: ICSF FMIDs HCR7770 - HCR77A1 (z/OS V1R12 - z/OS V2R1).
Applies to migration from:	ICSF FMIDs HCR7770 - HCR77A1, without the PTF for OA43937.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have archived hash values created before the installation of the PTFs for OA43937 which meet the length restrictions described here.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	If you do not use the legacy rule array keywords for affected applications, then the application may fail to verify the legacy hashes/signatures.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Identify if your application needs to verify archived hash values created by either of the ICSF callable service One-Way Hash Generate (CSNBOWH or CSNBOWH1 and CSNEOWH or CSNEOWH1) or PKCS11 One-Way Hash (CSFPOWH and CSFPOWH6) on releases pre-OA43937 at HCR7770 and higher. (See the ICSF Application Programmer's Guide documentation changes in this APAR for new ICSF callable service keywords that support the creation of hashes for the verification of archived hash values and the input text length requirements.)

Migration actions from z/OS V2R1: Cryptographic Services

2. If your application has these archived hash values and intends to verify them, then invocations of ICSF callable services One-Way Hash Generate, PKCS11 One-Way Hash, sign, or verify that create hashes for verification of the archived hash values may need to be updated to use the new legacy rule array keywords (ONLY if those archived hash values were created with input text length exceeding the limits described).

Reference information

For more information, see *z/OS Cryptographic Services ICSF Application Programmer's Guide* .

ICSF: Deprecated parameters in installation options data set

Description

The ICSF installation options data set parameters COMPENC and PKDSCACHE were deprecated in FMID HCR7751 and parameters CKTAUTH, KEYAUTH, and TRACEENTRY were deprecated in FMID HCR77A1.

Table 99 provides more details about this migration action. Use this information to plan your changes to the system.

Table 99. Information about this migration action

Element or feature:	Cryptographic Services.
When change was introduced:	ICSF FMIDs HCR7751 and HCR77A1.
Applies to migration from:	All ICSF FMIDs before FMID HCR77B0.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Edit the ICSF installation options data set and remove all of the deprecated parameters.

Note: ICSF starts with the deprecated parameters in the ICSF installation options data set, but the parameters are ignored and message CSFO0212 is issued for each deprecated parameter.

Reference information

For more information, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.

OCSF: Migrate the directory structure

Description

If you previously configured Open Cryptographic Services Facility (OCSF), you need to verify that the OCSF directories have been migrated to the target system. When your system is up and running, customize OCSF by running the customization script and then the IVP.

Migration actions from z/OS V2R1: Cryptographic Services

Note: If you want to take advantage of the Software Cryptographic Service Provider 2 (SWCSP2), you should bypass this migration action. When your system is up and running, install OCSF by running the install script and then the IVP.

Table 100 provides more details about this migration action. Use this information to plan your changes to the system.

Table 100. Information about this migration action

Element or feature:	Cryptographic Services.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you currently use OCSF or if new products or functions on your new z/OS system require OCSF to be active. However, if you installed your new z/OS system with ServerPac or SystemPac, the OCSF installation script has been run and you do not have to perform this migration action for that system.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Migrate the OCSF /var directory structure to the target system. If you installed z/OS with CBPDO or by cloning an already-installed z/OS system, you can either copy the /var/ocsf directory from your old system or rerun the installation script. If you installed z/OS with ServerPac, the OCSF installation script has been run and you have no migration actions for that target system (although you still have to migrate the directory structure to any cloned systems, as already described).

If you installed z/OS V1R13 with CBPDO or by cloning an already-installed V1R13 system, you can either copy the /var/ocsf directory from your old system or rerun the installation script. If you installed z/OS V1R13 with ServerPac or SystemPac, the OCSF installation script has been run and you have no migration actions for that target system (although you still have to migrate the directory structure to any cloned systems, as already described).

If you copy /var/ocsf, verify that the OCSF /var directory structure has been migrated to the target system as described in “Migrate /etc and /var system control files” on page 16. The OCSF registry (the /var/ocsf files) contains the directory path names to the code libraries. If the registry files are copied, the CSSM DLL and the add-ins must be in the same location on the target system as on the prior release. The normal locations are /usr/lpp/ocsf/lib for the CSSM and supporting DLLs and /usr/lpp/ocsf/addins for the add-in libraries.

If you copied /var/ocsf, do the following:

1. Verify that the following four files exist in that directory:
 - CDSA_Registry.dir with permissions (-rw-r--r--)
 - CDSA_Registry.pag with permissions (-rw-r--r--)
 - CDSA_Sections.dir with permissions (-rw-r--r--)
 - CDSA_Sections.pag with permissions (-rw-r--r--)

Migration actions from z/OS V2R1: Cryptographic Services

2. Verify that the required RACF FACILITY class profiles are defined and set up:
 - CDS.CSSM — authorizes the daemon to call OCSF services
 - CDS.CSSM.CRYPTO — authorizes the daemon to call a cryptographic service provider (CSP)
 - CDS.CSSM.DATALIB — authorizes the daemon to call a data storage library (DL) service provider
3. Ensure that the necessary libraries are program controlled:
 - XL C/C++ runtime libraries
 - Language Environment libraries
 - SYS1.LINKLIB
 - SYS1.SIEALNKE

If you did not copy /var/ocsf, rerun the installation script:

1. Set up the RACF FACILITY class profiles required by OCSF and authorize the appropriate user IDs to those profiles:
 - CDS.CSSM — authorizes the daemon to call OCSF services
 - CDS.CSSM.CRYPTO — authorizes the daemon to call a cryptographic service provider (CSP)
 - CDS.CSSM.DATALIB — authorizes the daemon to call a data storage library (DL) service provider
2. Ensure that the following libraries are defined as program controlled:
 - XL C/C++ runtime libraries
 - Language Environment libraries
 - SYS1.LINKLIB
 - SYS1.SIEALNKE
3. Run the `ocsf_install_crypto` script from the OMVS shell. This must be run from the target system.
 - a. Verify and update \$LIBPATH.
 - b. Change directory to the location of the script (/usr/lpp/ocsf/bin).
 - c. Run the script.

Whether you reinstalled or migrated, it is strongly recommended that you rerun IVP `ocsf_baseivp` from the OMVS shell. This IVP verifies that OCSF is installed and configured correctly. To run the IVP:

1. Mount /usr/lpp/ocsf/ivp.
2. Read the README file and follow the instructions.
3. Run the IVP.

If you were using other IBM or non-IBM services to supplement the functions in OCSF, such as the Open Cryptographic Enhanced Plug-ins (OCEP) component of base element Integrated Security Services, or the PKI Services component of base element Cryptographic Services, you must ensure that these are migrated or reinstalled.

Reference information

For more information, see *Integrated Security Services Open Cryptographic Enhanced Plug-ins Application Programming*.

System SSL: Modify code or System SSL application configurations to enable SSLV2 or SSLV3

Description

Starting in z/OS V2R2, z/OS System SSL has changed its default protocol support. When a System SSL application calls the `gsk_environment_open()` routine to establish a secure environment, SSL V2 and SSL V3 will now be disabled by default. TLS V1.0 will continue to be enabled by default. For applications that must continue to use these protocols, the protocol must be explicitly enabled.

If SSL V2, SSL V3, or both are the only supported protocols in the application, the following are example SSL errors that may occur when the SSL V2 or SSL V3 protocols are disabled:

- Return code 402: No SSL cipher specifications.
- Return code 412: SSL protocol or certificate type is not supported.

Migration actions from z/OS V2R1: Cryptographic Services

- Return code 429: SSL V2 header is not valid.

For applications that use the SSL V2 or SSL V3 protocol, evaluate the application's usage and change the application to use the TLS protocols if possible. TLS has addressed many security deficiencies in the prior SSL V2 and SSL V3 protocols.

Table 101 provides more details about this migration action. Use this information to plan your changes to the system.

Table 101. Information about this migration action

Element or feature:	Cryptographic Services
When change was introduced:	z/OS V2R2. z/OS V2R1 and z/OS V1R13, both with APAR OA46489.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA46489.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if System SSL applications for secure SSL/TLS connections are used.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If your installation utilizes System SSL applications for secure SSL/TLS connections, examine those applications to determine if they require either the SSL V2 or SSL V3 protocols to be enabled.

z/OS System SSL provides two methods for controlling the SSL/TLS protocols supported when negotiating a secure connection:

- The first method is the Application Programming Interface (API) **gsk_attribute_set_enum()** routine. This routine allows the enablement of the SSL/TLS protocols at either the SSL/TLS environment or connection level. To enable the usage of SSL V2, enumeration parameter GSK_PROTOCOL_SSLV2 must be set to GSK_PROTOCOL_SSLV2_ON. To enable the usage of SSL V3, enumeration parameter GSK_PROTOCOL_SSLV3 must be set to GSK_PROTOCOL_SSLV3_ON.
- The second method uses environment variables GSK_PROTOCOL_SSLV3 and GSK_PROTOCOL_SSLV2. To enable the usage of SSL V2, environment variable GSK_PROTOCOL_SSLV2 must be set to ON, 1, or ENABLED. To enable the usage of SSL V3, environment variable GSK_PROTOCOL_SSLV3 must be set to ON, 1, or ENABLED. Note that an environment variable setting is overridden if the application calls the **gsk_attribute_set_enum()** routine to set the GSK_PROTOCOL_SSLV2 and GSK_PROTOCOL_SSLV3 values.

If the protocols are required, consult each application configuration documentation to determine the appropriate enablement capability.

Reference information

For more information about System SSL, see *z/OS Cryptographic Services System SSL Programming*.

Migration actions from z/OS V2R1: Cryptographic Services

System SSL: Modify code or System SSL application configurations to enable null encryption, RSA-Export, or RC4 ciphers

Description

Starting in z/OS V2R2, z/OS System SSL has changed its default SSL and TLS cipher support. The cipher defines the authentication, encryption, message authentication code (MAC), and key exchange algorithm used when negotiating a secure connection using SSL or TLS. When a System SSL application calls the **gsk_environment_open()** routine to establish a secure environment or the deprecated SSL or TLS **gsk_secure_soc_init()** routine specifying *cipher_specs* or *v3cipher_spec* set as NULL, the default enabled ciphers no longer includes the NULL encryption, RSA-EXPORT, or RC4 ciphers.

Table 102. SSL V3 and TLS ciphers

2 character cipher number	4 character cipher number	Short name	Description
00	0000	TLS_NULL_WITH_NULL_NULL	No encryption or message authentication and RSA key exchange.
01	0001	TLS_RSA_WITH_NULL_MD5	No encryption with MD5 message authentication and RSA key exchange.
02	0002	TLS_RSA_WITH_NULL_SHA	No encryption with SHA-1 message authentication and RSA key exchange.
03	0003	TLS_RSA_EXPORT_WITH_RC4_40_MD5 ¹	40-bit RC4 encryption with MD5 message authentication and RSA (export) key exchange.
04	0004	TLS_RSA_WITH_RC4_128_MD5	128-bit RC4 encryption with MD5 message authentication and RSA key exchange.
05	0005	TLS_RSA_WITH_RC4_128_SHA	128-bit RC4 encryption with SHA-1 message authentication and RSA key exchange.
06	0006	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 ¹	40-bit RC2 encryption with MD5 message authentication and RSA (export) key exchange.

¹ Ciphers are not supported for TLS V1.1 and TLS V1.2.

Table 103. SSL V2 ciphers

Cipher number	Description
1	128-bit RC4 encryption with MD5 message authentication.
2	128-bit RC4 export encryption with MD5 message authentication.

Notes:

1. The null encryption, RSA-EXPORT, and RC4 based ciphers are not supported when running in FIPS mode.
2. The SSL V2 and SSL V3 protocols are no longer being enabled by default. Therefore, the ciphers for those protocols do not have any meaning unless the protocol is explicitly enabled. See "System SSL: Modify code or System SSL application configurations to enable SSLV2 or SSLV3" on page 158 for more information about protocol defaults and enabling the protocols.

For the cipher values that are in the default cipher specification list along with their order, see the description of the **gsk_environment_open()** routine in *z/OS Cryptographic Services System SSL Programming*.

For applications that must continue to use these ciphers, the ciphers must be explicitly enabled.

Migration actions from z/OS V2R1: Cryptographic Services

If the ciphers in Table 102 on page 160 and Table 103 on page 160 are the only ciphers in common between the two secure connection endpoints, the following are example SSL errors that may occur when the ciphers are not explicitly enabled:

- Return code 402: No SSL cipher specifications.
- Return code -1: No SSL cipher specifications.

The full list of supported ciphers is available in *z/OS Cryptographic Services System SSL Programming*.

Table 104 provides more details about this migration action. Use this information to plan your changes to the system.

Table 104. Information about this migration action

Element or feature:	Cryptographic Services
When change was introduced:	z/OS V2R2. z/OS V2R1 and z/OS V1R13, both with APAR OA47405.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA47405.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if System SSL applications for secure SSL/TLS connections are used.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	SSL and TLS secure connections may fail if a System SSL application is relying on one of the System SSL defined default ciphers and it is no longer enabled.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If your installation utilizes System SSL applications for secure SSL/TLS connections, examine those applications to determine if they require the usage of null encryption, RSA-EXPORT, or RC4 based ciphers.

If the System SSL application runs in FIPS mode, these ciphers are not supported and no migration action is needed.

For each System SSL application that requires the usage of one or more of these ciphers, consult each application's configuration documentation to determine the appropriate enablement capability. If the application supports the use of environment variables, see Method 2 in this section for environment variable information.

If your System SSL written application needs to support one or more of the removed ciphers, z/OS System SSL provides two methods to override the default SSL/TLS ciphers enabled when negotiating a secure connection using the SSL/TLS routines. Your application will need to utilize one of the following methods:

Method 1

Use the `gsk_attribute_set_buffer()` or `gsk_secure_soc_init()` routine:

`gsk_attribute_set_buffer()`

The `gsk_attribute_set_buffer()` routine supports the specification of SSL V2 and SSL

Migration actions from z/OS V2R1: Cryptographic Services

V3/TLS ciphers in preference order through the GSK_V2_CIPHER_SPECS, GSK_V3_CIPHER_SPECS, and GSK_V3_CIPHER_SPECS_EXPANDED attributes. Each attribute buffer consists of a single character string consisting of the cipher values enabled to be used for the secure connection.

To re-enable one or more of the SSL V2 ciphers, specify the GSK_V2_CIPHER_SPECS attribute along with the complete list of ciphers to be available during the negotiation of the secure connection. For example, if you want to restore the V2 default cipher list, you need to set the buffer value to "713642" when the System SSL Security Level 3 FMID (JCPT421) is installed. Otherwise, set the buffer to "642". Setting the value to "713642" when the System SSL Security Level 3 FMID (JCPT421) is not installed results in ciphers "713" being ignored.

To re-enable one or more of the SSL V3 ciphers, specify GSK_V3_CIPHER_SPECS if 2-character cipher specifications is enabled (this is the default), or GSK_V3_CIPHER_SPECS_EXPANDED if 4-character cipher specifications is enabled along with the complete list of ciphers to be available during the negotiation of the secure connection. For example, if you want to restore the SSL V3 2-character default cipher list, set the buffer value to "050435363738392F303132330A1613100D0915120F0C0306020100" when the System SSL Security Level 3 FMID (JCPT421) is installed. Otherwise, set the buffer to "0915120F0C0306020100". Setting the value to "050435363738392F303132330A1613100D0915120F0C0306020100" when the System SSL Security Level 3 FMID (JCPT421) is not installed results in ciphers "050435363738392F303132330A1613100D" being ignored. When using the 4-character cipher values, the buffer value is "0005000400350036003700380039002F0030003100320033000A001600130010000D000900150012000F000C00030006000200010000" when the System SSL Security Level 3 FMID (JCPT421) is installed. Otherwise, set the buffer to "000900150012000F000C00030006000200010000". Setting the value to "0005000400350036003700380039002F0030003100320033000A001600130010000D000900150012000F000C00030006000200010000" when the System SSL Security Level 3 FMID (JCPT421) is not installed results in ciphers "0005000400350036003700380039002F0030003100320033000A001600130010000D" being ignored.

gsk_secure_soc_init()

The **gsk_secure_soc_init()** routine (deprecated API) supports the specification of SSL V2 and SSL V3/TLS ciphers through the *cipher_specs* and *v3cipher_specs* fields in the *gsk_soc_init_data* structure.

To re-enable one or more of the SSL V2 ciphers, specify the complete list of ciphers to be available during the negotiation of the secure connection in the *cipher_specs* field. For example, if you want to restore the SSL V2 default cipher list, set the buffer value to "713642" when the System SSL Security Level 3 FMID (JCPT421) is installed. Otherwise, set the buffer to "642". Setting the value to "713642" when the System SSL Security Level 3 FMID (JCPT421) is not installed results in ciphers "713" being ignored.

To re-enable one or more of the SSL V3/TLS ciphers, specify the complete list of ciphers to be available during the negotiation of the secure connection in the *v3cipher_specs* field. For example, if you want to restore the SSL V3 2-character default cipher list, set the buffer value to "050435363738392F303132330A1613100D0915120F0C0306020100" when the System SSL Security Level 3 FMID (JCPT421) is installed. Otherwise, set the buffer to "0915120F0C0306020100". Setting the value to "050435363738392F303132330A1613100D0915120F0C0306020100" when the System SSL Security Level 3 FMID (JCPT421) is not installed results in ciphers "050435363738392F303132330A1613100D" being ignored.

Method 2

Use the environment variables GSK_V2_CIPHER_SPECS, GSK_V3_CIPHER_SPECS, and GSK_V3_CIPHER_SPECS_EXPANDED:

GSK_V2_CIPHER_SPECS

To re-enable one or more of the SSL V2 ciphers, specify the GSK_V2_CIPHER_SPECS attribute along with the complete list of ciphers to be available during the negotiation of the secure connection. See Method 1 in this section for cipher specification list examples.

GSK_V3_CIPHER_SPECS

To re-enable one or more of the SSL V3 ciphers, specify GSK_V3_CIPHER_SPECS if 2-character cipher specifications is enabled (this is the default) along with the complete list of ciphers to be available during the negotiation of the secure connection. See Method 1 in this section for cipher specification list examples.

GSK_V3_CIPHER_SPECS_EXPANDED

To re-enable one or more of the SSL V3 ciphers, specify GSK_V3_CIPHER_SPECS_EXPANDED if 4-character cipher specifications is enabled along with the complete list of ciphers to be available during the negotiation of the secure connection. See Method 1 in this section for cipher specification list examples.

Note: Applications that have specified the SSL V3 cipher specifications using the `gsk_attribute_set_buffer()` or `gsk_secure_soc_init()` routine override the respective environment variable settings.

Reference information

For more information about System SSL, see *z/OS Cryptographic Services System SSL Programming*.

Cryptographic Services actions to perform after the first IPL of z/OS V2R2

This topic describes Cryptographic Services migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

ICSF: Accommodate the TRACEENTRY option deprecation

Description

Starting with ICSF HCR77A1, option TRACEENTRY has been deprecated and ICSF CTRACE support has been enhanced to support configurable ICSF CTRACE options from PARMLIB. A default CTICSF00 PARMLIB member is installed in SYS1.PARMLIB. The CTICSF00 PARMLIB member provides default component trace values for ICSF. By default, ICSF CTRACE support will trace with the KdsIO, CardIO, and SysCall filters using a 2M buffer. Configurable options are commented out within this PARMLIB member to provide examples of how to turn them on.

Table 105 provides more details about this migration action. Use this information to plan your changes to the system.

Table 105. Information about this migration action

Element or feature:	Cryptographic Services
When change was introduced:	Cryptographic Support for z/OS V1R13 - z/OS V2R1 web deliverable (FMID HCR77A1), which installs only on z/OS V1R13 or z/OS V2R1.

Migration actions from z/OS V2R1: Cryptographic Services

Table 105. Information about this migration action (continued)

Applies to migration from:	z/OS V2R1 and z/OS V1R13 without the Cryptographic Support for z/OS V1R13 - z/OS V2R1 web deliverable (FMID HCR77A1). Note that when the Cryptographic Support for z/OS V1R13 - z/OS V2R1 Web deliverable (FMID HCR77A1) is not installed, this migration item is not applicable.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have installed the Cryptographic Support for z/OS V1R13 - z/OS V2R1 web deliverable (FMID HCR77A1) to handle TKDS with PKDS #11 objects for the new format in HCR77A1.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	If the TRACEENTRY option is specified it will be ignored and will produce message CSFO0212 at startup; processing continues.
Related IBM Health Checker for z/OS check:	None.

Steps to take

You can code the new CTRACE option within a BEGIN(HCR77A1) END option pair in a options data set shared between multiple releases of ICSF.

- If you share the installation options data set between HCR77A1 and pre-HCR77A1 systems, you can continue to supply the TRACEENTRY option at the lower-level systems as it is ignored, and processing will continue on the HCR77A1 systems.
- If your installation cannot tolerate the CSFO0212 message that is issued at startup, you need to use different installation option data sets. Note that new CTRACE options will be in effect:
 - Review the default CTRACE options to ensure that they are satisfactory for your system.
 - Make any necessary changes. Use the CTICSF00 PARMLIB to create customized ICSF CTRACE Configuration Data Sets in PARMLIB. You can use the new CTRACE option to specify the customized ICSF CTRACE Configuration Data Set in the ICSF Options Data Set.

For example, you can specify CTRACE(CTICSFxx), where xx is any two characters that were used when copying the default CTICSF00 parmlib member.

Component tracing is active when ICSF starts using the trace options defined in the CTICSFxx PARMLIB member, where 00 is the default. If the CTICSF00 PARMLIB member is incorrect or missing, ICSF CTRACE performs tracing using an internal default set of trace options. The operator can specify trace options individually on the TRACE CT command or specify the name of a CTICSFxx PARMLIB member containing the desired trace options. Using a PARMLIB member on the TRACE CT command can help minimize operator intervention and avoid syntax or keystroke errors

Reference information

For more information, see the following references:

- *z/OS Cryptographic Services ICSF Administrator's Guide*
- For information about TKDS, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.
- For IBM Health Checker, see *IBM Health Checker for z/OS User's Guide*.

PKI Services: Migrate to IBM HTTP Server - Powered by Apache

Description

Before z/OS V2R2, PKI Services used IBM HTTP Server powered by Domino. In z/OS V2R2, IBM HTTP Server - Powered by Apache replaces it as a base element of z/OS V2R2. You must now use the IBM HTTP Server - Powered by Apache.

Table 106 provides more details about this migration action. Use this information to plan your changes to the system.

Table 106. Information about this migration action

Element or feature:	Cryptographic Services
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

This information assumes that you used the installer program (*bin/install_ihs*) to install IBM HTTP Server - Powered by Apache. You must know the installation directory for the server instance, which is referred to as *ihs-install-dir* in the sample commands. (This directory must be different from the product directory, usually */usr/lpp/ihsa_zos*).

Replace the references to *pki-install-dir* with the z/OS UNIX file system directory where z/OS PKI Services was installed. Usually, the directory is */usr/lpp/pkiserv/*.

The IBM HTTP Server installer program creates the *ihs-install-dir/conf/httpd.conf* configuration file that must be updated with directives provided in samples that are shipped by PKI Services and with information specific to your installation. The samples that are provided by PKI Services assume that the *conf/httpd.conf* contains directives that apply to each HTTP Server process, and that configuration directives for unsecure port, SSL server authentication port, and SSL client authentication port configuration are in separate configuration files that contain the `<VirtualHost>` directives that are then included in the *conf/httpd.conf* file. The port-specific configuration files are then included in the base *conf/httpd.conf* file. Follow the steps that follow to incorporate information from the PKI Services sample *httpd.conf* file into your *conf/httpd.conf* file, and to create and update the `VirtualHost` files specific to the PKI Services configuration.

Follow these steps:

1. Incorporate the directives from the PKI Services sample *httpd.conf* file (*pki-install-dir/samples/httpd.conf*) into the *ihs-install-dir/conf/httpd.conf* configuration file.
 - a. Locate the section of the *conf/httpd.conf* file that contains the `LoadModule` directives. Ensure that the following directives are specified and not commented out (a `#` in the first position of a line indicates that the line is a comment).
 - `LoadModule rewrite_module modules/mod_rewrite.so`

Migration actions from z/OS V2R1: Cryptographic Services

- LoadModule alias_module modules/mod_alias.so
 - LoadModule authnz_saf_module modules/mod_authnz_saf.so (This LoadModule directive is located after the # z/OS specific modules comment.)
- b. Locate the existing AddType directives in the conf/httpd.conf and add the AddType directives from the PKI Services sample httpd.conf file:
 - AddType application/x-x509-user-cert.cer
 - AddType application/x-x509-ca-cert.der
 - AddType application/octet-stream.msi
 - AddType application/pkix-crl.crl
 - c. Add the Include directives for the VirtualHost configuration files from the PKI Services sample httpd.conf file near the end of the conf/httpd.conf file:
 - Include conf/vhost80.conf
 - Include conf/vhost443.conf
 - Include conf/vhost1443.conf

Note: If you use different port numbers than 80, 443, and 1443, change the name of the files to match the port numbers that are used. For example, if you use port 1080 instead of 80 for the unsecure port, change the vhost80.conf file to vhost1080.conf. Also, make sure that the port number change is made within the vhost*.conf files. For example, change the <VirtualHost *:80> directive to <VirtualHost *:1080>.

2. Copy the sample VirtualHost configuration files from the PKI Services samples directory to the *his-install-dir/conf* directory. For example, if the *pki-install-dir* is */usr/lpp/pkiserv*, and the *his-install-dir* is */etc/websrvissue* the following command to copy the VirtualHost *:80 files:

```
cp /usr/lpp/pkiserv/samples/vhost*.conf /etc/websrv/conf
```

Note: To fully support the capabilities of PKI Services, the IBM HTTP Server powered by Domino required these instances to be running:

- An instance for non-secure and server authentication SSL connections, and
- an instance for client authentication SSL connections.

The IBM HTTP Server - Powered by Apache fully supports PKI Services capabilities in a single instance using VirtualHost configuration files for non-secure, server authentication SSL, and client authentication SSL connections.

3. Make the following updates to each of the VirtualHost configuration files using information from the httpd.conf files from the IBM HTTP Server powered by Domino (These are referred to as the old httpd.conf files). The sample VirtualHost configuration files that are shipped with PKI Services have directives that assume the use of the PKIServ and Customers domain names. If you use different or additional domain names, you must update or add additional directives to the vhost*.conf files.
 - a. Change all instances of <server-domain-name> to the fully qualified domain name of your web server. (This is in the Hostname directive value that is from the old httpd.conf files).
 - b. Change all instances of <application-root> to the *pki-install-dir* value. (*/usr/lpp/pkiserv/* by default).
 - c. If you are not using the default location of */etc/pkiserv* for the PKI Service configuration directory, update the SetEnv directive for *_PKISERV_CONFIG_PATH* with the value specified in the old httpd.conf files (as InheritEnv directives) or in the old httpd.envvars file. If additional *_PKISERV_CONFIG_PATH_** environment variables are defined in your old httpd.conf or httpd.envvars files, add another SetEnv directive for each in the VirtualHost configuration files.
 - d. The ScriptAliasMatch directives replace the Exec directives from the old httpd.conf files. The sample vhost*.conf files provide ScriptAliasMatch directives for the PKIServ and Customers domain names. Change or add additional ScriptAliasMatch directives based on the Exec directives from the old httpd.conf file. (ScriptAliasMatch directives for public-cgi URLs are placed in the vhost80.conf file, ssl-cgi-bin URLs are placed in the vhost443.conf file, and clientauth-cgi-bin URLs are placed in the vhost1443.conf file).

Old httpd.conf file Exec directives:

Migration actions from z/OS V2R1: Cryptographic Services

```
Exec /PKIServ/public-cgi/* /usr/lpp/pkiserv/PKIServ/public-cgi/*
Exec /Customers/public-cgi/* /usr/lpp/pkiserv/PKIServ/public-cgi/*
```

Equivalent vhost80.conf file ScriptAliasMatch directive:

```
ScriptAliasMatch /(PKIServ|Customers)/public-cgi/(.*) /usr/lpp/pkiserv/PKIServ/public-cgi/$2
```

- e. The AliasMatch directives replace the Pass directives from the old httpd.conf files. The sample vhost*.conf files provide AliasMatch directives for the PKIServ and Customers domain names. Change or add additional AliasMatch directives based on the Pass directives from the old httpd.conf file. (AliasMatch directives for public-cgi URLs are placed in the vhost80.conf file, ssl-cgi-bin URLs are placed in the vhost443.conf file, and clientauth-cgi-bin URLs are placed in the vhost1443.conf file).

Old httpd.conf Pass directives:

```
Pass /PKIServ/cacerts/* /var/pkiserv/*
Pass /PKIServ/PKIXEnroll/* /usr/lpp/pkiserv/ActiveX/PKIXEnroll/*
Pass /PKIServ/PKICEnroll/* /usr/lpp/pkiserv/ActiveX/PKICEnroll/*
```

Equivalent vhost80.conf file AliasMatch directives:

```
AliasMatch /PKIServ/cacerts/(.*) /var/pkiserv/$1
AliasMatch /PKIServ/(PKIXEnroll|PKICEnroll)/(.*) /usr/lpp/pkiserv/ActiveX/$1/$2
```

- f. The Redirect directives from the old httpd.conf files are replaced with RewriteRule directives in the vhost*.conf files. If you are not using the PKIServ and Customers domain names or have additional domain names, you will need to change or create new RewriteRule directives. Also, if you are not using ports 80 and 443, the ports you are using for the non-secure and server authentication SSL must be added to the URL in the RewriteRule directives.

Old httpd.conf Redirect directive:

```
Redirect /PKIServ/ssl-cgi/* https://pokey.example.com/PKIServ/ssl-cgi-bin/*
Redirect /PKIServ/ssl-cgi/auth/* https://pokey.example.com/PKIServ/ssl-cgi-bin/auth/*
```

Equivalent RewriteRule directive:

```
RewriteRule ^/(PKIServ|Customers)/ssl-cgi/(.*)https://pokey.example.com/$1/ssl-cgi-bin/$2 [R,NE]
```

Note: This example is for redirecting from a non-secure URL to a server authentication SSL URL using the standard SSL port of 443. If a non-standard port is being used, the port number must be specified after the host name. For example, if port 4443 is used instead of 443, the URL starts with: https://pokey.example.com:4443/PKIServ/....

- g. The Directory and DirectoryMatch directives replace the Protect and Protection directives from the old httpd.conf files. The sample vhost*.conf files provide Directory and DirectoryMatch directives for the PKIServ and Customers domain names. Change or add additional Directory and DirectoryMatch directives based on the Protect and Protection directives from the old httpd.conf file. The surrogate user ID specified in the Directory/DirectoryMatch directives is PKISERV. If you use a different surrogate user ID, you must change PKISERV to the user ID specified in the old httpd.conf files.
 - h. The LocationMatch directives in the vhost*.conf files apply specific behavior to a specific URL for the PKIServ and Customers domain names. Change or add LocationMatch directives based on the domain names in the old httpd.conf files.
4. Update the vhost443.conf file to specify the keyfile value from the old httpd.conf file. (This assumes the IBM HTTP Server - Powered by Apache runs as the same USERID as the IBM HTTP Server powered by Domino.)

Old httpd.conf keyfile directive:

```
keyfile SSLring SAF
```

Equivalent keyfile directive:

```
Keyfile /saf SSLring
```

5. Take the following steps to update the vhost1443.conf file:
 - a. Update the keyfile value from the value that is specified in the old httpd.conf file. (This assumes the IBM HTTP Server - Powered by Apache runs as the same USERID as the IBM HTTP Server powered by Domino.)

Migration actions from z/OS V2R1: Cryptographic Services

Old httpd.conf keyfile directive:

```
keyfile SSLring SAF
```

Equivalent keyfile directive:

```
Keyfile /saf SSLring
```

- b. If you configured the IBM HTTP Server powered by Domino to perform revocation checking and want to continue to perform revocation checking in the IBM HTTP Server - Powered by Apache, add the following directive to the vhost1443.conf file after the SSLClientAuth directive:
- SSLCRLHostName - Set the value from the old httpd.conf file SSLX500Host directive.
 - SSLCRLPort - Set the value from the old httpd.conf file SSLX500Port directive.
 - SSLCRLUserID - Set the value from the old httpd.conf file SSLX500UserID directive.
 - SSLStashfile - Set the value from the old httpd.conf file SSLX500Password directive.

Note: SSLStashfile is the fully qualified path to the file that contains the password for the user name on the LDAP server. This directive is not required for an anonymous bind. Use it when you specify a user ID. Use the **sslstash** command, which is in the bin directory of IBM HTTP Server, to create your CRL password stash file. Specify the password that you use to log in to your LDAP server as the password on the **sslstash** command. The format of the **sslstash** command is:

```
sslstash [-c] file function password
```

where:

-c Creates a new stash file. If not specified, an existing file is updated.

file

Is the fully qualified name of the file to create or update.

function

Indicates the function for which the password is to be used. Valid values include crl and crypto.

password

Is the password to stash.

Reference information

For more information, see the following references:

- *z/OS Cryptographic Services PKI Services Guide and Reference*
- WebSphere Application Server Knowledge Center (www.ibm.com/support/knowledgecenter/SSEQTP)

DFSMS migration actions

This topic describes migration actions for base element DFSMSdfp and optional features DFSMSdss, DFSMSshsm, DFSMSrmm, and DFSMSstvs.

DFSMS actions to perform before installing z/OS V2R2

This topic describes DFSMS migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

DFSMSdfp: Back up SMS control data sets

Description

In a multisystem Storage Management Subsystem (SMS) complex, operating systems share a common set of SMS classes, groups, ACS routines, and a configuration base, which make up the storage management policy for the complex. This storage management policy is maintained in a source control data set (SCDS). When this policy is activated for SMS, the bound policy is maintained in processor storage and on DASD in an active control data set (ACDS). Systems in the complex communicate SMS information through a common communications data set (COMMDS).

It is recommended that to successfully share SMS control data sets in a multisystem environment where there are mixed levels of DFSMS, you update, translate, validate, and activate SMS policies on the system with the latest level of DFSMS. When an earlier control data set is to be updated or activated, the control data set is formatted by the later-level system. The shared SMS control blocks reflect the new, rather than the previous, lengths and control information.

For fallback, IBM recommends restoring SMS control data sets from backups taken on the fallback release.

Editing a policy on an earlier system could invalidate unused control information and prevent the control data set from being accessed by a later system. A warning message is provided before a policy can be changed on an earlier system. ACS routines may need to be updated and translated so to not reference policy items not known to the earlier system.

Remember, you risk policy activation failures if SCDS changes are not validated using the latest-level system in a sysplex.

Table 107 provides more details about this migration action. Use this information to plan your changes to the system.

Table 107. Information about this migration action

Element or feature:	DFSMSdfp.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended to ensure data integrity.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	Install the PTFs in “Install coexistence and fallback PTFs” on page 6 if they are not already installed.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Do the following on your pre-z/OS V2R2 systems:

1. Back up SMS control data sets according to established procedures in the event that fallback is required. The control data set format is VSAM linear.
2. Install all coexistence PTFs in “Install coexistence and fallback PTFs” on page 6.

In addition, if you modified and activated a higher-level policy on a pre-z/OS V2R2 system, do the following to ensure that the ACDS can be accessed on z/OS V2R2 and that the SMS control block reflect the new lengths and control information:

1. On the pre-z/OS V2R2 system, save the active ACDS as an SCDS with the SETSMS SAVESCDs command.
2. On z/OS V2R2, update, translate, validate, and activate the saved SMS policy.

Migration actions from z/OS V2R1: DFSMS

Reference information

For more information, see the following references:

- *z/OS DFSMS Implementing System-Managed Storage*
- *z/OS DFSMSdfp Storage Administration*

DFSMSdss: Determine whether you need DISABLE(REFUCB) in parmlib member DEVSUPxx

Description

With z/OS V2R2, the automatic refresh UCB (REFUCB) function of the Device Manager is enabled by default. Previously, it was disabled by default. If you want the function to be disabled, you must explicitly disable it by using the statement `DISABLE(REFUCB)` in parmlib member `DEVSUPxx`.

ICKDSF `FLASHCPY`, `INIT`, and `REFORMAT` commands, and DFSMSdss full volume `COPY` and `RESTORE` functions, might update the volume serial and location of the volume table of contents (VTOC). This behavior can present a problem when the device is online to other systems. To address this problem, the automatic refresh UCB function (REFUCB) was introduced in z/OS V1R13, and is controlled by `DISABLE | ENABLE(REFUCB)` in parmlib member `DEVSUPxx`. `DISABLE(REFUCB)` was the default.

Table 108 provides more details about this migration action. Use this information to plan your changes to the system.

Table 108. Information about this migration action

Element or feature:	DFSMSdss
When change was introduced:	z/OS V2R2
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you require the automatic refresh UCB function to be disabled. Note that the automatic refresh UCB function is only applicable to volumes that are shared with other systems in the same sysplex.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	For each system that has enabled the REFUCB function, an unconditional <code>VARY ONLINE</code> to the device is performed when the system is notified that the volume serial, the VTOC location, or both, has changed since the device was last varied online. This action updates fields in the UCB, including the volume serial (UCBVOLI) and the start location of the VTOC (UCBVTOC). If the <code>VARY ONLINE,UNCOND</code> fails for the device, or if the <code>VARY ONLINE,UNCOND</code> is not performed because the REFUCB function is not enabled on a system in the sysplex, the following write-to-operator (WTO) message is written to the system console: <code>DM00063E dddd,volser,UCB NOT UPDATED REFUCB=[Y/N],USERS=xxxx</code> .
Related IBM Health Checker for z/OS check:	Use check <code>IBMDMO</code> , <code>DMO_REFUCB</code> to determine whether the REFUCB function is disabled by the system. This check is provided as of z/OS V2R2. For more information, see <i>IBM Health Checker for z/OS User's Guide</i> .

Steps to take

If you determine that you need the automatic refresh UCB function to be disabled, review your current parmlib member DEVSUPxx. If DISABLE(REFUCB) is not present, add DISABLE(REFUCB). If ENABLE(REFUCB) is present, delete it.

Reference information

For information about enabling or disabling the automatic refresh UCB function, see the description of parmlib member DEVSUPxx in *z/OS MVS Initialization and Tuning Reference*.

DFSMSdfp: Prepare for the removal of TSO copy services commands

Description

z/OS V2R2 is planned to be the last release to include a number of TSO/E-based System Data Mover (SDM) related commands. Except for the query commands (CQUERY, FCQUERY, RQUERY, XQUERY, XSTATUS), the ANTRQST API, and the XSET command, which will remain, IBM recommends that users migrate to the REXX versions of these commands.

Specifically, the following commands will no longer supported in TSO:

- FCESTABL
- FCWITHDR
- CDELPAIR
- CDELPATH
- CESTPAIR
- CESTPATH
- CGROUP
- CRECOVER
- CSUSPEND
- RSESSION
- RVOLUME
- XADDPAIR
- XADVANCE
- XCOUPLE
- XDELPAIR
- XEND
- XRECOVER
- XSTART
- XSUSPEND

Table 109 provides more details about this migration action. Use this information to plan your changes to the system.

Table 109. Information about this migration action

Element or feature:	DFSMSdfp
When change was introduced:	See IBM United States Software Announcement 215-267 "IBM z/OS Version 2 Release 2—Fueling the new digital enterprise," dated July 28, 2015.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use the TSO commands.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.

Migration actions from z/OS V2R1: DFSMS

Table 109. Information about this migration action (continued)

Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS checks:	None.

Steps to take

Convert existing non-query TSO commands to the REXX version using the programs provided in SYS1.DGTCLIB (ANTFREXX for FlashCopy, ANTPREXX for PPRC, ANTXREXX for XRC). Some of the command keywords are slightly different than the TSO version, and might need to be modified. For example, for full volume FlashCopy establish, you might enter the TSO command, as follows:

```
FCESTABL SDEVN(0F60) TDEVN(0F61)
```

To use the REXX interface, you can enter:

```
ANTFREXX FCESTABLISH SDEVN(0F60) TDEVN(0F61) SRCEXTNA() andTGTEXTNA()
```

Reference information

For more information about using the REXX commands, see *z/OS DFSMS Advanced Copy Services*.

DFSMSrmm: Prepare for the removal of the DFSMSrmm CIM provider Description

z/OS V2R2 is planned to be the last release to support the DFSMSrmm Common Information Model (CIM) provider. The DFSMSrmm CIM provider uses the DFSMSrmm application programming interface (API) to retrieve information about DFSMSrmm resources in real time.

IBM recommends that you remove the provider registration and its associated files from your system. If you need to retrieve information about DFSMSrmm resources, see “Steps to take” on page 173 for alternative methods.

Table 110 provides more details about this migration action. Use this information to plan your changes to the system.

Table 110. Information about this migration action

Element or feature:	DFSMSrmm
When change was introduced:	See IBM United States Software Announcement 215-267 “IBM z/OS Version 2 Release 2—Fueling the new digital enterprise,” dated July 28, 2015.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you configured the DFSMSrmm CIM provider.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS checks:	None.

Steps to take

Follow these steps:

1. Determine whether the DFSMSrmm CIM provider is configured on your system. Check for the following conditions, which must be true if the DFSMSrmm CIM provider is active:
 - Determine whether Java Version 1.5.x is active on your system. This level is the maximum supported Java version for the DFSMSrmm CIM provider. You can use the following shell command: **java -version**
 - Determine whether the following files exist in z/OS UNIX System Services:


```
/etc/rmm/rmmcust.properties
/var/rmm/rmm.properties
```

or equivalent files exist in Linux, for example, in the \$RMM_DIR- directory.
 - Determine whether the cimserver process is running under z/OS UNIX, or the CFZCIM started task procedure is running under z/OS.
 - Determine whether any DFSMSrmm providers are registered and running. You can use the following shell command: **cimprovider -l -s**
2. For any DFSMSrmm CIM providers that you find, unregister the providers. You can use the following shell command: **cimprovider -r -m module_name**
3. Remove the following files from z/OS UNIX or the equivalent files in Linux:


```
/var/rmm/rmm.properties
/etc/rmm/rmmcust.properties
/etc/rmm/rmmlog.properties
```

If you need to display information about DFSMSrmm resources in real time, you can use DFSMSrmm subcommands or panels. To obtain this information programmatically, for example, to create reports or implement automation, you can retrieve the output through:

- REXX variables
- Structured field introducers (SFIs) or XML, by using high-level language APIs or web services.

Reference information

For more information, see the following references:

- For information about the DFSMSrmm CIM provider, see *z/OS DFSMSrmm Implementation and Customization Guide*
- For information about the DFSMSrmm API, see *z/OS DFSMSrmm Application Programming Interface*

DFSMS actions to perform before the first IPL of z/OS V2R2

This topic describes DFSMS migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

DFSMSdfp: Ensure that the Language Environment runtime library is available for DLLs

Description

Language Environment provides common services and language-specific routines in a single runtime environment. You can use Language Environment to build and use dynamic link libraries (DLLs) for applications.

Table 111 on page 174 provides more details about this migration action. Use this information to plan your changes to the system.

Migration actions from z/OS V2R1: DFSMS

Table 111. Information about this migration action

Element or feature:	DFSMSdftp.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if your installation builds or references DLLs.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If your installation builds or references DLLs, either you must set up the system link list to refer to the Language Environment runtime libraries (SCEERUN and SCEERUN2), or each job that creates or uses a DLL must include a STEPLIB DD statement referencing these libraries.

Reference information

For more information, see the following references:

- *z/OS V2R1.0 Language Environment Runtime Application Migration Guide*
- *z/OS Language Environment Customization*
- *z/OS Language Environment Programming Guide*

DFSMSdftp: Update SYS1.IMAGELIB Description

If you use page mode printers such as the IBM 3800 or the IBM 3900 running in line mode (not page mode), you must install library character sets, graphic character modification modules, and character arrangement tables in SYS1.IMAGELIB. This migration action does not apply if you are using IBM 3900 printers that are driven by PSF.

Table 112 provides more details about this migration action. Use this information to plan your changes to the system.

Table 112. Information about this migration action

Element or feature:	DFSMSdftp.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you are not using your old SYS1.IMAGELIB, you are installing with ServerPac or SystemPac, and you are using line mode printers such as the 3800 or 3900.
Target system hardware requirements:	IBM 3800 or 3900 printers.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.

Table 112. Information about this migration action (continued)

Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Run the LCSBLD1 job from the samplib data set to create character sets, graphic character modification modules, and character arrangement tables in SYS1.IMAGELIB.
2. Copy customized or locally-written FCBs and UCS images from your old system's SYS1.IMAGELIB data set to the new system's SYS1.IMAGELIB data set.

Reference information

For information about maintaining SYS1.IMAGELIB, see *z/OS DFSMSdfp Advanced Services*.

DFSMSdfp: Adjust parameters to control whether offline device discovery is performed

Description

Beginning in APAR OA43706 (PTFs: UA74649 for z/OS V2R1 and UA74648 for z/OS V1R13), the System Data Mover (ANTAS000 address space) is changed to conditionally invoke offline device discovery during IPL. Prior to this APAR, offline device discovery was always performed.

APAR OA43706 introduced a new keyword called `OfflineDiscovery` to the `ANTXIN00` parmlib member to allow you to control whether offline device discovery is performed during IPL when `ANTAS000` first starts up, and thereafter when `ANTAS000` restarts following a `CANCEL`. A value of `YES` causes offline discovery to take place. A value of `NO` bypasses offline device discovery. If `OfflineDiscovery` is not specified, the default is `OfflineDiscovery(NO)`.

Tip: The Offline Device Discovery was introduced by APAR OA36570 (PTFs for z/OS V1R12 and V1R13) and incorporated into z/OS V2R1 to reduce the `XSTART` time following an IPL.

SYSLOG messages example:

```
ANTB8000I XRC INITIALIZATION STARTED
ANTB8002I OFFLINE DEVICE DISCOVERY COMPLETE; RC=0 REAS=606
ANTB8001I XRC INITIALIZATION COMPLETED
```

Table 113 provides more details about this migration action. Use this information to plan your changes to the system.

Table 113. Information about this migration action

Element or feature:	DFSMSdfp.
When change was introduced:	z/OS V2R1 and z/OS V1R13, both with APAR OA43706 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA43706 applied.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you need offline device discovery to be performed during IPL.
Target system hardware requirements:	None.

Migration actions from z/OS V2R1: DFSMS

Table 113. Information about this migration action (continued)

Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	See “Steps to take” for specific configuration considerations.
Related IBM Health Checker for z/OS check:	None.

Steps to take

You should only need to perform offline device discovery during IPL (that is, specify `OfflineDiscovery(YES)` in `ANTXIN00`) if you are using one of the following:

- GDPS MzGM (aka XRC) in HYPER-PPRC mode (Incremental Resynch)
- GDPS MzGM under z/OS with XRC Offline Primary devices

Other XRC configurations or non-XRC environments will not directly benefit from having offline discovery performed at IPL. Therefore, if it is not required, do not specify the keyword and avoid discovery, which may reduce overall IPL elapsed time.

Tip: The value of `OfflineDiscovery` takes effect when the `ANTAS000` address space is started during IPL, or with the automatic restart of `ANTAS000` after it has been cancelled. To activate a new value for `OfflineDiscovery` without an IPL, do the following:

1. Update the value in `PARMLIB` member `ANTXIN00`
2. Issue the system command `CANCEL ANTAS000`

The `OfflineDiscovery` keyword is ignored and will not be processed if it is specified in the `ALL` or session member of `hlq.XCOPY.PARMLIB`.

Reference information

For more information, see *z/OS DFSMS Advanced Copy Services* .

DFSMSdfp: Define a security profile for VSAM exception exits Description

VSAM users can specify an exit to receive control for physical I/O errors that might occur against a VSAM data set, through either of the following methods:

- `EXCEPTIONEXIT` keyword of the `IDCAMS` define function
- `SYNAD=` sub-parameter of the `AMP=` keyword of the `DDNAME` JCL statement.

As of APAR OA46090, the exit name that can be specified on these keywords is controlled through a `FACILITY` class profile. The `FACILITY` class profile is named `IDA.VSAMEXIT.exitname` where *exitname* identifies the exit to be invoked.

You must ensure that the exit name is protected through a `FACILITY` class profile, and that callers of the exit have at least `READ` authority.

Table 114 provides more details about this migration action. Use this information to plan your changes to the system.

Table 114. Information about this migration action

Element or feature:	DFSMSdfp.
---------------------	-----------

Table 114. Information about this migration action (continued)

When change was introduced:	z/OS V2R1 and z/OS V1R13, both with APAR OA46090 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA46090 applied.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if your installation has VSAM exception exits that are specified through the AMP or EXCEPTIONEXIT parameters.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	<p>If you have programs that specify VSAM exception exits in this manner and you do not take the necessary migration action, the programs will encounter the following open errors:</p> <ul style="list-style-type: none"> • Non-authorized exits specified in the EXCEPTIONEXIT parm: IEC161I 40(1)-53 • Non-authorized exits specified in the SYNAD parm: IEC161I 40(2)-81
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Define a FACILITY class profile with the resource name IDA.VSAMEXIT.*exitname*, where *exitname* is the EXCEPTIONEXIT or SYNAD parameter value.
- Ensure that callers of the exit have at least READ authority to the FACILITY class resource name.

Use caution if you choose to use a generic RACF profile to ensure that you do not allow unintended modules to be used as VSAM exception exits.

Note: This action must be taken even if the exits do not actually exist, unless you choose to remove the EXCEPTIONEXIT or SYNAD parameter.

Reference information

For more information, see *z/OS DFSMS Using Data Sets*.

DFSMSdftp: Accommodate change for data set name prefix in IDCAMS ALLOCATE Description

With IDCAMS APAR OA42679 and TSO/E APAR OA43330 applied, the **IDCAMS ALLOCATE** command is changed in the way that it starts TSO/E to allocate a data set. IDCAMS processing now uses the TSO/E Service Facility (TSF) to allocate a data set, rather than running the **ALLOCATE** command under the TSO/E terminal monitor program (IKJEFT01). With this change, the user ID assigned to the IDCAMS batch job is treated as the default data set prefix. That is, the user ID for the IDCAMS batch job is appended to the data set name as a high-level qualifier, if you specify the data set name on the DATASET keyword without quotation marks and the user ID does not have a RACF TSO segment.

Migration actions from z/OS V2R1: DFSMS

Previously, the **IDCAMS ALLOCATE** command used a null prefix for the allocated data set, if you specified the data set name on the **DATASET** keyword without quotation marks and the user ID did not have a RACF TSO segment.

Assume, for example, that the user ID **ZZZZZZZ** is defined in both UADS and in RACF without a TSO segment; note the following differences in behavior:

- Before this change, TSO runs under the UADS user. If the data set name is specified without quotation marks on the **DATASET** keyword, and the user has a UADS PROFILE PREFIX(*prefix*), the prefix is used as the data set prefix. Otherwise, the user ID is used as the data set prefix.
- After this change, the user ID is always used as the data set prefix. Therefore, if the user ID and UADS PROFILE PREFIX(*prefix*) are different, the high-level qualifier for the data set is changed.

Table 115 provides more details about this migration action. Use this information to plan your changes to the system.

Table 115. Information about this migration action

Element or feature:	DFSMSdfp
When change was introduced:	z/OS V2R1 and z/OS V1R13, both with APARs OA42679 (DFSMS) and OA43330 (TSO/E) applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APARs OA42679 (DFSMS) and OA43330 (TSO/E).
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use IDCAMS ALLOCATE , do not specify the data set name in quotation marks on the DATASET keyword, and the user ID assigned to the IDCAMS batch job does not have a RACF TSO segment.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Failure to include the data set name in quotation marks can result in allocation errors.
Related IBM Health Checker for z/OS checks:	None.

Steps to take

Check for JCL and programs that use the **IDCAMS ALLOCATE** command. Ensure that the data set name is specified in quotation marks on the **DATASET** keyword. Doing so ensures that the user ID is not appended to the data set name as a high-level qualifier.

When the **IDCAMS ALLOCATE** command is run by a user with a RACF TSO segment defined, no change is required.

Reference information

Documentation APAR OA47508 describes these changes. For more information about the IDCAMS utility, see *z/OS DFSMS Access Method Services Commands* .

DFSMSdftp: Accommodate new authorization requirements for users of the IDCAMS DEFINE command

Description

IDCAMS APAR OA47269 introduces changes to the RACF authorization checking of data set aliases, VSAM cluster paths, and alternate indexes (AIXs). As a result of this change, users of the **IDCAMS DEFINE** command might require additional security authorizations for defining these objects.

In previous releases:

- For a **DEFINE ALIAS** request, if the alias was for a generation data set or a non-VSAM data set, the generation data set name or the non-VSAM data set name was used for RACF authorization checking
- For a **DEFINE ALTERNATEINDEX** or **DEFINE PATH** request, the associated cluster name was used for RACF authorization checking.

With IDCAMS APAR OA47269 applied, the user of the **IDCAMS DEFINE** command requires SAF ALTER authority:

- To the target data set when defining an alias for the data set. This requirement is added to the existing requirement that users have SAF UPDATE authority to the catalog that is to contain the alias, if the associated data set is non-SMS-managed. If the associated data set is SMS-managed, no SAF authority is required.
- To the VSAM cluster, when defining a VSAM path or alternate index name (AIX) for the cluster. This requirement is added to the existing requirement that users have SAF UPDATE authority to the catalog, if the related cluster is not SMS-managed.

Table 116 summarizes the changes to authorization requirements for defining data set aliases, VSAM cluster paths, and alternate indexes.

Table 116. Required security authorization for data set aliases, VSAM cluster paths, and alternate indexes

IDCAMS command	Function performed	Authorization that is required for the related data set or cluster (without APAR OA47269 applied)	Authorization that is required for the related data set or cluster (with APAR OA47269 applied)
DEFINE ALIAS	Defines an alternate name for a non-VSAM data set or a user catalog.	NONE	ALTER See Note 1.
DEFINE PATH	Defines a path directly over a base cluster or over an alternate index and its related base cluster.	NONE	ALTER See Note 2.
DEFINE ALTERNATEINDEX	Defines an alternate index.	NONE	ALTER See Note 2.

Notes:

1. The user requires ALTER authority to the alias name, unless the user has READ authority to resource name STGADMIN.IGG.CATALOG.SECURITY.CHANGE. If so, the user does not require authorization to the data set name.
2. The user requires ALTER authority to the entry name, unless the user has READ authority to resource name STGADMIN.IGG.CATALOG.SECURITY.CHANGE. If so, the user requires ALTER authority to the cluster name.

Table 117 on page 180 provides more details about this migration action. Use this information to plan your changes to the system.

Migration actions from z/OS V2R1: DFSMS

Table 117. Information about this migration action

Element or feature:	DFSMSdftp.
When change was introduced:	z/OS V2R1 and z/OS V1R13, both with APAR OA47269 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA47269 applied.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if your installation has data sets with aliases, paths, or alternate indexes (AIXs) that are not covered by existing security profiles.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	If you do define the required security profiles, authorization errors might occur, due to insufficient authority.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Review the security profiles for data sets that use aliases, paths, and alternate indexes. For any alias, path, or alternate index (AIX) that is not covered by an existing security profile, add or change security profiles for alias, path, or AIX to grant the appropriate authority.
Depending on your installation's naming conventions, you might find that your existing security profiles do not require any changes. For example, if the user ID of the user is the data set high-level qualifier.
- If your installation cannot immediately tolerate the change in authorization checking, you can reinstate the previous method of authorization checking by doing the following:
 - Defining a FACILITY class profile with the resource name of STGADMIN.IGG.CATALOG.SECURITY.CHANGE
 - Ensuring that users have at least READ authority to the FACILITY class resource name.

Reference information

For more information about creating authorizations for IDCAMS commands, see *z/OS DFSMS Access Method Services Commands*.

DFSMSdss: Build the IPLable stand-alone DFSMSdss image Description

Starting with z/OS V1R12, DFSMSdss uses BSAM instead of EXCP to read from and write to DFSMSdss dump data sets during DUMP, COPYDUMP, and RESTORE operations. As a result, if you plan to use DFSMSdss Stand-Alone Services, you must rebuild the IPL-capable core image for the Stand-Alone Services program.

Table 118 on page 181 provides more details about this migration action. Use this information to plan your changes to the system.

Table 118. Information about this migration action

Element or feature:	DFSMSdss.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you want to use DFSMSdss Stand-Alone Services.
Target system hardware requirements:	Stand-Alone Services supports the IBM 3494 TotalStorage Enterprise Automated Tape Library, the IBM 3495 TotalStorage Enterprise Automated Tape Library, and the IBM 3590 TotalStorage Enterprise Tape Subsystem.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	Stand-Alone Services does not support the creation of the core image on an SMS-managed volume.
System impacts:	<p>If this migration action is not performed, users of DFSMSdss standalone restore cannot restore to tape any backups that were created with greater than 65520-byte blocks. The operation fails with the message ADRY3530I SEQUENCE ERROR ON RESTORE TAPE.</p> <p>Backups created with 65520 byte blocks can be restored as before.</p>
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Use the DFSMSdss command BUILDSEA to create a Stand-Alone Services IP-capable core image. On the command, you can specify:
 - Device from which Stand-Alone Services are to be IPLed (such as a card reader, tape drive, or DASD volume)
 - Operator console to be used for Stand-Alone Services

The BUILDSEA command builds the IPLable core image on the current operating system and determines a record size, based on whether the IPL is performed from a card, tape, or DASD.
2. Use your security management product, such as RACF, to protect the SYS1.ADR.SAIPLD.Vvolser data set and the Stand-Alone Services modules.
3. If you have not already done so, create a backup copy of your system that can be restored by this function. For information about backing up volumes, see *z/OS DFSMSdfp Storage Administration*.

Notes:

1. To ensure that Stand-Alone Services is available when you run from DASD, do not delete the SYS1.ADR.SAIPLD.Vvolser data set or move it to another volume.
2. If you IPL from DASD and later change the volume serial number, you must rerun the BUILDSEA function to create a new core image data set with the new volume serial number in the name.
3. If you attempt to use the DFSMSdss stand-alone restore program from z/OS V1R11 to restore a backup that was created with a block size greater than 65520 bytes, the operation fails with the message ADRY3530I SEQUENCE ERROR ON RESTORE TAPE.

Migration actions from z/OS V2R1: DFSMS

Reference information

For more information, see *z/OS DFSMSdss Storage Administration*.

DFSMSdss: Accommodate ADREID0 EIREC14 expansion

Description

With APAR OA42238, the length of the EIREC14 structure in the ADREID0 macro is increased by 16 bytes. This expansion, which is related to DFSMSdss support for dump data sets compressed with zEDC services, may require changes for applications that invoke DFSMSdss using its application programming interface.

Table 119 provides more details about this migration action. Use this information to plan your changes to the system.

Table 119. Information about this migration action

Element or feature:	DFSMSdss
When change was introduced:	z/OS V2R1 and z/OS V1R13, both with APAR OA42238 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA42238 applied.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use the DFSMSdss application programming interface.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Check for use of the Function Ending user interaction module exit option (EIOPTION14) in applications that exploit the DFSMSdss application programming interface. If EIOPTION14 is used, determine if the UIM copies the structure pointed to by EIRECPTR. In this exit the structure pointed to by EIRECPTR is named EIREC14. If the application copies the area of storage pointed to by EIRECPTR, then action may be required.

If the application copies the area of storage using EIRECLEN for the amount of data to copy, then the application must ensure the area that is the destination of the copy is large enough to accommodate the larger EIREC14 structure.

The length of the EIREC14 structure is not provided in the ADREID0 data area. Prior to the application of the PTFs for OA42238, determine the length of the EIREC14 structure with an equate of this form:

```
EQU EI14CPUT+L'EI14CPUT-EIREC14
```

After the application of the PTFs for OA42238, determine the length of the EIREC14 structure with an equate of this form:

```
EQU EI14ZCSV+L'EI14ZCSV+15-EIREC14
```

Reference information

For more information about the application programming interface and Eioption 14, see *z/OS DFSMSdss Storage Administration*.

DFSMSHsm: Update applications that depend on LIST command output

Description

Beginning in z/OS V2R2, the output of the **LIST DUMPCLASS** command includes a new MINSTACK value, and the position of the existing STACK value in the output has changed. This new and changed output is displayed when OUTDATASET, SYSOUT (the default), or TERMINAL is specified as the destination for the output.

Table 120 provides more details about this migration action. Use this information to plan your changes to the system.

Table 120. Information about this migration action

Element or feature:	DFSMSHsm
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if your application depends on the output of the LIST DUMPCLASS command.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Remove any dependency on the STACK field location in the **LIST DUMPCLASS** command with a output target of TERM, OUTDATASET, or SYSOUT. Also, update applications as needed for the new MINSTACK field in the **LIST DUMPCLASS** command with a output target of TERM, OUTDATASET, or SYSOUT.

Reference information

For information about the **LIST DUMPCLASS** command, see *z/OS DFSMSHsm Storage Administration*.

DFSMS actions to perform after the first IPL of z/OS V2R2

This topic describes DFSMS migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

DFSMSdfp: Run OAM DB2 BIND jobs

Description

When migrating to any new release of z/OS, you must run OAM DB2 BIND jobs if you are using OAM for object support. The BIND jobs update DB2 with new OAM DB2 code.

Table 121 on page 184 provides more details about this migration action. Use this information to plan your changes to the system.

Migration actions from z/OS V2R1: DFSMS

Table 121. Information about this migration action

Element or feature:	DFSMSsdfp.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use OAM object support.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Run the BIND jobs appropriate to your installation:

1. Update and execute the samplib job CBRPBIND (OAM DB2 Bind Package Job).
2. Do one of the following:
 - If your installation starts OAM, uses the file system sublevel or optical or tape devices, or uses the OAM storage management component (OSMC), do the following:
 - Update and execute samplib job CBRABIND (OAM DB2 Application Plan Bind for LCS and OSR).
 - Update and execute samplib job CBRHBIND (OAM DB2 Application Plan Bind for OSMC).
 - If your installation does not start OAM, use the file system sublevel or optical or tape devices, or use OSMC, update and execute samplib job CBRIBIND (OAM DB2 Application Plan Bind for OSR only).
3. For more information, see the topic on migrating, installing, and customizing OAM in *z/OS DFSMS OAM Planning, Installation, and Storage Administration Guide for Object Support*.

Note: If you choose to edit a previous version of an OAM BIND job, you must incorporate any new changes as described in the header of each samplib OAM BIND job.

Reference information

For more information about OAM, see *z/OS DFSMS OAM Planning, Installation, and Storage Administration Guide for Object Support*.

DFSMSsdfp: Define a security product profile for IDCAMS DCOLLECT exit Description

The EXITNAME parameter of the IDCAMS DCOLLECT command allows you to specify an exit to receive control during DCOLLECT processing. After applying the PTF for APAR OA46062 (which was shipped for z/OS V2R1 and V1R13), you must ensure that the exit name is protected through a FACILITY class profile, and that callers of the exit have the appropriate authorization.

Table 122 on page 185 provides more details about this migration action. Use this information to plan your changes to the system.

Table 122. Information about this migration action

Element or feature:	DFSMSdftp.
When change was introduced:	z/OS V2R1 and z/OS V1R13, both with APAR OA46062 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA46062 applied.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if your installation uses the EXITNAME parameter on the IDCAMS DCOLLECT command.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	If a caller attempts to invoke the exit without the proper authorization, the DCOLLECT command fails with the error message: IDC31811I INSUFFICIENT FACILITY CLASS AUTHORIZATION TO INVOKE <i>exitname</i>
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Define a FACILITY class profile with resource name STGADMIN.IDC.DCOLLECT.*exitname*, where *exitname* is the DCOLLECT EXITNAME parameter value.
If the EXITNAME parameter is not specified, the default name is IDCDCX1. You do not require a FACILITY class profile for the default name IDCDCX1.
- Ensure that callers of the exit have at least READ authority to the FACILITY class resource name. If callers have READ authority to one of the FACILITY class profiles STGADMIN.**, STGADMIN.IDC.**, and STGADMIN.IDC.DCOLLECT.*, no action is needed.

Reference information

For more information, see *z/OS DFSMS Access Method Services Commands* .

DFSORT migration actions

This topic describes migration actions for optional feature DFSORT.

DFSORT actions to perform before installing z/OS V2R2

This topic describes DFSORT migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

DFSORT actions to perform before the first IPL of z/OS V2R2

This topic describes DFSORT migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Migration actions from z/OS V2R1: DFSORT

Update automation for changed DFSORT messages

Description

In z/OS V2R2, the text for some DFSORT messages (ICExxxx) is changed. Text and insert fields have been added, changed, or removed in the messages listed in “Steps to take.” These changes can affect automation programs that examine the text of the messages.

Table 123 provides more details about this migration action. Use this information to plan your changes to the system.

Table 123. Information about this migration action

Element or feature:	DFSORT.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have automation routines that examine the message text of the messages listed in “Steps to take.”
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Update your automation to handle the following DFSORT message changes:

- Text and insert fields have been changed in the following messages to provide new information:
 - ICE099A
 - ICE121A
 - ICE288I

Reference information

For information about the ICE messages, see *z/OS DFSORT Messages, Codes and Diagnosis Guide*.

DFSORT actions to perform after the first IPL of z/OS V2R2

This topic describes DFSORT migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

Distributed File Service migration actions

This topic describes migration actions for base element Distributed File Service.

Distributed File Service actions to perform before installing z/OS V2R2

This topic describes Distributed File Service migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

Distributed File Service actions to perform before the first IPL of z/OS V2R2

This topic describes Distributed File Service migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

None.

Distributed File Service actions to perform after the first IPL of z/OS V2R2

This topic describes Distributed File Service migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

SMB: Add `_BPXK_UNUSEDTASKS=KEEP` to the DFSCNTL environment file Description

Before z/OS V2R2 and without the z/OS UNIX PTF for APAR OA39909, which changed threading behavior, SMB users did not have to specify that medium weight threads were to be kept. As of APAR OA39909 and z/OS V2R2, SMB users must keep the original threading behavior by setting the `_BPXK_UNUSEDTASKS=KEEP` environment variable, as described in DFS SMB APAR OA45175.

Table 124 provides more details about this migration action. Use this information to plan your changes to the system.

Table 124. Information about this migration action

Element or feature:	Server Message Block (SMB) support of the IBM z/OS Distributed File Service base element.
When change was introduced:	z/OS V2R2, and z/OS V1R13 and V2R1 with PTFs for APARs OA39909 and APAR OA43472 installed.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APARs OA39909 and APAR OA43472 installed.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use SMB.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Failure to implement this migration action prevents the DFS/SMB server from starting or restarting because z/OS UNIX System Services issues a SIGKILL to the DFS/SMB server. The following symptoms might be encountered if this migration action is not implemented: DFSKERN S069 422 SA03 BPXP023I IOEP01100I IOEP01123A RESTART SIGKILL or SYSTEM ABEND S069 - REASON CODE 04
Related IBM Health Checker for z/OS check:	None.

Migration actions from z/OS V2R1: Distributed File Service

Steps to take

Because SMB is dependent on the threading model that was in effect before the PTFs for APAR OA39909 and APAR OA43472 were installed, you need to take the following steps:

1. To allow SMB to use the original threading behavior, add the environment variable `_BPXK_UNUSEDTASKS=KEEP` to the SMB DFSCNTL environment file, which is typically found in the `/opt/dfslocal/home/dfscntl/envar` directory.
2. If SMB is started, it must be stopped and restarted using the C DFS and S DFS commands.

After you complete the steps, SMB will use the original threading behavior that was in place prior to the PTF for APAR OA39909.

Reference information

For more information, see the following references:

- *z/OS Distributed File Service SMB Administration*
- *z/OS UNIX System Services Planning*

HCD migration actions

This topic describes migration actions for the base element Hardware Configuration Definition (HCD).

HCD actions to perform before installing z/OS V2R2

This topic describes HCD migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

HCD actions to perform before the first IPL of z/OS V2R2

This topic describes HCD migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

None.

HCD actions to perform after the first IPL of z/OS V2R2

This topic describes HCD migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

HLASM migration actions

This topic describes migration actions for the base element High Level Assembler (HLASM).

HLASM actions to perform before installing z/OS V2R2

This topic describes HLASM migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Accommodate new assembler mnemonics for new machine instructions

Description

IBM z Systems introduced new instructions with mnemonics that might collide with existing macro instruction names. Collisions can be managed by using a different OPTABLE option or mnemonic tag.

Note: HLASM APAR PM79901 provides new hardware support for IBM z13. New instructions have been added to the UNI and ZS7 optables. The ESA vector facility instructions have been removed from the UNI optable. For a complete list of the instructions that are affected, see the technote *New hardware support - APAR PM79901* at the following web site: IBM Support Portal.

Table 125 provides more details about this migration action. Use this information to plan your changes to the system.

Table 125. Information about this migration action

Element or feature:	HLASM
When change was introduced:	z/OS V2R1, z/OS V1R13, and z/OS V1R12, all with hardware support HLASM APARs. Some of the most recent APARs include PM79901, PM49761, and PM86821.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, without hardware support HLASM APARs installed.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you have a collision with a new instruction mnemonic.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Look for possible conflicts between new mnemonics and existing macro instructions with the same name:

1. Assemble an END statement with the OPTABLE(UNI,LIST) option to cause HLASM to display all mnemonics in the UNI opcode table.
2. If a conflicting name appears, do one of the following:
 - Use either a different OPTABLE option to avoid the new mnemonics or mnemonic tags to distinguish machine instruction use from macro instruction use.
 - Change the macro names.

Tip: For a tool to help in identifying mnemonic conflicts, see *Techdoc PRS5289* at the IBM Techdocs website.

Reference information

For more information, see the following references:

- For information about the OPTABLE option, see *HLASM Programmer's Guide*.
- For information about mnemonic tags, see *HLASM Language Reference*.

Migration actions from z/OS V2R1: IBM HLASM

HLASM actions to perform before the first IPL of z/OS V2R2

This topic describes HLASM migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Adjust the block size on assembler SYSLIN when using the HEWLKED linkage editor program

Description

Historically, when a SYSPUNCH or SYSLIN data set is created by HLASM on z/OS and the BLKSIZE parameter is either not specified or specified with a value of 0, HLASM will create a data set which has a BLKSIZE equal to the LRECL value. This is typically not an optimal BLKSIZE value and may result in a poorly performing data set.

By the enhancement of APAR PI10515 (PTF UI15579 for z/OS V2R1, V1R13, and V1R12), HLASM has been modified not to set the default BLKSIZE to LRECL if a block size of zero is supplied for SYSLIN and SYSPUNCH data sets. HLASM will now leave the BLKSIZE as zero to allow DFSMS to determine the block size based upon the its criteria.

Note: When system-determined block sizes (SDBs) are used for SYSLIN data sets, the data set may be created with a larger block size than supported by the HEWLKED linkage editor.

Table 126 provides more details about this migration action. Use this information to plan your changes to the system.

Table 126. Information about this migration action

Element or feature:	HLASM.
When change was introduced:	z/OS V2R1 and z/OS V1R13, both with APAR PI10515 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR PI10515 applied.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you invoke the linkage editor (HEWLKED) rather than the Binder (IEWBLINK) and will be affected by the block size selection as described.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

When you invoke the linkage editor (HEWLKED) rather than the Binder (IEWBLINK), the maximum block size of data sets defined in the SYSLIN definition is 3200 bytes. After the HLASM APAR PI10515 (PTF UI15579), when the BLKSIZE is not supplied to the SYSLIN data set in the ASM step, it is created with large block size (for example, 27920) by the SDB. The old linkage editor does not accept the block size larger than 3200, which results in the following error message:

```
CC16.IEW0594 ERROR - INPUT DATA SET BLOCKSIZE IS INVALID
```

To avoid using SDB when invoking the HEWLKED linkage editor, you need to supply a BLKSIZE of 3200 or less (which is a multiple of the LRECL) in the SYSLIN data set in ASM step.

Reference information

For more information, see the following references:

- PTF UI15579 and DOC APAR PI19003.
- PSP Bucket (Upgrade HLASM160, Subset HMQ4160).
- For more information on HEWLKED, see *z/OS MVS Program Management: User's Guide and Reference* .
- For more information on system-determined block sizes, see *z/OS DFSMS Using Data Sets* .
- For more information on assembler data set characteristics, see *HLASM Programmer's Guide* .

HLASM actions to perform after the first IPL of z/OS V2R2

This topic describes HLASM migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

IBM HTTP Server migration actions

This topic describes migration actions for base element IBM HTTP Server.

IBM HTTP Server actions to perform before installing z/OS V2R2

This topic describes IBM HTTP Server migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Plan for the removal of IBM HTTP Server powered by Domino Description

z/OS V2R1 was the last release to include the IBM HTTP Server powered by Domino. New base element, IBM HTTP Server - Powered by Apache (IHSA), is introduced in z/OS V2R2. This element replaces IBM HTTP Server powered by Domino. z/OS V2R2 contains IHSA at level 9.0.

If your installation is using IBM HTTP Server powered by Domino, you must migrate to IBM HTTP Server - Powered by Apache. It is strongly recommended that you perform this migration in two phases, as described in "Steps to take" on page 192. Both IBM HTTP Server - Powered by Apache 8.5.5 and IBM HTTP Server - Powered by Apache 9.0 are supported on z/OS V2R2. Note, however, that IBM HTTP Server - Powered by Apache 8.5.5 support on z/OS V2R2 is planned to continue only until the end of service date for z/OS V2R1 (planned for September 2018).

IBM HTTP Server powered by Domino is not supported on z/OS V2R2.

Table 127 provides more details about this migration action. Use this information to plan your changes to the system.

Table 127. Information about this migration action

Element or feature:	IBM HTTP Server powered by Domino.
When change was introduced:	z/OS V2R2. This change was also announced in the statement of direction <i>IBM United States Software Announcement 213-292 "IBM z/OS Version 2 Release 1 delivers the foundation for Smarter Computing,"</i> dated July 23, 2013.

Migration actions from z/OS V2R1: IBM HTTP Server

Table 127. Information about this migration action (continued)

Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you currently use IBM HTTP Server powered by Domino.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	The HTTP servers that are included in other IBM licensed programs, such as WebSphere Application Server, are not affected. This migration action applies only to users of the IBM HTTP Server that is included in the base z/OS operating system.
Related IBM Health Checker for z/OS check:	<p>The check IBMZMIG,ZOSMIG_HTTP_SERVER_DOMINO is used to determine whether IBM HTTP Server powered by Domino is in use on your system. The check is written in REXX and is provided on an as-is basis at http://www.ibm.com/systems/z/os/zos/installation/HTTP_Health_Checker.html.</p> <p>The check is not provided in an APAR; for instructions on adding it to your system, see the web page.</p>

Steps to take

In z/OS V2R2, you must migrate to IBM HTTP Server - Powered by Apache, which is included as a base element of z/OS. It is recommended that you perform this migration in two phases, as follows:

1. Before you install z/OS V2R2, use the separate licensed program z/OS Ported Tools HTTP Server feature (5655-M23) on z/OS V2R1 or z/OS V1R13. You can run the IBM Ported Tools HTTP Server and the IBM HTTP Server powered by Domino concurrently, if necessary, for certain functions that do not support the IBM Ported Tools HTTP Server on z/OS V2R1 or z/OS V1R13, such as Infoprint Server at those release levels (see "Infoprint migration action for HTTP Server").

In this phase of the migration, you can perform much of the migration work for z/OS V2R2 IBM HTTP Server in advance and stabilize on IBM HTTP Server - Powered by Apache. The z/OS Ported Tools HTTP Server feature is at level 8.5.5 (Apache V2.2.8 level).

2. After you install z/OS V2R2, migrate from z/OS Ported Tools HTTP Server feature to z/OS V2R2 IBM HTTP Server - Powered by Apache. In z/OS V2R2, IBM HTTP Server - Powered by Apache is at the 9.0 level (based on Apache V2.4). Here, you need only to perform the migration actions between IBM HTTP Server 8.5.5 and 9.0, which are fewer than the number of migration actions that are needed to move from IBM HTTP Server powered by Domino directly to IBM HTTP Server - Powered by Apache at the 9.0 level.

Note: To avoid an error (condition code 0137 and ABENDU4093 RC00000281) ensure that REGION=0M is specified on the EXEC statement of the IBM HTTP Server started procedure. APAR PI47828 (Apache 8.5.5) and APAR PI50373 (Apache 9.0) updates the sample procedure to specify REGION=0M and TIME=NOLIMIT.

Reference information

For more information, see the following references:

- For information about supported versions of IBM HTTP Server, see Washington Systems Center flash 10857 at <http://www.ibm.com/support/techdocs>. Search for "flash10857".
- For instructions on migrating from IBM HTTP Server powered by Domino to IBM HTTP Server - Powered by Apache, see IBM Redbook "IBM HTTP Server on z/OS: Migrating from Domino-powered to Apache-powered", REDP-4987.
- For instructions on migrating from IBM HTTP Server - Powered by Apache 8.5.5 to 9.0, see <http://httpd.apache.org/docs/2.4/upgrading.html>.

IBM HTTP Server actions to perform before the first IPL of z/OS V2R2

This topic describes IBM HTTP Server migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

None.

IBM HTTP Server actions to perform after the first IPL of z/OS V2R2

This topic describes IBM HTTP Server migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

IBM Tivoli Directory Server migration actions

This topic describes migration actions for the base element IBM Tivoli Directory Server.

IBM Tivoli Directory Server actions to perform before installing z/OS V2R2

This topic describes IBM Tivoli Directory Server migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Accommodate new sslCipherSpecs default Description

Starting in z/OS V2R2, z/OS IBM Tivoli® Directory Server changed its default setting for the LDAP server **sslCipherSpecs** configuration file option. This configuration option specifies the accepted cipher suites that are used in SSL/TLS secure connections. The **sslCipherSpecs** configuration file option can be specified in various ways as an arithmetic expression that represents a mask, including decimal values, hexadecimal values, or keywords that are included or excluded in combination with the **ANY** keyword.

If the LDAP server uses SSL/TLS secure connections and the **sslCipherSpecs** configuration option is not specified in the LDAP server configuration file, the default enabled ciphers no longer include the RSA-EXPORT or RC4 ciphers "03", "04", "05", or "06".

These ciphers are specified in the **sslCipherSpecs** configuration file option individually in numeric or keyword form as follows:

Table 128. SSL ciphers supported by the sslCipherSpecs configuration option

SSL Cipher	LDAP Server keyword	Decimal value	Hexadecimal value	Description
"03"	RC4_MD5_EXPORT	8192	x00002000	40-bit RC4 encryption with MD5 message authentication and RSA key exchange.

Migration actions from z/OS V2R1: IBM Tivoli Directory Server

Table 128. SSL ciphers supported by the `sslCipherSpecs` configuration option (continued)

SSL Cipher	LDAP Server keyword	Decimal value	Hexadecimal value	Description
"04"	RC4_MD5_US	2048	x00000800	128-bit RC4 encryption with MD5 message authentication and RSA key exchange.
"05"	RC4_SHA_US	1024	x00000800	128-bit RC4 encryption with SHA-1 message authentication and RSA key exchange.
"06"	RC2_MD5_EXPORT	4096	x00001000	40-bit RC2 encryption with MD5 message authentication and RSA key exchange.

Table 129 provides more details about this migration action. Use this information to plan your changes to the system.

Table 129. Information about this migration action

Element or feature:	z/OS IBM Tivoli Directory Server.
When change was introduced:	z/OS V2R2. z/OS V2R1 and z/OS V1R13, both with APAR OA47491.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA47491.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you are using SSL/TLS secure connections.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	LDAP SSL/TLS secure connections might fail if a client application is relying on one of the defined default ciphers and it is no longer enabled.
Related IBM Health Checker for z/OS check:	None.

Steps to take

These ciphers are also included when the `sslCipherSpecs` configuration file option is specified as **ANY**. The `sslCipherSpecs` configuration file option includes 24 different ciphers in the **ANY** keyword.

For a complete description of the `sslCipherSpecs` configuration file option, see *Setting up the security options, and SSL ciphers supported by the sslCipherSpecs configuration option in z/OS IBM Tivoli Directory Server Administration and Use for z/OS*.

In z/OS V2R2, z/OS IBM Tivoli Directory Server has changed its default setting for the LDAP server `sslCipherSpecs` configuration file option from **ANY** to **ANY-RC4_MD5_EXPORT-RC4_MD5_US-RC4_SHA_US-RC2_MD5_EXPORT**. If you currently omit the `sslCipherSpecs` configuration file option and want to continue accepting all ciphers included in the **ANY** keyword, specify `sslCipherSpecs ANY` in the general section of the LDAP server configuration file. Consider determining the actual set of ciphers that are needed and specify the appropriate value for the `sslCipherSpecs` configuration file option.

Reference information

For more information, see *z/OS IBM Tivoli Directory Server Administration and Use for z/OS*.

IBM Tivoli Directory Server actions to perform before the first IPL of z/OS V2R2

This topic describes IBM Tivoli Directory Server migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

None.

IBM Tivoli Directory Server actions to perform after the first IPL of z/OS V2R2

This topic describes IBM Tivoli Directory Server migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

IBM z/OS Management Facility migration actions

This topic describes migration actions for the base element IBM z/OS Management Facility (z/OSMF).

z/OSMF actions to perform before installing z/OS V2R2

This topic describes z/OSMF migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

z/OSMF actions to perform before the first IPL of z/OS V2R2

This topic describes z/OSMF migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

None.

z/OSMF actions to perform after the first IPL of z/OS V2R2

This topic describes z/OSMF migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

Migrate to the new release of z/OSMF Description

As in previous releases, migrating to the new release of z/OSMF includes running the script **izumigrate.sh**. In z/OS V2R2, this script is enhanced to create a customized IZUPRMxx parmlib member, based on the configuration settings from your current (old) system. The parmlib member replaces the interactive scripts that you used to configure z/OSMF in previous releases.

Table 130 on page 196 provides more details about this migration action. Use this information to plan your changes to the system.

Migration actions from z/OS V2R1: z/OSMF

Table 130. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	z/OSMF plug-ins and applications might have requirements for specific software. See each plug-in or application for its requirements.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

For ServerPac users, use the jobs and documentation supplied with your ServerPac order to create an initial instance of z/OSMF. Installations that install z/OSMF from a Custom-Built Product Delivery Option (CBPDO) software delivery package, or from a ServerPac order using the software upgrade method of installation, should follow the instructions in the migration chapter in *IBM z/OS Management Facility Configuration Guide*. This work includes running the **izumigrate.sh** script on the z/OS V2R2 system.

After you complete the ServerPac installation, you can add plug-ins to z/OSMF through the Configuration Workflow, as described in *IBM z/OS Management Facility Configuration Guide*.

Reference information

For more information, see the following references:

- For information about the ServerPac post-install jobs, see *ServerPac: Installing Your Order*.
- For information about configuring z/OSMF, see *IBM z/OS Management Facility Configuration Guide*.

Remove the most-generic profile for z/OSMF authorizations

Description

In previous releases of z/OSMF, the generated program **izuconfig1.cfg.rexx** included RACF commands for defining the following generic profile in the ZMFAPLA class, and for creating permissions to it:

```
<SAF-prefix>.ZOSMF.**
```

where *<SAF-prefix>* is the SAF profile prefix that was defined for your configuration (by default, IZUDFLT). If you used **izuconfig1.cfg.rexx** in a previous release, this generic profile was created for your configuration.

As of z/OS V2R2, the z/OSMF configuration process no longer creates authorizations based on this most-generic profile. Instead, authorizations are now created based on the following discrete generic profile:

```
<SAF-prefix>.ZOSMF
```

In this release, a sample job is provided in SYS1.SAMPLIB(IZUSEC) to help you create the resource names and security authorizations for z/OSMF. Your security administrator can edit and run this job to secure various resources on the z/OS system.

For the profiles and permissions that are created, see the contents of the IZUSEC sample job.

Table 131 provides more details about this migration action. Use this information to plan your changes to the system.

Table 131. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OSMF V2R1 with APAR PI20091 applied.
Applies to migration from:	z/OSMF V2R1 without APAR PI20091 applied, and z/OSMF V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have used a generic profile and want to use discrete profiles for more granular control.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	The older generic profiles still work, but you do not have the granularity of more discrete profiles, which provide better control over access to specific resources.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Create the discrete profiles that you need for z/OSMF. In a RACF installation, you can use the commands in job IZUSEC to define profiles and create authorizations.
2. Ensure that your existing user authorizations are converted to user authorizations based on the discrete profiles. To preserve your existing authorizations, you can copy the access list from an existing profile into another existing profile, using the FROM operand on the **PERMIT** command.
3. Remove the most-generic profile for z/OSMF authorizations. In a RACF installation, you can use the following commands to remove the generic profile:

```
RDELETE ZMFAPLA IZUDFLT.ZOSMF.**
SETROPTS RACLIST(ZMFAPLA) REFRESH
```

Reference information

For a list of the authorizations required in z/OSMF, see *IBM z/OS Management Facility Configuration Guide*.

Recreate all table filters in the z/OSMF user interface

Description

To display a subset of the items in a table in the IBM z/OS Management Facility (z/OSMF) user interface, you must define filter rules that show only the items in which you are interested. Before z/OS V2R2, the filter rules you set were saved and reapplied for subsequent views of the table. Starting with z/OS V2R2, z/OSMF provides a modern, intuitive interface that is consistent with other IBM products. The enhanced user interface does not support the filter rules that were preserved in previous z/OSMF

Migration actions from z/OS V2R1: z/OSMF

releases; therefore, when you display a table in z/OSMF V2R2, you might see more data or different data than you are accustomed to seeing. To show only the items in which you are interested, recreate the filter rules you set in previous releases of z/OSMF.

Table 132 provides more details about this migration action. Use this information to plan your changes to the system.

Table 132. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OS V2R2
Applies to migration from:	z/OSMF V2R1 and z/OSMF V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if users want to view only a subset of the data included in a table.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Log into the z/OSMF V2R2 user interface.
2. Navigate to the tables for which you previously set filters.
3. In the filter row in the table, click the *Filter* link. The Build Filter window is displayed.
4. In the columns field (the first field), select the name of the column to be filtered, if needed. This field lists all the columns in the table that are visible and filterable, and it includes an *Any Column* option so that you can apply the filter rule to any column in the table.
5. In the filter condition field (the second field), select the filter condition.
6. In the value field, select or specify the value for which to filter. All the fields that follow the filter condition field are value fields. The number of value fields displayed depends on the type of data being filtered and the filter condition. If a value field is enabled, a value is required.
To filter a single column for multiple values, create a separate filter rule for each value.
7. To create additional rules, click the add filter rule icon -- a plus (+) sign -- and specify the column, condition, and value for the new rule.
8. To remove a rule, click the remove rule icon -- a minus (-) sign. If the remove rule icon is disabled, the rule cannot be removed.
9. If you specified more than one filter rule, in the **Match** field, indicate whether all the rules (**All rules**) or at least one rule (**Any rule**) must be satisfied for an item to be displayed in the table. By default, **All rules** is selected.
If the **Match** field is disabled (grayed out), you cannot change the relationship between the rules. In this case, all rules must be satisfied.
10. If you want the filter criteria to be case sensitive for all the rules you specified, select **Match case**. Otherwise, case is ignored.
11. Click **Filter** to filter the table.

Reference information

For more information, see the following references:

- For information about configuring z/OSMF, see *IBM z/OS Management Facility Configuration Guide*.
- For information about z/OSMF tables, see the *Getting Started with z/OSMF* section in the help system that is shipped with z/OSMF.

ICKDSF (Device Support Facility)

This topic describes migration actions for the base element ICKDSF (Device Support Facility).

ICKDSF actions to perform before installing z/OS V2R2

This topic describes ICKDSF migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

ICKDSF actions to perform before the first IPL of z/OS V2R2

This topic describes ICKDSF migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

None.

ICKDSF actions to perform after the first IPL of z/OS V2R2

This topic describes ICKDSF migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

ICKDSF: Accommodate new default for INIT and REFORMAT commands

Description

The VERIFYOFFLINE parameter of the INIT and REFORMAT commands verifies that the device is offline to all other systems before the command is attempted. Beginning with ICKDSF APAR PI25913, if the UNIT parameter is specified for the INIT or REFORMAT command, and the required storage control microcode support and software support exists, and the device is not a minidisk, the VERIFYOFFLINE parameter is the default, meaning that verification that the device is offline occurs even if VERIFYOFFLINE is not specified. Prior to ICKDSF APAR PI25913, verification occurred only when VERIFYOFFLINE was specified.

If the VERIFYOFFLINE parameter is processed as the default, and the device is online to another system, the command terminates, with message ICK31306I in the job output.

To request that verification not take place, you can use a new NOVERIFYOFFLINE parameter.

Note: The VERIFYOFFLINE parameter of the INIT and REFORMAT commands was introduced by ICKDSF APAR PM76231

Table 133 provides more details about this migration action. Use this information to plan your changes to the system.

Table 133. Information about this migration action

Element or feature:	ICKDSF
---------------------	--------

Migration actions from z/OS V2R1: ICKDSF

Table 133. Information about this migration action (continued)

When change was introduced:	APAR PI25913 (on ICKDSF R17) for both z/OS V2R1 and z/OS V1R13.
Applies to migration from:	z/OS V2R1 and z/OS V1R13 (on ICKDSF R17), both without APAR PI25913.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you require that the new default not be used.
Target system hardware requirements:	DS8870 R7.1 GA, Bundle 87.10.87.0, LIC 7.7.10.287 DS8700 R6.3 SP6, Bundle 76.31.79.0, LIC 6.6.31.670 DS8800 R6.3 SP6, Bundle 86.31.95.0, LIC 7.6.31.1150
Target system software requirements:	The software support is provided in APAR OA40719 for z/OS V2R1 and V1R13, and incorporated into z/OS V2R2.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	If the VERIFYOFFLINE parameter is specified either explicitly or by default, and the device is online to any other systems, message ICK31306I VERIFICATION FAILED: DEVICE FOUND TO BE GROUPED is issued and the command is terminated. If the NOVERIFYOFFLINE parameter is specified and the device is online, command processing continues.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you do not want INIT and REFORMAT commands with the UNIT parameter to verify that the device is offline to all other systems before the command is attempted, add the new NOVERIFYOFFLINE parameter to those commands.

Reference information

For more information, see the descriptions of the INIT and REFORMAT commands in *Device Support Facilities (ICKDSF) User's Guide and Reference*.

Infoprint Server migration actions

This topic describes migration actions for optional feature Infoprint Server.

Infoprint Server actions to perform before installing z/OS V2R2

This topic describes Infoprint Server migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Discontinue use of the Infoprint Server SNMP subagent Description

In z/OS V2R2, the Simple Network Management Protocol (SNMP) subagent is no longer provided with Infoprint Server, so you must take steps to stop using it. The SNMP subagent lets network management systems (such as Ricoh Network Printer Manager for the web) communicate with PSF-controlled printers that do not have internal SNMP agents. However, because most newer printers contain internal SNMP agents, network management systems can communicate directly with these printers.

Migration actions from z/OS V2R1: Infoprint Server

As an alternative to using a network management system to monitor PSF-controlled printers, you can use Infoprint Central, a web-based print management system. Infoprint Central can display the status of all your PSF-controlled printers. In addition, Infoprint Central lets you stop and start the printers, change printer work-selection criteria, and turn TCP/IP-connected printers online and offline.

Table 134 provides more details about this migration action. Use this information to plan your changes to the system.

Table 134. Information about this migration action

Element or feature:	z/OS Infoprint Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use the SNMP subagent. You are using the SNMP subagent if the start-daemons={snmpd} attribute is specified in the Infoprint Server configuration file. The configuration file's default location is <code>/etc/Printsrv/aopd.conf</code> . However, you might have specified a different location in environment variable AOPCONF in the aopstart EXEC.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. If you use a network management system to monitor PSF-controlled printers, do one of these:
 - Configure the network management system to communicate with the printers directly.
 - Use Infoprint Central to manage the printers. To use Infoprint Central, you must customize PSF to use the Infoprint Server Printer Inventory.
2. Stop the SNMP subagent daemon:
 - a. (Optional) Edit the Infoprint Server configuration file (`aopd.conf`) to remove the **snmp** value from the **start-daemons** attribute. This step is optional because Infoprint Server will ignore the **snmp** value.
 - b. If Infoprint Server is running, stop the SNMP subagent daemon (**aopsnmpd**). For example, enter this MVS START command to run the AOPSTOP procedure to stop daemon **aopsnmpd**:

```
START AOPSTOP,OPTIONS='-d snmpd'
```

Reference information

For more information, see the following references:

- How to edit the Infoprint Server configuration file (`aopd.conf`) and how to customize Infoprint Central, see *z/OS Infoprint Server Customization*.
- How to use Infoprint Central and how to stop Infoprint Server daemons, see *z/OS Infoprint Server Operation and Administration*.

Migration actions from z/OS V2R1: Infoprint Server

Upgrade web browser support for Infoprint Central Description

In z/OS V2R2, the Infoprint Central component of Infoprint Server requires Microsoft Internet Explorer 9.0 or later or Mozilla Firefox 24 ESR or later.

Table 135 provides more details about this migration action. Use this information to plan your changes to the system.

Table 135. Information about this migration action

Element or feature:	z/OS Infoprint Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use Infoprint Central.
Target system hardware requirements:	None.
Target system software requirements:	If you use Infoprint Central to work with IP PrintWay™ extended mode print jobs and printers, you need: <ul style="list-style-type: none">• IBM HTTP Server - Powered by Apache base element of z/OS• The XML Toolkit for z/OS V1.10 (5655-J51)• One of these Java products:<ul style="list-style-type: none">– IBM 31-bit SDK for z/OS, Java Technology Edition, V7.1 (5655-W43)– IBM 64-bit SDK for z/OS, Java Technology Edition, V7.1 (5655-W44)• Microsoft Internet Explorer 9.0 or later or Mozilla Firefox 24 ESR or later
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Install Microsoft Internet Explorer 9.0 or later, or Mozilla Firefox 24 ESR or later.

Reference information

For more information, see *z/OS Infoprint Server Operation and Administration* describes how to start and stop Infoprint Server and how to use Infoprint Central.

Upgrade Java support for IPP Server and Infoprint Central Description

In z/OS V2R2, the Internet Printing Protocol (IPP) Server used in Infoprint Server and Infoprint Central require Java V7.1. If the JAVA_HOME environment variable specifies the location of an earlier version of Java, you must update the JAVA_HOME environment variable.

Table 136 on page 203 provides more details about this migration action. Use this information to plan your changes to the system.

Table 136. Information about this migration action

Element or feature:	z/OS Infoprint Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use IPP Server or Infoprint Central and specify the JAVA_HOME environment variable. You are using IPP Server if start-daemons={ippd} is specified in the Infoprint Server configuration file. You are using Infoprint Central if the start-daemons={ssid} attribute is specified in the Infoprint Server configuration file. The configuration file's default location is /etc/Printsrv/aopd.conf. However, you might have specified a different location in environment variable AOPCONF.
Target system hardware requirements:	None.
Target system software requirements:	IBM 31-bit SDK for z/OS, Java Technology Edition, V7.1 (5655-W43); Infoprint Central can also use IBM 64-bit SDK for z/OS, Java Technology Edition, V7.1 (5655-W44).
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	z/OS V2R1 and V1R13 Infoprint Server will not operate with IBM HTTP Server - Powered by Apache. After you install z/OS V2R2, you must change the configuration of the z/OS V2R2 Infoprint Server to operate with IBM HTTP Server - Powered by Apache, which is included in z/OS V2R2 as a base element.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Install IBM 31-bit SDK for z/OS, Java Technology Edition, V7.1 (5655-W43) or IBM 64-bit SDK for z/OS, Java Technology Edition, V7.1 (5655-W44). IPP Server requires the 31-bit version of Java V7.1.
2. If you use the IPP Server, edit the **aopstart** EXEC to update the directory path specified in the JAVA_HOME environment variable to /usr/lpp/java/J7.1 or wherever you specified the location.

Note: If you installed Java V7.1 in the default Java directories, you do not need to specify the JAVA_HOME environment variable. If JAVA_HOME is not specified, IPP Server or Infoprint Central looks for Java files in the /usr/lpp/java/J7.1 directory.

Reference information

For more information, see the following references:

- For information about editing the **aopstart** EXEC, see *z/OS Infoprint Server Customization*.
- For information about Java products, see the Java Standard Edition Products on z/OS page: <http://www.ibm.com/systems/z/os/zos/tools/java/>.

Migration actions from z/OS V2R1: Infoprint Server

Infoprint Server actions to perform before the first IPL of z/OS V2R2

This topic describes Infoprint Server migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Discontinue use of Infoprint Server **aophinvd**, **aoplogd**, and **aopsdbd** daemons

Description

In z/OS V2R2, the following daemons are no longer provided with Infoprint Server:

aophinvd

Historical Inventory daemon.

aoplogd

Common message log daemon.

aopsdbd

Search database daemon.

The functions that are previously provided by the **aophinvd**, **aoplogd**, and **aopsdbd** daemons are now performed by the **aopd** daemon. You do not need to take any steps to update your Infoprint Server configuration. However, if you use an automation product to monitor daemons, you might need to make configuration changes to the product.

Table 137 provides more details about this migration action. Use this information to plan your changes to the system.

Table 137. Information about this migration action

Element or feature:	z/OS Infoprint Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use an automation product that monitors the aophinvd , aoplogd , and aopsdbd daemons, you need to make configuration changes for the product.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	You might see an increase in CPU consumption for the aopd daemon because it now handles additional workload from the removed daemons.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you use an automation product that monitors the **aophinvd**, **aoplogd**, and **aopsdbd** daemons, remove the daemons from your product configuration.

Reference information

For more information, see the following references:

- *z/OS Infoprint Server Customization*.

- *z/OS Infoprint Server Operation and Administration.*
- *z/OS Infoprint Server Printer Inventory for PSF.*

Remount the Printer Inventory and copy files that were customized

Description

When you migrate to the latest z/OS system, you must bring forward the customized data from your previous system.

Table 138 provides more details about this migration action. Use this information to plan your changes to the system.

Table 138. Information about this migration action

Element or feature:	z/OS Infoprint Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

aopstart EXEC

If you modified the **aopstart EXEC**, copy it to the z/OS V2R2 system.

Configuration file

If you are using the ServerPac Full System Replace option and you have modified the Infoprint Server configuration file, copy the file to the z/OS V2R2 system. Its default location is `/etc/Printsrv/aopd.conf`. However, you might have specified a different location in environment variable `AOPCONF`.

Infoprint Central

When you are customizing the new script **bin/envvars** for IBM HTTP Server - Powered by Apache, you might want to refer to the old z/OS HTTP Server environment variables file as a reference. By default, the file was located at `/etc/httpd.envvars`.

IP PrintWay

If you currently use the IP PrintWay component of Infoprint Server, copy to the z/OS V2R2 system any IP PrintWay exit routines and data stream filters you have written. It is a good practice to recompile the exits and filters on z/OS V2R2.

NetSpool

If you currently use the NetSpool component of Infoprint Server, copy to the z/OS V2R2 system any NetSpool exit routines you have written. It is a good practice to recompile the exits and filters on z/OS V2R2.

Printer Inventory

Migration actions from z/OS V2R1: Infoprint Server

- Remount the /var/Printsrv directory from the earlier system on the z/OS V2R2 system. The /var/Printsrv directory contains the Printer Inventory as well as other Infoprint Server files. The default directory is /var/Printsrv. However, you might have changed the directory name in the base-directory attribute in the aopd.conf configuration file.

Notes:

1. After you start Infoprint Server on the z/OS system, you should use the Infoprint Server **pidu** command to export the Printer Inventory on the z/OS V2R2 system so that you have a backup of the Printer Inventory.
 2. If /var/Printsrv is not mounted at a separate mount point, use the Infoprint Server **pidu** command to export the Printer Inventory on the original system; restore it on the z/OS V2R2 system after the first IPL. Do not use other copy commands to copy the Printer Inventory. (Mounting /var/Printsrv at a separate mount point can result in better management of disk space and easier migration.)
- Configure the Infoprint Server environment variables (for example, AOPCONF, PATH, LIBPATH, NLSPATH, MANPATH) in /etc/profile.

Print Interface

If you currently use the Print Interface component of Infoprint Server, take these actions:

- If you have written any data stream filters, copy them to the z/OS V2R2 system. You do not need to recompile them.
- If you run the SAP R/3 application server on the z/OS system, copy the SAP callback daemon configuration file to the z/OS V2R2 system. Its default location is /etc/Printsrv/aopsapd.conf. However, you might have specified a different location in environment variable AOPSAPD_CONF.

Reference information

For more information, see *z/OS Infoprint Server Customization*.

Infoprint Server actions to perform after the first IPL of z/OS V2R2

This topic describes Infoprint Server migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

Run aopsetup

Description

When migrating to z/OS V2R2 Infoprint Server, you must run the **aopsetup** shell script to establish the correct file permissions for Infoprint Server directories and files.

Table 139 provides more details about this migration action. Use this information to plan your changes to the system.

Table 139. Information about this migration action

Element or feature:	z/OS Infoprint Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.

Table 139. Information about this migration action (continued)

Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Run the **aopsetup** shell script from an **rlogin** shell, from an OMVS session, or with the BPXBATCH command. Specify the names of the RACF groups that you defined for Infoprint Server operators and administrators as arguments to **aopsetup**. For example, if you defined group AOPOPER for operators and group AOPADMIN for administrators, enter:

```
/usr/lpp/Printsrv/bin/aopsetup AOPOPER AOPADMIN
```

Rule: You must run **aopsetup** from a user ID with a UID of 0. You can use the **su** command to switch to an effective UID of 0 if you have READ access to the BPX.SUPERUSER profile in the RACF FACILITY class.

Tip: You can run **aopsetup** from the driving system (instead of the target system) if all of these are true:

- You have the target system's /var/Printsrv directory accessible.
- You reference the target system's /usr/lpp/Printsrv directory mounted under a /service directory as described in the comments at the beginning of the **aopsetup** shell script.
- The RACF database groups for operators and administrators are the same on the driving and target system.

Reference information

For information about running **aopsetup**, see *z/OS Infoprint Server Customization*.

Configure IBM HTTP Server - Powered by Apache Description

In z/OS V2R1 and earlier versions, the Infoprint Central component of Infoprint Server was designed to work only with the IBM HTTP Server powered by Domino®. In z/OS V2R2, IBM removed support for IBM HTTP Server powered by Domino and only IBM HTTP Server - Powered by Apache, a base element of z/OS V2R2, is supported. You must now use the IBM HTTP Server powered by Apache 31-bit.

Table 140 provides more details about this migration action. Use this information to plan your changes to the system.

Table 140. Information about this migration action

Element or feature:	z/OS Infoprint Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use the Infoprint Central component of Infoprint Server. You are using Infoprint Central if start-daemons={ssid} is specified in the Infoprint Server configuration file, which has a default location of /etc/Printsrv/aopd.conf. However, you might have specified a different location in environment variable AOPCONF in the aopstart EXEC.
Target system hardware requirements:	None.

Migration actions from z/OS V2R1: Infoprint Server

Table 140. Information about this migration action (continued)

Target system software requirements:	IBM HTTP Server - Powered by Apache.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

See “Customizing IBM HTTP Server - Powered by Apache” in *z/OS Infoprint Server Customization*.

Reference information

For information about how to configure Infoprint Server and Infoprint Central, see *z/OS Infoprint Server Customization*.

JES2 migration actions

This topic describes migration actions for base element JES2.

JES2 actions to perform before installing z/OS V2R2

This topic describes JES2 migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Activate z11 mode

Description

JES2 z/OS V2R1 is the last release level that will support z2 checkpoint mode. JES2 must be activated to z11 mode before migrating to z/OS V2R2. Activating z11 mode upgrades the JES2 checkpoint and enables JES2 function that is introduced in z/OS V1R11, including JOE data area extensions supported by BERTs. For more information on the JES2 functionality introduced in z/OS V1R11, see “Reference information” on page 209.

Table 141 provides more details about this migration action. Use this information to plan your changes to the system.

Table 141. Information about this migration action

Element or feature:	JES2.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	You are able to fall back to z2 mode, if necessary, prior to z/OS V2R2. After z/OS V2R2, you cannot fall back to z2 mode.
System impacts:	None.

Table 141. Information about this migration action (continued)

Related IBM Health Checker for z/OS check:	Use check JES2_Z11_Upgrade_CK_JES2 to determine if your system is ready to upgrade the JES2 checkpoint to z11 mode. For more information, see <i>IBM Health Checker for z/OS User's Guide</i> .
--	---

Steps to take

Follow these steps:

- After migrating to z/OS V1R11 JES2, or later, on all systems in your MAS, determine your z11 checkpoint activation readiness:
 1. Use the **\$D ACTIVATE** command. This command indicates if activation to z11 mode will succeed.
 2. Review your current utilization of BERT data to determine if there are sufficient BERTS, as detailed in "Check BERT utilization."
 3. If you issue the **\$ACTIVATE,LEVEL=z11** command, activation of LARGEDS support is required.
 4. An additional *mmm* 4K records for CKPT1 is required for z11 mode.
- Run the **JES2 \$ACTIVATE** command to verify non-configuration changes that must be accommodated before going to z11, and to activate z11 mode following the considerations for this command found in *z/OS JES2 Commands*.

Note: The SPOOLDEF LARGEDS=FAIL (default value) in JES2PARM parmlib member is not supported in z11 mode. In z11 mode, on a COLD start, JES2 defaults to LARGEDS=ALLOWED. However, you cannot issue the **\$ACTIVATE,LEVEL=z11** command in the environment of SPOOLDEF LARGEDS=FAIL.

By default, JES2 V1R13 and V2R1 restart in the same mode (z2 or z11) as other members of the MAS (if any are active) or the mode the last active JES2 member was in when it came down. To restart JES2 in z2 mode, specify UNACT on PARM=. On a cold start, JES2 starts in z11 mode unless overridden by OPTSDEF COLD_START_MODE or UNACT parameter.

Reference information

For more information, see the following references:

- For a list of the enhancements introduced in z/OS V1R11 for z11 mode, see *z/OS Introduction and Release Guide*.
- For **\$ACTIVATE**, **\$D ACTIVATE**, **\$D CKPTSPACE** and **\$JD HISTORY** command details, see *z/OS JES2 Commands*.

Check BERT utilization: Before issuing the **\$ACTIVATE,LEVEL=z11** command, review the current utilization of BERT data to determine whether there are sufficient BERTs. Additional BERTs are needed for each SYSOUT data set that has transaction data associated with it. These SYSOUT data sets can be seen using SDSF by setting APPC ON and examining SYSOUT data sets on the H and O panels; SYSOUT data sets with transaction data have nontraditional JES2 job IDs. Consider increasing the number of BERTs to correspond to two times the maximum number of transaction SYSOUT data sets on the system. BERT utilization should be monitored after the **\$ACTIVATE** to z11 mode to ensure there are sufficient BERTs for the jobs and SYSOUT in the MAS. There are several ways to determine your current BERT usage.

- The **\$D CKPTSPACE,BERTUSE** command displays a table of the types of control blocks in BERTs and how many BERTs are used by each control block type. The example shows the output of the command:

```

$HASP852 CKPTSPACE  CURRENT BERT UTILIZATION
$HASP852          TYPE          COUNT  CB COUNT
$HASP852          -----  -----
$HASP852          INTERNAL          11          1

```

Migration actions from z/OS V2R1: JES2

\$HASP852	JQE	211	108
\$HASP852	CAT	114	38
\$HASP852	WSCQ	1	1
\$HASP852	DJBQ	0	0
\$HASP852	JOE	0	0
\$HASP852	FREE	763	0

In the example, there are 108 JQEs that have a total of 211 BERTs associated with them. This example is for a system in z2 mode and does not have any BERTs associated with JOEs.

- The \$D ACTIVATE command displays the number of BERTs that are needed for activation to z11 mode. This is the number of BERTs that will be associated with JOEs after the \$ACTIVATE. The example shows the output of the \$D ACTIVATE command:

```
$HASP895 $DACTIVATE
$HASP895 JES2 CHECKPOINT MODE IS CURRENTLY Z2
$HASP895 THE CURRENT CHECKPOINT:
$HASP895 -- CONTAINS 1100 BERTS AND BERT UTILIZATION IS 30
$HASP895 PERCENT.
$HASP895 -- CONTAINS 158 4K RECORDS.
$HASP895 z11 CHECKPOINT MODE ACTIVATION WILL:
$HASP895 -- EXPAND CHECKPOINT SIZE TO 165 4K RECORDS.
$HASP895 -- REQUIRE 22 ADDITIONAL BERTS AND UTILIZATION
$HASP895 WOULD REACH 32 PERCENT.
$HASP895 z11 ACTIVATION WILL SUCCEED IF ISSUED FROM THIS MEMBER.
```

In the example, there are 22 additional BERTs that will be used after the \$ACTIVATE to z11 mode, for transaction data associated with JOEs.

Note: When the SPOOLDEF LARGEDS=FAIL (default value) is in effect in your JES2PARM parmlib member, the following message will be issued by the \$ACTIVATE command:

```
$HASP895 z11 ACTIVATION WILL FAIL IF ISSUED FROM THIS MEMBER.
$HASP895 THE FOLLOWING ISSUES PREVENT ACTIVATION:
$HASP895 -- LARGEDS SUPPORT MUST BE ACTIVATED.
```

- A general history of BERT usage can be obtained by using the \$JD HISTORY(BERT) command or by using the SDSF RM panel. This displays the usage of BERTs after the system was IPLed. The following example shows the output of the \$JD HISTORY(BERT) command:

```
$HASP9130 D HISTORY
$HASP9131 JES2 BERT      USAGE HISTORY
DATE      TIME          LIMIT  USAGE    LOW    HIGH  AVERAGE
-----
2009.086 16:00:00    1100    337    337    337    337
2009.086 15:50:09    1100    337    125    337    192
```

JES2 actions to perform before the first IPL of z/OS V2R2

This topic describes JES2 migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Review changes applicable to JES2 exits

Description

In z/OS V2R2, exit changes might be necessary, depending on which exits you are using and which JES2 data areas those exits are referencing.

Table 142 provides more details about this migration action. Use this information to plan your changes to the system.

Table 142. Information about this migration action

Element or feature:	z/OS JES2.
---------------------	------------

Table 142. Information about this migration action (continued)

When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have any affected JES2 exits.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

See the "JES2 migration details" section of *z/OS JES2 Installation Exits*. This section details the changed information which you might need to accommodate. Generally, assembly errors in JES2 exits indicate that you were affected by a JES2 data area change.

Reference information

For more information, see *z/OS JES2 Installation Exits*.

JES2 actions to perform after the first IPL of z/OS V2R2

This topic describes JES2 migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

JES3 migration actions

This topic describes migration actions for optional feature JES3.

JES3 actions to perform before installing z/OS V2R2

This topic describes JES3 migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

JES3 actions to perform before the first IPL of z/OS V2R2

This topic describes JES3 migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Be aware that JES3 honors the DSI setting in SCHEDxx Description

Before z/OS V2R2, if data set integrity (DSI) was specified for the JES3 programs IATINTK or IATINTKF in your SCHEDxx parmlib member, ENQs would occur, but only for batch allocation of JES3 data sets that were identified in the JES3 start procedure with DD statements. If you did not specify IATINTK or

Migration actions from z/OS V2R1: JES3

IATINTKF in SCHEDxx, no ENQs would occur. The reason is that the value of NODSI for IATINTK and IATINTKF is coded in the IBM-supplied Program Properties Table (PPT, or IEFSDPPT). NODSI remains coded in IEFSDPPT in z/OS V2R2, as was done in previous releases.

Starting with z/OS V2R2, if you override the IBM-supplied PPT with a SCHEDxx entry of DSI for IATINTK or IATINTKF, ENQs occur for batch allocations of JES3 data sets identified in the JES3 start procedure with DD statements (as in previous releases). In addition, JES3 now also obtains ENQs for all dynamic allocations of JES3 data sets.

It is recommended that you take advantage of DSI protection by specifying DSI for IATINTK and IATINTKF in your SCHEDxx member. The SCHEDxx default when you specify a program name, is that the program name has DSI. Thus, if you do not specify any DSI value (DSI or NODSI) for a SCHEDxx program name, the program receives DSI protection. Therefore, it is recommended that you explicitly code a value of DSI in the SCHEDxx member for IATINTK and IATINTKF to avoid any confusion over which value is being used.

You can use the following PPT statements to add the DSI specification to SCHEDxx and maintain the attributes from the IBM-supplied default entries:

```
PPT PGMNAME(IATINTK) NOCANCEL NOSWAP SYST DSI KEY(1) NOHONORIEFUSIREGION
PPT PGMNAME(IATINTKF) NOSWAP SYST DSI KEY(1)
```

Table 143 provides more details about this migration action. Use this information to plan your changes to the system.

Table 143. Information about this migration action

Element or feature:	JES3
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you previously set DSI in the SCHEDxx member; JES3 was ignoring it for dynamic allocations. When z/OS V2R2 is started, an ENQ results from the allocations, which might lead to unexpected consequences. It is recommended that you use DSI to prevent accidental damage to your data sets due to the lack of an ENQ.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	Use IBM Health Checker for z/OS check IBMJES3,JES3_DATASET_INTEGRITY, which determines whether DSI or NODSI is specified on the JES3 entries in the program properties table (PPT). The check generates an exception message when the current DSI setting does not match the specified setting. This check is provided as of z/OS V2R2.

Steps to take

Follow these steps:

- If you use DD allocations in your JES3 start procedure (not recommended), ensure that the DISP keyword specifies SHR, not OLD. Otherwise, the first JES3 that comes up locks out other JES3 address spaces in the same sysplex. All dynamic allocations by JES3 use DISP=SHR.
- Because an ENQ is held on the data set names, it is recommended that you use unique spool data set names to allow for offline allocation, unallocation, and formatting. Check your JES3 start procedure and your DSN specification on the DYNALLOC statement in your inish deck for duplicate names.

Reference information

For more information, see *z/OS MVS Initialization and Tuning Reference*.

JES3 actions to perform after the first IPL of z/OS V2R2

This topic describes JES3 migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

Check code that references the JES3 Locate Response control block in IATYLRS Description

Starting with z/OS V2R2, the JES3 macro IATYLRS fixed entry is extended to support new generation data group (GDG) limits greater than 255. This change allows up to 999 active GDSs. The new format is called GDG Extended (GDGE). To support 999 active GDSs, the size of a JES3 Locator Response (LRS) fixed entry is extended and a new 2-byte GDG limit field is added.

Flag byte LRSFLG2 contains a new flag that indicates when an LRS with an extended fixed entry is used:

LRSFIXEX EQU X'04' LRS extended fixed entry is used

The LRS fixed entry size is being extended from 12 bytes as represented by the equate LRSFXLEN. Two fields are defined in the extended fixed entry:

LRSXFXLN DS H Length of LRS fixed entry
 LRSGDLME DS H GDG limit from catalog management (GDGLIMTE)

When flag LRSFIXEX is set, the extended format of the LRS fixed entry is present and the value of field LRSXFXLN should be used for the length of the LRS fixed entry. Otherwise, the previous format of the LRS fixed entry is present and the existing equate LRSFXLEN is used for the length.

When existing flag LRSGDG is set, the LRS entry is for a GDG ALL request with a GDG limit value provided. When LRSFIXEX is set, the value of field LRSGDLME will contain the 2-byte GDG limit. Existing field LRSGDLIM is maintained and is set to the lesser of 255 and the value in LRSGDLME. When LRSFIXEX is not set, the value of field LRSGDLIM will contain the 1-byte GDG limit.

Table 144 provides more details about this migration action. Use this information to plan your changes to the system.

Table 144. Information about this migration action

Element or feature:	JES3
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.

Migration actions from z/OS V2R1: JES3

Table 144. Information about this migration action (continued)

Is the migration action required?	Yes, if you have code that references the JES3 Locate Response control block as defined in IATYLRS. No changes are required if only the LRS fixed entry fields are referenced and if the existing GDG limit field LRSGDLIM is not referenced.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Look for code, especially JES3 user exits, that refers to IATYLRS with the supplied address, referencing any of the following fields or equates from IATYLRS: LRSFXLEN, LRSGDLIM, or LRSDATA.
- Code using the length in equate LRSFXLEN to advance beyond the LRS fixed entry must be changed to use the value in field LRSXFXLN when flag LRSFIXEX is set.
- Code directly referencing the LRS data entry using the label LRSDATA must be changed to advance beyond the LRS fixed entry using the length value in field LRSXFXLN or equate LRSFXLEN based upon the flag LRSFIXEX.
- Code using the GDG limit in LRSGDLIM must be changed to use the new 2-byte GDG limit in field LRSGDLME when flag LRSFIXEX is set.

Reference information

For more information about the GDGE format, see the descriptions of the GDGLIMIT and GDGLIMTE fields in *z/OS DFSMS Managing Catalogs*.

Language Environment migration actions

This topic describes migration actions for base element Language Environment.

Language Environment actions to perform before installing z/OS V2R2

This topic describes Language Environment migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Ensure that the name of the debug tool event handler is recognized by Language Environment

Description

Before z/OS V2R2, the value for the debug tool event handler name that is specified by the `_CEE_DEBUG_FILENAME31` environment variable was not restricted. Starting in V2R2, the name must be `/bin/dbx31vdbg` or be defined in a file that contains a list of allowed values.

Table 145 on page 215 provides more details about this migration action. Use this information to plan your changes to the system.

Migration actions from z/OS V2R1: Language Environment

Table 145. Information about this migration action

Element or feature:	Language Environment
When change was introduced:	z/OS V2R1, z/OS V1R13, and z/OS V1R12 (all with APAR PM99349 applied).
Applies to migration from:	z/OS V2R1 and z/OS V1R13 (both without APAR PM99349 applied).
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended if you use debuggers in certain circumstances. Many debuggers will not be affected for any of these reasons: <ul style="list-style-type: none">• They do not provide a debug tool event handler. (HLASM Toolkit Feature Interactive Debug Facility (ASMIDF), TSO/E TEST)• They do not install a debug tool event handler in z/OS UNIX file systems. (Debug Tool for z/OS, Rational Developer for System z Integrated debugger)• They use a debug tool event handler in the z/OS UNIX file system that is allowed by default. (dbx)
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Message CEE2532S is issued, indicating that use of the debug tool event handler specified by the <code>_CEE_DEBUG_FILENAME31</code> environment variable is not allowed.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Look for any vendor product or your own software that is a debugger and uses the environment variable `_CEE_DEBUG_FILENAME31` to identify a debug tool event handler in the z/OS UNIX file system.
- If any are found, create the file `/etc/_CEE_DEBUG_FILENAME31.list` and add the file name that is specified by the environment variable `_CEE_DEBUG_FILENAME31` to it.

Note: The file name `/bin/dbx31vdbg`, used by dbx, does not need to be added to this file.

After you complete the steps, the name of the debug tool event handler will be recognized by Language Environment.

Reference information

For more information about the `_CEE_DEBUG_FILENAME31` environment variable, see *z/OS Language Environment Vendor Interfaces*

Migration actions from z/OS V2R1: Language Environment

Language Environment actions to perform before the first IPL of z/OS V2R2

This topic describes Language Environment migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Update the CSD based on the newest CEECCSD Description

Each release, Language Environment adds or deletes load modules in the CICS system definition (CSD) file. Thus, you should update the file each release using the program definitions found in members CEECCSD and CEECCSDX found in the SCEESAMP data set. The CSD samples provided by Language Environment (CEECCSD and CEECCSDX) at the latest release can be used for systems at earlier releases that can co-exist with this level of z/OS.

Table 146 provides more details about this migration action. Use this information to plan your changes to the system.

Table 146. Information about this migration action

Element or feature:	Language Environment.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use CICS.
Target system hardware requirements:	None.
Target system software requirements:	CICS.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Failure to perform this migration action may result in several various program ABENDs, such as ABENDU4093 RC=3EC. Which ABEND you see will depend on which programming language (and which level of the programming language) you are using.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Update the CSD file using the program definitions in member CEECCSD (and member CEECCSDX if using CICS TS V3 or later) found in the hlq.SCEESAMP data set.

Note: The group containing the Language Environment runtime routines must be in the group list used during CICS startup.

Reference information

For more information, see *z/OS V2R1.0 Language Environment Runtime Application Migration Guide*.

Update Language Environment load modules in the LPA

Description

Each release you must update the Language Environment load modules that you make accessible through the link pack area (LPA). In addition, each release you should review your list of Language Environment load modules in the LPA to determine if it is still suitable.

Table 147 provides more details about this migration action. Use this information to plan your changes to the system.

Table 147. Information about this migration action

Element or feature:	Language Environment.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you need to make modules accessible through the link pack area (LPA).
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Review Language Environment load modules in the LPA.

To move load modules into the LPA, use the following sample members in the CEE.SCEESAMP data set:

- *AFHWMLP2*: This is a sample of all Language Environment Fortran component modules eligible for the LPA.
- *CEEWLPA*: This is a sample of a PROGxx member of SYS1.PARMLIB that includes all Language Environment CEE-prefixed runtime modules eligible for the LPA (that is, all Language Environment base modules) except the callable services stubs.
- *CELQWLPA*: This is a sample for AMODE 64 runtime support.
- *EDCWLPA*: This is a sample of a PROGxx member of SYS1.PARMLIB that includes all Language Environment EDC-prefixed and CEH-prefixed runtime modules eligible for the LPA (that is, all XL C/C++ component modules) except locales and code page converters.
- *IBMALLP2* (or *IBMPLPA1* for Enterprise PL/I for z/OS): This is a sample of all Language Environment PL/I component modules eligible for the LPA.
- *IGZWMLP4*: This is a sample of all Language Environment COBOL component modules eligible for the LPA.

To see which modules are eligible for the LPA, refer to *z/OS Language Environment Customization*. The modules listed there can be put in the LPA or extended LPA (ELPA) depending on their RMODE value:

- If the RMODE is ANY, the module can reside in the LPA or in the ELPA (above or below the 16 MB line).
- If the RMODE is 24, the module can reside only in the LPA (below the 16 MB line).

Migration actions from z/OS V2R1: Language Environment

If you are considering placing the modules listed in *z/OS Language Environment Customization* in the LPA or the ELPA, then IBM recommends that you place the SCEELPA data set in the LPA list (LPALSTxx). SCEELPA contains Language Environment load modules that are reentrant, that reside above the 16 MB line, and that are heavily used by z/OS.

In *z/OS Language Environment Customization* you will also see tables of modules eligible for the LPA and the ELPA above and beyond what is found in the SCEELPA data set. You will need to use the dynamic LPA or MLPA approach to move these modules into the LPA or ELPA. You do not need to include recommended modules if they contain functions your installation does not use. Language Environment modules not listed in these tables can be moved into the LPA or ELPA at your discretion.

Reference information

For more information, see the table “Language Environment sample IEALPAnn or PROGxx members in *hlq.SCEESAMP*” for the list of sample members and their changed content in *z/OS Language Environment Customization*. The table contains a list of eligible load modules for:

- Language Environment base modules
- Language Environment XL C/C++ component modules
- Language Environment COBOL component modules
- Language Environment Fortran component modules
- Language Environment PL/1 component modules

Language Environment actions to perform after the first IPL of z/OS V2R2

This topic describes Language Environment migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

Library Server migration actions

This topic describes migration actions for base element Library Server.

Library Server actions to perform before installing z/OS V2R2

This topic describes Library Server migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

Library Server actions to perform before the first IPL of z/OS V2R2

This topic describes Library Server migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Copy Library Server configuration files

Description

The Library Server configuration files (*bookmgr.80*, *booksrv.80*) contain information about your environment and preferences. The information in *bookmgr.80* includes the names of bookshelf lists for bookshelves in z/OS data sets and the names of the file system directories that Library Server reads and writes during execution. The information in *booksrv.80* includes the file system directory names of book collections, shelves, and bookcases, as well as product option settings configured via the Library Server Administration Page. There are default values but normally you would customize them. In order to bring

Migration actions from z/OS V2R1: Library Server

the customized values over to your new system, you have to copy them. (Note that port number suffix .80, used in bookmgr.80 and booksrv.80, is an example. Your port number suffix might be different.)

Table 148 provides more details about this migration action. Use this information to plan your changes to the system.

Table 148. Information about this migration action

Element or feature:	Library Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you intend to preserve your Library Server configuration.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Copy your current (customized) configuration files, usually bookmgr.80 and booksrv.80, to your new system and add any configuration parameters that are new since the z/OS release from which you are migrating. Otherwise Library Server will run with default values, not the values you're used to. A suggested (but not required) place for these configuration files is /etc/booksrv. Library Server will also search /etc and the original cgi-bin for them. If you place the files in any other directory, use the EPHConfigPath environment variable to tell Library Server where to find them.

Reference information

For description of each parameter of the Library Server configuration files, see *z/OS Program Directory* at the z/OS installation related information website.

Copy Library Server notes files

Description

Users can make comments in book topics by creating notes that are appended to the end of each topic. If you do not copy these notes to the new system, they will be lost.

Table 149 provides more details about this migration action. Use this information to plan your changes to the system.

Table 149. Information about this migration action

Element or feature:	Library Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you intend to preserve notes from release to release.

Migration actions from z/OS V2R1: Library Server

Table 149. Information about this migration action (continued)

Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Copy all the files from your existing notes directory to the new one. The default directory for saving book notes is `/usr/lpp/booksrv/public/bookmgr/notes`. You can override this default by specifying a directory on the `NOTEDIR` parameter of the `bookmgr.80` configuration file.

Reference information

For a description of each parameter of the Library Server configuration files, see *z/OS Program Directory* at the z/OS installation related information website.

Migrate the Library Server configuration to work with IBM HTTP Server - Powered by Apache

Description

Starting with z/OS V2R2, the web server is IBM HTTP Server - Powered by Apache. As a result, the HTTP Server configuration required by Library Server, particularly the configuration file directives, is significantly different than that required for the Domino-based HTTP Server used prior to z/OS V2R2.

If Library Server on your z/OS V2R1 or V1R13 system was not already configured to use an Apache-based HTTP Server, you must change the configuration of the z/OS V2R2 Library Server to operate with IBM HTTP Server - Powered by Apache. z/OS V2R2 includes IBM HTTP Server - Powered by Apache as a base element.

Table 150 provides more details about this migration action. Use this information to plan your changes to the system.

Table 150. Information about this migration action

Element or feature:	Library Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if Library Server on your z/OS V2R1 or V1R13 system was not already configured to use an Apache-based HTTP Server.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

The following steps summarize the Library Server changes to consider when migrating from IBM HTTP Server powered by Domino to IBM HTTP Server - Powered by Apache in z/OS V2R2:

1. The envvars file of environment variable settings moves from conf/httpd.envvars to bin/envvars.
2. For each environment variable set in bin/envvars, a **PassEnv** directive is needed in conf/httpd.conf.
3. All **Pass** directives are required to become **Alias** directives in conf/httpd.conf.
4. All **Exec** directives are required to become **ScriptAlias** directives in conf/httpd.conf.
5. Multiple port support is configured in a single conf/httpd.conf using the VirtualHost directive, such as **<VirtualHost *:8080>**.
6. A **Listen port#** directive must be specified for each port (default and VirtualHost) configured in conf/httpd.conf.
7. A **<LocationMatch>** directive is required in conf/httpd.conf to prevent EBCDIC to ASCII translation when downloading CSS files.
8. If configuring an SSL port in conf/httpd.conf, the **LoadModule ibm_ssl_module modules/mod_ibm_ssl.so** directive must be enabled.
9. A self-identifying **ServerName** directive, such as **ServerName MYMVS.ibm.com:80**, should be specified in conf/httpd.conf.
10. Other directives such as **ErrorLog**, **CustomLog**, and **ServerAdmin** should be configured as needed in conf/httpd.conf.

Add the new directives mentioned here to the conf/httpd.conf file that is installed with IBM HTTP Server - Powered by Apache, and base them on the corresponding directives, if applicable, from your conf/httpd.conf file that was previously used with IBM HTTP Server powered by Domino. Examples of the new directives are provided in the HTTP server customization topic of the *Library Server Customization Considerations* section in the *z/OS Program Directory*.

Reference information

For more information, see the following references:

- For Library Server customization considerations, see *z/OS Program Directory* at the z/OS installation related information website
- For information about how to plan for, install, configure and use IBM HTTP Server - Powered by Apache, see *z/OS V2R2.0 HTTP Server - Powered by Apache User's Guide* .

Library Server actions to perform after the first IPL of z/OS V2R2

This topic describes Library Server migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

RMF migration actions

This topic describes migration actions for optional feature Resource Measurement Facility™ (RMF).

RMF actions to perform before installing z/OS V2R2

This topic describes RMF migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

Migration actions from z/OS V2R1: RMF

RMF actions to perform before the first IPL of z/OS V2R2

This topic describes RMF migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

None.

RMF actions to perform after the first IPL of z/OS V2R2

This topic describes RMF migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

Determine whether RMF should monitor zFS file system activity by default Description

The Monitor III data gatherer can be used to monitor zFS file system activity; this function is enabled or disabled through the options ZFS and NOZFS, which are set in ERBRMF04. Before z/OS V2R1, the default setting was ZFS. In z/OS V2R1, the default changed to NOZFS. Starting in z/OS V2R2, RMF introduces new Monitor III zFS sysplex reports that gather zFS performance data through new zFS APIs. As a result, the default Monitor III gatherer option is changed to ZFS.

Table 151 provides more details about this migration action. Use this information to plan your changes to the system.

Table 151. Information about this migration action

Element or feature:	RMF
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you do not want to collect data about zFS file system activity.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Determine whether you want RMF to monitor zFS file system activity.
- If you want to always monitor zFS file system activity, no action is required.
- If you do not always want to monitor zFS file system activity, then you can either:
 - Specify the NOZFS option in the ERBRMFxx parmlib member, so it will always be in effect for all of your Monitor III data gatherer sessions.
 - Use the **MODIFY RMF,MODIFY III,NOZFS** command during a running session.

Reference information

For more information about the NOZFS option, see *z/OS RMF User's Guide*.

Update programs that use ERBZFST3 or ERBZFAT3

Description

Before z/OS V2R2, RMF provided ZFSSUM or ZFSACT reports, which stored results in Monitor III tabular report data tables ERBZFST3 and ERBZFAT3. Starting with z/OS V2R2, RMF provides ZFSOVW or ZFSFS reports, which store results in Monitor III tabular report data tables ERBZFOT3 and ERBZFFT3. This change will affect any user written programs and applications that reference ERBZFST3 or ERBZFAT3.

Table 152 provides more details about this migration action. Use this information to plan your changes to the system.

Table 152. Information about this migration action

Element or feature:	RMF
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you modified any of the four Monitor III reporter session phases to refer to any of the fields in ERBZFST3 or ERBZFAT3, or have programs or applications that refer to any of the fields in ERBZFST3 or ERBZFAT3.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- If you have used the RMF Monitor III utility to modify any of the four Monitor III reporter session phases, search the programs or applications provided as user exits for these Monitor III phases for fields from the RMF Monitor III tabular report data tables ERBZFST3 and ERBZFAT3.

Likewise, look for Monitor III reports that have been modified or created with the Monitor III utility that make use of any of the fields in ERBZFST3 or ERBZFAT3.

The RMF Monitor III tabular report data tables ERBZFST3 and ERBZFAT3 will be empty (the tables exist, but contain no data) when running RMF Monitor III in V2R2, because zFS performance data will be stored to ERBZFOT3 and ERBZFFT3. Programs or applications using values from ERBZFST3 or ERBZFAT3 will always find empty fields (no data contained).

To access zFS performance data with your existing user exits or modified Monitor III reports, you must use ZFSOVW and ZFSFS instead of ZFSSUM and ZFSACT. You must also replace the field names from ERBZFST3 and ERBZFAT3 you have identified in the previous step with the corresponding fields from ERBZFOT3 and ERBZFFT3.

- Look for applications requesting ZFSSUM or ZFSACT data from the RMF Distributed Data Server using the HTTP API (a request for a complete ZFSSUM or ZFSACT report or requests for metrics based on one of these reports), such as:

```
http://hostname:8803/gpm/reports/ZFSSUM?resource=",S4,MVS_IMAGE"
```

or

Migration actions from z/OS V2R1: RMF

[http://hostname:8803/gpm/perform.xml?resource="S4,*,ZFS"&id=8D2AC0](http://hostname:8803/gpm/perform.xml?resource=)

HTTP applications requesting data based on ZFSSUM or ZFSACT will receive an HTTP response containing a GPM0630I message stating that no data is available for this request. Therefore HTTP applications must be changed to use requests for ZFSOVW or ZFSFS reports and requests for metrics based on these reports, if you want to monitor zFS performance data.

Reference information

For more information, see the following references:

- For information about ZFSOVW and ZFSFS reports, see *z/OS RMF Report Analysis*.
- For information about Monitor III tabular report data tables ERBZFOT3 and ERBZFFT3, see *z/OS RMF Programmer's Guide*.

Use an RMF Monitor III reporter version equal to or later than your RMF Monitor III gatherer version

Description

To avoid problems when reporting Monitor III data, use an RMF reporter version that is equal to or later than the latest RMF gatherer version used to collect the data to be reported. For example, it is safe to use an RMF reporter version from z/OS V2R2 for data collected with an RMF gatherer from z/OS V1R13, but not vice versa.

Mixed (and therefore problematic) levels of collected data can occur in the following scenarios:

- *Single system*: You install and test a new release, then fall back to an earlier one; your data sets might contain data collected with different versions of the RMF gatherer.
- *Sysplex*: You migrate to a new release on one system in a sysplex but try to use an earlier reporter version from another system to report on the migrated system's data.

Table 153 provides more details about this migration action. Use this information to plan your changes to the system.

Table 153. Information about this migration action

Element or feature:	RMF.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you had planned to use an earlier level RMF reporter on data that was collected with a later level RMF gatherer.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	See "Steps to take."
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Always use an RMF Monitor III reporter version that is equal to or later than the gatherer version used to collect the data from which you want to produce a report.

Note: Monitor III notifies users by issuing information message ERB948I when a reporter session is started on a system in a sysplex that is not running with the highest RMF level available in the sysplex. The message helps users to avoid reporting problems.

Reference information

For more information, see *z/OS RMF User's Guide*.

SDSF migration actions

This topic describes migration actions for optional feature SDSF.

SDSF actions to perform before installing z/OS V2R2

This topic describes SDSF migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

SDSF actions to perform before the first IPL of z/OS V2R2

This topic describes SDSF migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Review and reassemble user exit routines

Description

If you have written user exit routines, review them to ensure they are still appropriate for the current environment, and make changes as necessary. All user exit routines must be reassembled with the z/OS V2R2 level of the SDSF macro library.

Table 154 provides more details about this migration action. Use this information to plan your changes to the system.

Table 154. Information about this migration action

Element or feature:	SDSF.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if user exit routines are in use.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Migration actions from z/OS V2R1: SDSF

Steps to take

Review user exit routines to ensure they are appropriate for z/OS V2R2. Make changes as necessary. Regardless of whether you have made changes, reassemble the user exit routines with the z/OS V2R2 level of the SDSF macro library.

Tip: A PROPLIST statement, along with PROPERTY statements, both in the ISFPRMxx parmlib member, defines customized values for certain SDSF properties. It provides an alternative to writing user exit routines to customize those properties. A user exit routine that customizes the same property as a PROPERTY statement overrides the value on the PROPERTY statement.

Reference information

For more information, see *z/OS SDSF Operation and Customization*.

Use dynamic statements for ISFPARMS to avoid reassembly

Description

ISFPARMS in SDSF is used for specifying global options, the format of panels, and security for SDSF functions. SDSF provides two alternatives for ISFPARMS:

- Assembler macros that you define, assemble, and then link into the SDSF load library. This is the original format for defining ISFPARMS and it continues to be supported for compatibility.
- Dynamic statements, which are in parmlib member ISFPRMxx. Dynamic statements are the recommended format. They are easier to code and are more dynamic than the assembler macros; they can be updated without reassembling or link-editing. The statements are processed by an SDSF server, which is controlled by MVS™ operator commands.

Table 155 provides more details about this migration action. Use this information to plan your changes to the system.

Table 155. Information about this migration action

Element or feature:	SDSF.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	No, but recommended to avoid the migration action of reassembling your customized ISFPARMS for each z/OS release. (If you do not use dynamic statements for ISFPARMS, reassembly of your customized ISFPARMS is required on each release.)
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Table 155. Information about this migration action (continued)

<p>Related IBM Health Checker for z/OS check:</p>	<p>Use check SDSF_ISFPARMS_IN_USE to verify that SDSF dynamic statements in ISFPRMxx are being used rather than the assembler macros. If the check determines that the assembler macro ISFPARMS is in use instead, and that it has been modified, the check generates an exception. If the assembler macro ISFPARMS is in use but it has not been modified, so that all defaults are in effect, the check does not generate an exception.</p> <p>SDSF registers this check with the IBM Health Checker for z/OS infrastructure when the SDSF server address space is initialized. However, one of the items this check verifies is that the SDSF server itself is in use, so you have to manually add this check (particularly if you do not use the SDSF server) so that the IBM Health Checker for z/OS infrastructure will invoke the check. To add the check, put the following statement in your PROGxx parmlib member: EXIT ADD EXITNAME(HZSADDCK) MODNAME(ISFHCADC).</p> <p>SDSF health checks are distributed in ISF.SISFLOAD for installations running SDSF in the LNKLST. The checks are also distributed in ISF.SISFLINK for installations that do not run SDSF in the LNKLST. For those installations, ISF.SISFLINK must be added to the LNKLST.</p> <p>Note: To avoid a possible ABEND 290 with reason code 02014007 issued by HZSADDCK:</p> <ul style="list-style-type: none"> Specify the proper check routine name. The check routine module must be in an APF-authorized library. The system must be able to locate the check routine within the joblib, the steplib of the IBM Health Checker for z/OS address space, the LPA, or the LNKLST. Specify the proper message table name. The message table module must be in an APF-authorized library. The system must be able to locate the message table within the joblib, the steplib of the IBM Health Checker for z/OS address space, the LPA, or the LNKLST.
---	---

Steps to take

If you are already using dynamic statements for ISFPARMS, there is no migration action to perform.

If you are using assembler macros for ISFPARMS, do one of the following:

- Convert your existing ISFPARMS to dynamic statements by using a conversion utility that you invoke with the ISFACP command.
- Reassemble your customized ISFPARMS for use with z/OS V2R2. Reassembly must be done whenever you change your z/OS release. Before reassembling ISFPARMS, you might want to update it for new function. The assembler ISFPARMS cannot be shared with any other release of SDSF. Only use ISFPARMS for the release on which it is assembled.

Note: If you have an SMP/E usermod that specifies modifications to assembler macro ISFPARMS, change the usermod to indicate that module ISFPARMS is now owned by the z/OS base V2R2 SDSF FMID (HQX77A0). The correct SMP/E syntax is ++VER(Z038) FMID(HQX77A0)

Migration actions from z/OS V2R1: SDSF

Also, in the SMP/E usermod, change the distlib to reference DISTLIB(AISFSRC). The correct SMP/E syntax is ++VER(Z038) FMID(HQX77A0). Your ++SRC or ++SRCUPD statement must specify DISTLIB(AISFSRC).

Reference information

For information about invoking the conversion utility with the ISFACP command, and the ISFPARMS and the ISFPRMxx parmlib members, see *z/OS SDSF Operation and Customization*.

SDSF actions to perform after the first IPL of z/OS V2R2

This topic describes SDSF migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

Security Server migration actions

This topic describes migration actions for optional feature Security Server.

Security Server actions to perform before installing z/OS V2R2

This topic describes Security Server migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Accommodate the removal of default passwords on RACF commands

Description

- | As of z/OS V2R2, the RACF commands **ADDUSER**, **ALTUSER**, and **PASSWORD** no longer set a default password for the target user ID. In previous releases, these commands used the user's default group name as the password by default.
- | Specifically, the commands are changed as follows to remove the generation of default passwords:
 - | • Command **ADDUSER** defaults to PROTECTED when no password or phrase is specified.
 - | • Commands **ADDUSER**, **ALTUSER**, and **PASSWORD** no longer set a default password for the target user ID.

Table 156 summarizes the new RACF command behavior in z/OS V2R2.

| *Table 156. New RACF command behavior in z/OS V2R2*

Command	Condition	New behavior with z/OS V2R2 with APAR OA48667 applied
ADDUSER <i>user</i>	PASSWORD keyword is omitted.	The user is defined as a PROTECTED user, unless a PHRASE or OIDCARD value is specified. Also, message ICH01024I is issued, stating that the user is defined as PROTECTED.
ADDUSER <i>user</i> PASSWORD	PASSWORD keyword is specified, but its value is omitted.	PASSWORD keyword is ignored with message ICH01025I and the user ID is defined as PROTECTED.
ALTUSER <i>user</i> PASSWORD	PASSWORD keyword is specified, but its value is omitted.	PASSWORD keyword is ignored with message ICH21045I.
PASSWORD USER(<i>user</i>)	INTERVAL NOINTERVAL keyword is omitted.	USER keyword is ignored and message ICH08027I is issued.

Notes:

1. As in previous releases, when a new RACF database is initialized through the IRRMIN00 utility, the IBMUSER user ID is created with a password value of 'SYS1'
2. In previous releases, if the **ADDUSER** command was issued without the PASSWORD keyword:
 - RACF common command exit (IRREVX01) received the **ADDUSER** command with the PASSWORD keyword, but without a value for PASSWORD. As of z/OS V2R2, the PASSWORD keyword is not passed to the exit.
 - Type 80 record for the ALTUSER event code indicated that the PASSWORD keyword was specified. As of z/OS V2R2, the Type 80 record no longer indicates that the PASSWORD keyword was specified.

Table 157 provides more details about this migration action. Use this information to plan your changes to the system.

Table 157. Information about this migration action

Element or feature:	Security Server.
When change was introduced:	z/OS V2R2 with APAR OA48667 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13 (with APAR OA48667 applied or without APAR OA47396 applied).
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you rely on RACF to create a default password.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Identify any programs or jobs that issue RACF commands with the following conditions:
 - **ADDUSER** command that does not specify the PASSWORD keyword.
 - **ADDUSER** and **ALTUSER** commands that specify the PASSWORD keyword, but omit an explicit password value.
 - Programs that call the ADMN_RUN_COMD function of the R_admin SAF callable service (IRRSEQ00) on the **ADDUSER**, **ALTUSER**, or **PASSWORD** commands, as described here.
 - Programs that call the ADMN_ADD_USER or ADMN_ALT_USER functions of the R_admin SAF callable service (IRRSEQ00) with input parameter lists that are functionally equivalent to the **ADDUSER**, **ALTUSER**, or **PASSWORD** commands, as described here.
2. Depending on the condition listed above, either remove the command, change it to one that specifies an explicit password value, or leave it as-is and tolerate the change of behavior, as appropriate.

Example: Before z/OS V2R2, the following **ALTUSER** command would reset the password for user BECKYH to the user's default group name: ALTUSER BECKYH PASSWORD. In z/OS V2R2 with OA48667 applied, the PASSWORD operand is ignored. To reset a password, you must provide a temporary password explicitly: ALTUSER BECKYH PASSWORD(TEMP1234).

Migration actions from z/OS V2R1: Security Server

Reference information

For more information, see *z/OS Security Server RACF Command Language Reference*.

Security Server actions to perform before the first IPL of z/OS V2R2

This topic describes Security Server migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Check for duplicate class names

Description

When new classes are shipped with RACF, you should verify that any installation-defined class names that have been added to the class descriptor table (CDT) do not conflict with the new classes. For a list of new classes shipped with RACF, see *z/OS Summary of Message and Interface Changes*.

Table 158 provides more details about this migration action. Use this information to plan your changes to the system.

Table 158. Information about this migration action

Element or feature:	Security Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have user-defined classes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Verify that any installation-defined class names that have been added to the class descriptor table (CDT) do not conflict with the new classes.

- If you have duplicate class names, RACF issues the following message and enters failsoft mode:
ICH564A RACF DETECTED AN ERROR IN THE INSTALLATION CLASS DESCRIPTOR TABLE,
ENTRY *class_name*, ERROR CODE 7
- If a conflict in class names occurs, resolve it as follows:
 1. Delete the profiles in the installation-defined class with the conflicting name.
 2. Delete the CDT entry for the class.
 3. Add a CDT entry with a different name.
 4. Redefine the profiles.

Reference information

For more information, see *z/OS Security Server RACF System Programmer's Guide*.

Evaluate your use of the ICHDEX01 exit routine

Description

Starting in z/OS V2R2, RACF no longer uses the masking algorithm (a weak form of encryption) by default to authenticate passwords and password phrases when the initial attempt using DES results in failure. To continue the use of masking, which is not recommended, your installation can do so only by using an ICHDEX01 (password authentication) exit routine. If no ICHDEX01 exit routine exists, RACF now uses only DES encryption for authentication.

The Key Derivation Function with AES (KDFAES) algorithm is the preferred method for authenticating passwords and password phrases. If your installation does not use KDFAES encryption, RACF performs authentication by using the DES algorithm, unless you supply an ICHDEX01 exit routine. In the ICHDEX01 exit routine, your installation can provide an encryption algorithm, or instruct RACF to use one of the following forms of authentication:

Return code 4

Use the masking algorithm.

Return code 8

Use the DES algorithm.

Return code 16

Attempt to use DES first. If DES processing fails, use masking. This was the default behavior before z/OS V2R2 if no ICHDEX01 exit routine was installed.

When the KDFAES algorithm is active, masking is never used, thus no migration action is needed. RACF continues to call ICHDEX01 to evaluate a legacy password, but no longer honors masking. When a password is changed under KDFAES, the ICHDEX01 exit is no longer called for that password.

If your installation uses KDFAES encryption, it is recommended that you remove the ICHDEX01 exit routine, if it is no longer needed. For example, if the exit routine was used previously to always pass return code 8 (DES only), you can achieve the same result in z/OS V2R2 by removing the exit routine.

If your installation uses DES encryption, and you suspect there might be masked passwords in your RACF database, and you need to avoid any application outages that would result from the change in the default behavior, you must install an ICHDEX01 exit that sets return code 16. IBM recommends, however, that you attempt to identify such passwords and change them so that they are encrypted using DES.

Table 159 provides more details about this migration action. Use this information to plan your changes to the system.

Table 159. Information about this migration action

Element or feature:	Security Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have masked passwords in the RACF database.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Migration actions from z/OS V2R1: Security Server

Table 159. Information about this migration action (continued)

Related IBM Health Checker for z/OS check:	The health check RACF_ENCRYPTION_ALGORITHM (provided in APAR OA45608) raises an exception if weaker (less secure than DES) encryption is allowed for logon passwords.
--	---

Steps to take

Check for the existence of the ICHDEX01 exit routine in your RACF configuration. If it is present, determine whether you still need it. If not, remove it.

Follow these steps:

1. Check for the existence of the ICHDEX01 exit routine in your RACF configuration. During IPL, message ICH508I identifies the active exits. Check the message output for the presence of an ICHDEX01 exit routine. Or, run health check RACF_ENCRYPTION_ALGORITHM, which can detect return codes from an active ICHDEX01 exit routine.
2. If an ICHDEX01 exit routine is present, determine whether you still need it. Be aware that the masking algorithm provides weaker protection, as compared to KDFAES or DES.
3. Remove the exit routine if it is no longer needed. As an extra precaution, check for user profiles with old password change dates, which might indicate masked passwords. In these cases, you should either reset the password or delete it, rather than using the ICHDEX01 exit to preserve the usage of weak passwords. Use the RACF **LISTUSER** command to determine when passwords were last updated.

Otherwise, if your installation uses DES encryption, and you suspect there might be masked passwords in your RACF database, and you need to avoid any application outages that would result from the change in the default behavior, you must install an ICHDEX01 exit routine that sets return code 16, which mimics the current default behavior. Here is an example of the exit code that you can use:

```
LA 15,16  
BR 14
```

Note: IBM recommends that you use KDFAES encryption, rather than DES encryption or masking. KDFAES provides improved cryptographic strength in RACF password algorithm processing, and helps to protect RACF password data if a copy of a RACF database becomes inadvertently accessible. KDFAES encryption was introduced by APAR OA43999 for z/OS V1R12, V1R13, and V2R1, which is deactivated by default.

Reference information

For more information, see *z/OS Security Server RACF System Programmer's Guide*.

Security Server actions to perform after the first IPL of z/OS V2R2

This topic describes Security Server migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

Update database templates

Description

To ensure that the RACF utilities function properly, use the IRRMIN00 utility to update the test and production RACF databases with the database templates for the current release level.

Table 160 on page 233 provides more details about this migration action. Use this information to plan your changes to the system.

Table 160. Information about this migration action

Element or feature:	Security Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

To install the database template updates, run the IRRMIN00 utility with PARM=UPDATE.

Tip: The RACF database templates have been updated for z/OS V2R2. The templates contain a version string with a value of HRF77A0 00000194.00000022.

Note: If IRRMIN00 produces a return code of 4 and message IRR8025 PARM=UPDATE specified, but template update not required, you do not necessarily have a problem. Check that your JCL points to the new level of IRRMIN00. If it does, ignore the return code and warning message. A PTF might have already brought your templates up to the current level for the new release. If your JCL accidentally points to an old copy of IRRMIN00, correct the JCL and run IRRMIN00 again.

Reference information

For more information, see the following references:

- *z/OS Program Directory* at the z/OS installation related information website
- *ServerPac: Installing Your Order*
- *z/OS Security Server RACF System Programmer's Guide*

XL C/C++ migration actions

This topic describes migration actions for optional feature XL C/C++.

XL C/C++ actions to perform before installing z/OS V2R2

This topic describes XL C/C++ migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Review the XL C/C++ Migration Guide for the Application Programmer Description

Review the publication *z/OS XL C/C++ Compiler and Runtime Migration Guide for the Application Programmer* for any z/OS C/C++ migration actions. It is written for application programmers, whereas this publication (*z/OS Migration*) is written for system programmers. In some customer locations, job

Migration actions from z/OS V2R1: XL C/C++

scope can overlap such that system programmers might find information in the XL C/C++ publication that is relevant to their responsibilities. For example, migration information related to the c89 utility in the XL C/C++ publication could be of interest.

Table 161 provides more details about this migration action. Use this information to plan your changes to the system.

Table 161. Information about this migration action

Element or feature:	XL C/C++
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended if you use XL C/C++.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

For migration information that is relevant to your installation, see *z/OS XL C/C++ Compiler and Runtime Migration Guide for the Application Programmer*.

Reference information

For more information, see *z/OS XL C/C++ Compiler and Runtime Migration Guide for the Application Programmer*.

XL C/C++ actions to perform before the first IPL of z/OS V2R2

This topic describes XL C/C++ migration actions that you can perform only before you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

XL C/C++ actions to perform after the first IPL of z/OS V2R2

This topic describes XL C/C++ migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

z/OS Font Collection migration actions

This topic describes migration actions for the base z/OS Font Collection.

z/OS Font Collection actions to perform before installing z/OS V2R2

This topic describes z/OS Font Collection actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

z/OS Font Collection actions to perform before the first IPL of z/OS V2R2

This topic describes z/OS Font Collection migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Use the font libraries that are shipped in z/OS V2R2

Description

z/OS Font Collection, a new element in z/OS V2R1, replaces earlier font products you might be using in z/OS V1R13. The FMIDs for the earlier font products that z/OS Font Collection replaces are listed in *z/OS Planning for Installation*.

Ensure that you are using the font libraries for z/OS Font Collection instead of the font libraries for the earlier font products. If you refer to the SYS1.FONTOLN font library for AFP outline fonts, replace the references with SYS1.SFNTILIB, which is the AFP outline font library for z/OS Font Collection.

Table 162 provides more details about this migration action. Use this information to plan your changes to the system.

Table 162. Information about this migration action

Element or feature:	z/OS Font Collection
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you reference the SYS1.FONTOLN font library for AFP outline fonts. These products might reference SYS1.FONTOLN: <ul style="list-style-type: none"> • Print Services Facility (PSF), PN 5655-M32 • AFP Conversion and Indexing Facility (ACIF), optional feature of PSF • IBM Print Transform from AFP to PCL for Infoprint Server for z/OS, PN 5655-TF2 • IBM Print Transform from AFP to PDF for Infoprint Server for z/OS, PN 5655-TF1 • IBM Print Transform from AFP to PostScript for Infoprint Server for z/OS, PN 5655-TF3
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Replace all references to SYS1.FONTOLN with SYS1.SFNTILIB. Look in these product locations for references:

PSF Startup procedure

Migration actions from z/OS V2R1: z/OS Font Collection

ACIF FONTLIB DD statement

Print Transforms from AFP for Infoprint Server

Infoprint Server transform configuration file (aopxfd.conf)

Reference information

For information about how to edit font library locations, see:

- *PSF for z/OS: Customization, S550-0427*
- *AFP Conversion and Indexing Facility User's Guide, S550-0436*
- *IBM Print Transforms from AFP for Infoprint Server for z/OS, G325-2634*

For more information about the z/OS Font Collection, see *z/OS Font Collection*.

z/OS Font Collection actions to perform after the first IPL of z/OS V2R2

This topic describes z/OS Font Collection migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

z/OS OpenSSH migration actions

This topic describes migration actions for base element z/OS OpenSSH.

z/OS OpenSSH actions to perform before installing z/OS V2R2

This topic describes z/OS OpenSSH migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

z/OS OpenSSH actions to perform before the first IPL of z/OS V2R2

This topic describes z/OS OpenSSH migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

None.

z/OS OpenSSH actions to perform after the first IPL of z/OS V2R2

This topic describes z/OS OpenSSH migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

Accommodate the OpenSSH ported level Description

Before z/OS V2R2 and IBM Ported Tools for z/OS V1R3, OpenSSH was version 5.0p1. Starting with z/OS V2R2 and IBM Ported Tools for z/OS V1R3, OpenSSH is version 6.4p1.

Before z/OS V2R2, OpenSSH was available from IBM Ported Tools for z/OS. Starting with z/OS V2R2, it is now available as a base element of z/OS.

Table 163 on page 237 provides more details about this migration action. Use this information to plan your changes to the system.

Table 163. Information about this migration action

Element or feature:	OpenSSH
When changes were introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both with IBM Ported Tools for OpenSSH V1R2.
Timing:	After the first IPL of z/OS V2R2.
Are the migration actions required?	Yes, if any of the changes in “Steps to take” are applicable to your environment.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

The following is a list of potential migration actions for the OpenSSH base element:

- “Changes to the ssh-rand-helper command that might require a migration action”
- “Changes to the sftp command that might require a migration action” on page 238
- “Changes to the ssh command that might require a migration action” on page 238
- “Changes to the ssh, sftp or scp client commands that might require a migration action” on page 238
- “Changes to the ssh_config file that might require a migration action” on page 239
- “Changes to the sshd command that might require a migration action” on page 239
- “Changes to the ssh, sftp or scp client commands that might require a migration action” on page 238
- “Changes to the sshd_config file that might require a migration action” on page 239
- “Changes to the ssh-keygen command that might require a migration action” on page 240
- “Changes to the ssh-keyscan command that might require a migration action” on page 240
- “Changes to the users running ssh, sftp or scp client commands that might require a migration action” on page 240
- “Changes to /samples/ssh_smf.h and FOTSMF77 in SYS1.MACLIB that might require a migration action” on page 241

Changes to the ssh-rand-helper command that might require a migration action: Table 164 lists the changes to the **ssh-rand-helper** command that might require a migration action and the accompanying actions.

Table 164. Changes to the ssh-rand-helper command that might require a migration action

What changed	Migration action needed?
The ssh-rand-helper command Now, the ssh-rand-helper is not supported.	Yes. If no migration action, the following message is returned: FOTS1949 PRNG is not seeded. Please activate the Integrated Cryptographic Service Facility (ICSF). Action: The new OpenSSH requires that a working /dev/random device be available to all OpenSSH client and server jobs. This requires that ICSF be configured to support /dev/random and that users have SAF authority to the CSFRNG service.

Migration actions from z/OS V2R1: OpenSSH

Changes to the sftp command that might require a migration action: Table 165 lists the changes to the **sftp** command that might require a migration action and the accompanying actions.

Table 165. Changes to the sftp command that might require a migration action

What changed	Migration action needed?
<p>The -P option</p> <p>Previously, this option was used to specify the <code>sftp_server_path</code>. Now, this option is used to specify the port to connect to on the remote host.</p>	<p>Yes, if you specify the <code>sftp_server_path</code>. If you specify -P <code>sftp_server_path</code>, the following message is returned: FOTS1401 filename line number: Bad line number</p> <p>Action: Use the -D option to specify the <code>sftp_server_path</code>.</p>
<p>ln and symlink subcommands</p> <p>Previously, the ln and symlink subcommands created a symbolic link from <code>oldpath</code> to <code>newpath</code> on the remote host. Now, if the -s flag is specified, the created link is a symbolic link. Otherwise it is a hard link.</p>	<p>Yes, if you create a symbolic link.</p> <p>Action: Run the sftp ln subcommand with the -s flag to create a symbolic link or create a hard link without the flag.</p>

Changes to the ssh command that might require a migration action: Table 166 lists the changes to the **ssh** command that might require a migration action and the accompanying actions.

Table 166. Changes to the ssh command that might require a migration action

What changed	Migration action needed?
<p>The -I option</p> <p>Previously, the argument was the device that ssh should use to communicate with a smart card used for storing the user's private RSA key. Now, the argument is the PKCS#11 shared library ssh should use to communicate with a PKCS#11 token providing the user's private RSA key.</p>	<p>No, because the option (-I smartcard_device) is not supported on z/OS systems.</p>
<p>The -R options</p> <p>Previously, the port argument "0" was not supported. Now, if the port argument is "0", the listen port will be dynamically allocated on the server and reported to the client at run time.</p>	<p>No, setting the port argument to 0 was considered to be illegal in the previous version.</p>

Changes to the ssh, sftp or scp client commands that might require a migration action: Table 167 lists the changes to the **ssh** command that might require a migration action and the accompanying actions.

Table 167. Changes to the users running the ssh, sftp, or scp client commands that might require a migration action

What changed	Migration action needed?
<p>Users running ssh, sftp, or scp client commands when collecting SMF records.</p> <p>New SMF subtype records have been added, which requires additional setup.</p>	<p>Yes, if you use ssh, sftp, or scp client commands to collect SMF records.</p> <p>Set up the users who run ssh, sftp, or scp client commands to have READ access to the BPX.SMF SAF profile. For example:</p> <pre>RDEFINE FACILITY BPX.SMF UACC(NONE) PERMIT BPX.SMF CLASS(FACILITY) ID(userid) ACCESS(READ) SETROPTS RACLIST(FACILITY) REFRESH</pre>

Changes to the ssh_config file that might require a migration action: Table 168 lists the changes to the ssh_config file that might require a migration action and the accompanying actions.

Table 168. Changes to the ssh_config file that might require a migration action

What changed	Migration action needed?
<p>The ControlPath keyword</p> <p>Previously, %l in the path was substituted by the local host name. Now, %l in the path is substituted by the local host name (including any domain name).</p>	<p>Yes, if you want to use substitute character to substitute the local host name without any domain name.</p> <p>Action: Use the %L in the path to substitute the first component of the local host name.</p>
<p>The RemoteForward keyword</p> <p>Previously, the port argument "0" was not supported. Now, if the port argument is "0", the listen port will be dynamically allocated on the server and reported to the client at run time.</p>	<p>No, set the port argument to 0 was considered to be illegal in the previous version.</p>
<p>The RhostsAuthentication keyword</p> <p>Previously, this option was supported for protocol version 1. Now this option is no longer supported for protocol version 1 on z/OS UNIX.</p>	<p>Yes, if you use RhostsAuthentication for protocol version 1 in your application. When setting this, you will receive the following message: filename line line_number: Deprecated option keyword.</p> <p>Action: Update your application.</p>

Changes to the sshd command that might require a migration action: Table 169 lists the changes to the sshd command that might require a migration action and the accompanying actions.

Table 169. Changes to the sshd command that might require a migration action

What changed	Migration action needed?
<p>The -b option</p> <p>Previously, the default number of bits in the ephemeral protocol version 1 server key was 768. Now, the default number of bits in the ephemeral protocol version 1 server key is 1024.</p>	<p>Yes, if you use the ephemeral protocol version 1 server key which is 768 bits.</p> <p>Action: Start the sshd daemon with specifying -b 768.</p>

Changes to the sshd_config file that might require a migration action: Table 170 lists the changes to the sshd_config file that might require a migration action and the accompanying actions.

Table 170. Changes to the sshd_config file that might require a migration action

What changed	Migration action needed?
<p>The RhostsAuthentication keyword</p> <p>Previously, this option was supported for protocol version 1. Now, this option is no longer supported for protocol version 1 on z/OS Unix.</p>	<p>Yes, if you use RhostsAuthentication for protocol version 1 in your application. When setting it, the following message is returned: F0TS2374 filename line line_number: Deprecated option keyword" is returned.</p> <p>Action: Update your application.</p>
<p>The ServerKeyBits keyword</p> <p>Previously, the default number of bits in the ephemeral protocol version 1 server key was 768. Now, the default number of bits in the ephemeral protocol version 1 server key is 1024.</p>	<p>Yes, if you use the ephemeral protocol version 1 server key which is 768 bits.</p> <p>Action: Start the sshd daemon with specifying -b 768, if you want to use the old default.</p>

Migration actions from z/OS V2R1: OpenSSH

Changes to the ssh-keygen command that might require a migration action: Table 171 lists the changes to the `ssh-keygen` command that might require a migration action and the accompanying actions.

Table 171. Changes to the `ssh-keygen` command that might require a migration action

What changed	Migration action needed?
<p>-d option</p> <p>Previously, -d option as alias of -t dsa was supported. Now, it is not supported.</p>	<p>Yes, if you use ssh-keygen command with -d option. Specifying the -d option will return the following error message: unknown option -- d.</p> <p>Action: Replace -d by -t dsa.</p>
<p>-b option (used in conjunction with -G)</p> <p>Previously, the minimum value on the ssh-keygen -b option used with -G options was 768. Now the minimum value is 512.</p>	<p>No. Because minimum value 512 is less than 768.</p>
<p>-b option (for RSA)</p> <p>Previously, the maximum RSA key size on the ssh-keygen -b option was 32768. Now the maximum size is 16384.</p>	<p>Yes, if you are using ssh-keygen to generate RSA keys with a size that is between 16384 and 32768 bits. If you specify an RSA key size larger than 16384, the following error message will be returned: key bits exceeds maximum 16384.</p> <p>Action: Use ssh-keygen to generate new RSA keys based on the new size requirement.</p>

Changes to the ssh-keyscan command that might require a migration action: Table 172 lists the changes to the `ssh-keyscan` command that might require a migration action and the accompanying actions.

Table 172. Changes to the `ssh-keyscan` command that might require a migration action

What changed	Migration action needed?
<p>The -t option</p> <p>Previously, if the -t option was not specified, ssh-keyscan searches only for SSH protocol version 1 keys ("rsa1") by default. Now, if the -t option is not specified, ssh-keyscan searches only for SSH protocol version 2 "rsa" and "ecdsa" keys by default.</p>	<p>Yes, if you search protocol version 1 keys ("rsa1") without specifying -t option.</p> <p>Action: Search protocol version 1 keys ("rsa1") with specifying -t rsa1 .</p>

Changes to the users running ssh, sftp or scp client commands that might require a migration action: Table 173 lists the changes to the users running the `ssh`, `sftp`, or `scp` commands that might require a migration action and the accompanying actions.

Table 173. Changes to the users running `ssh`, `sftp` or `scp` client commands that might require a migration action

What changed	Migration action needed?
<p>Users running ssh, sftp or scp client commands when collecting SMF records.</p> <p>New SMF subtype records have been added which requires additional setup.</p>	<p>Yes, if you use ssh, sftp or scp client commands to collect SMF records.</p> <p>Action: Setup the users who run ssh, sftp or scp client commands to have READ access to the BPX.SMF SAF/RACF profile. For example:</p> <pre>RDEFINE FACILITY BPX.SMF UACC(NONE) PERMIT BPX.SMF CLASS(FACILITY) ID(userid) ACCESS(READ) SETROPTS RACLIST(FACILITY) REFRESH</pre>

Changes to /samples/ssh_smf.h and FOTSMF77 in SYS1.MACLIB that might require a migration action: Table 174 lists the changes to /samples/ssh_smf.h and FOTSMF77 in SYS1.MACLIB that might require a migration action and the accompanying actions.

Table 174. Changes to /samples/ssh_smf.h and FOTSMF77 in SYS1.MACLIB that might require a migration action

What changed	Migration action needed?
<p>/samples/ssh_smf.h and SYS1.MACLIB(FOTSMF77)</p> <p>Now, new Ciphers and MACs, new subtypes (Client Connection Started 94 and Server Connection Started 95), and SFTP target path have been updated to the ssh_smf.h and FOTSMF77.</p> <p>For more information, see the topic on SMF Type 119 records in <i>IBM Ported Tools for z/OS: OpenSSH User's Guide</i>.</p>	<p>Yes, if you use ssh_smf.h and FOTSMF77.</p> <p>Action: Update your application.</p>

z/OS UNIX migration actions

This topic describes migration actions for base element z/OS UNIX System Services (z/OS UNIX).

z/OS UNIX actions to perform before installing z/OS V2R2

This topic describes z/OS UNIX migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Migrate from HFS file systems to zFS file systems

Description

Before z/OS V1R7, the HFS file system was the primary hierarchical file system. As of z/OS V1R7, you can use any combination of HFS and zFS file systems. Because zFS has higher performance characteristics than HFS and is the strategic file system, you should migrate your HFS file systems to zFS.

The HFS and zFS file system types in mount statements and command operands are now generic file system types that can mean either HFS or zFS. Based on the data set type, the system will determine which is appropriate. But note that you must still specify a type (HFS or zFS and it cannot be defaulted), and if the type you specify is not correct for the file system being mounted, any associated parameter string setting in the mount statement or command is ignored, even though the system sets the type correctly and processes the mount.

Table 175 provides more details about this migration action. Use this information to plan your changes to the system.

Table 175. Information about this migration action

Element or feature:	z/OS UNIX.
When change was introduced:	z/OS Distributed File Service zFS became the strategic file system in z/OS V1R7.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.

Migration actions from z/OS V2R1: z/OS UNIX

Table 175. Information about this migration action (continued)

Is the migration action required?	No, but recommended because the action is planned to become a requirement in a future release. zFS is the strategic file system for z/OS UNIX and continues to be enhanced to provide superior performance, reliability, and data integrity. z/OS V2R2 supports HFS file systems.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	<ul style="list-style-type: none">• Understand the zFS recommendations and limits. For more information, see “Minimum and maximum file sizes” in <i>z/OS Distributed File Service zFS Administration</i>• The DDNAME() keyword of the BPXPRMxx ROOT and MOUNT statements is not supported by zFS. Use the FILESYSTEM(<i>name</i>) keyword instead.
System impacts:	None.
Related IBM Health Checker for z/OS check:	Use check USS_HFS_DETECTED to verify all file systems mounted. This check issues exception message BPXH068E if any HFS file systems are found.

Steps to take

Follow these steps:

1. Before beginning the migration, do the following:

- Ensure that the PTF for APAR OA46639 is installed on your system. This APAR corrects a problem that can occur when socket type files are copied.
- Establish backout procedures.
- Decide on naming conventions.
- Decide on unavailability.
- Understand any cloning or deployment changes required by zFS systems being linear data sets. Considerations would include any copy utility invocations, BPXPRMxx specifications for symbolics, and placement of zFS file systems on system volumes.

2. Perform the conversion from an HFS to zFS file system.

You can use the BPXWH2Z tool to perform the conversion. It is an ISPF-based tool that migrates HFS file systems to zFS file systems. Using its panel interface, you can alter the space allocation, placement, SMS classes, and data set names. A HELP panel is provided. With this tool, you can:

- Migrate HFS file systems (both mounted and unmounted) to zFS file systems. If the HFS being migrated is mounted, the tool automatically unmounts it and then mounts the new zFS file system on its current mount point.
- Define zFS aggregates by default to be approximately the same size as the HFS. The new allocation size can also be increased or decreased. In z/OS V1R13, ZFS could require up to four times (4X) the space that HFS did; therefore, for z/OS V2R1 be sure to allocate more space. See zFS: Accommodate new DASD space requirements.
- Have the migration run in TSO/E foreground or UNIX background.

You can use the JCL sample ISPBTCH in SYS1.SAMPLIB to invoke BPXWH2Z as an ISPF batch job. Before you run the job, read the Notes section. When you run BPXWH2Z on your z/OS system, make

sure it uses that same z/OS level of the `pax` command. You can manually migrate from an HFS to zFS file system without using the tool. However, you would need to allocate and format the target zFS file systems.

You can use the JCL sample `ISPBTCH` in `SYS1.SAMPLIB` to invoke `BPXWH2Z` as an ISPF batch job. Before you run the job, read the notes section. When you run `BPXWH2Z` on your z/OS V1R13 system, it uses the z/OS V1R13 level of the `pax` command. This level was enhanced in z/OS V1R7 for sparse file support and other characteristics that are of concern when migrating from an HFS to zFS file system. You can manually migrate from an HFS to zFS file system without using the tool. However, you would need to allocate and format the target zFS file systems.

Requirement: The `BPXWH2Z` tool requires the zFS address space to be operational. Therefore, before attempting to migrate existing HFS to zFS file systems using `BPXWH2Z`, make sure that the zFS address space has been successfully configured and initialized.

Tip: You can dynamically migrate the HFS sysplex root in a shared file system configuration to zFS while the root is in use, without disrupting workloads. Although the shared file system configuration is required, the sysplex can be a single system. For the steps involved in migrating the sysplex root file system from HFS to zFS, see “Migrating the sysplex root file system from HFS to zFS after IPLing z/OS V1R12”.

3. Change policies and scripts, and so forth, to reflect the change from the HFS file system to zFS file system. Use the RMF Monitor III option to report on zFS activity. Refer to migration action “Monitor the zFS file system activity” for information on gathering zFS activity in RMF Monitor III.

Tip: Use the RMF Monitor III option to report on zFS activity.

4. The `DDNAME(name)` keyword of the `BPXPRMxx ROOT` and `MOUNT` statements is not supported by zFS. If you use them, change these statements to use the `FILESYSTEM(name)` keyword instead.

Migrating the sysplex root file system from HFS to zFS after IPLing your previous z/OS system:

Before you begin the migration:

- Ensure that the following requirements have been met:
 - All systems in the sysplex are at the V1R12 level.
 - The current sysplex root file system PFS, and the new sysplex root file system PFS, are up in all the systems in shared file system configuration.
- Be aware of the following restrictions:
 - The current sysplex root file system must be mounted as a read-only file system.
 - The systems that do not meet the requirements for this migration action cannot join the sysplex during the sysplex root file system migration processing, but they can join the sysplex after the sysplex root migration has completed.
 - The current sysplex root and the new sysplex root must be either HFS or zFS in any combination. If the new sysplex root is zFS, then it must be HFS-compatible.
 - The sysplex root or any directories on it cannot have been exported by the DFS or SMB server.
- Note the following:
 - Remote NFS mounts of the sysplex root or any directories on it are considered active use of the current sysplex root file system.
 - During the migration, the new zFS sysplex root file system must not be HSM-migrated, mounted, or in use.
 - Mount parameters are preserved during the migration or replacement of the sysplex root file system of the same file system type (PFS). They are dropped if the file system type is different.
 - Directories, data, files, and links are not copied from one file system to another.

Perform the migration as follows:

Migration actions from z/OS V2R1: z/OS UNIX

1. Ensure that a file system has been mounted read-only as the current sysplex root file system. When the root is mounted read-only, there are no function-shipping clients as long as physical paths to the DASD are available to each system. To verify that there are no function-shipping clients, issue:

```
D OMVS,F,NAME=root_file_system_name
```

You should see CLIENT=N on each system.

2. Allocate and set up the new zFS sysplex root file system:
 - a. Create a new zFS file system to be used as the new sysplex root file system. *z/OS Distributed File Service zFS Administration* discusses creating and managing zFS file systems.

Rules:

- The UID, GID and the permission bits of the root directory in the new sysplex root file system must be same as the root directory in the current sysplex root file system.
 - If the SECLABEL class is active and the MLFSOBJ option is active, the security label for the new zFS file system must match the assumed security label of the current sysplex root file system.
- b. On the new sysplex root file system, set up the active mount points and the symbolic links. The mount points and symbolic links must be the same as the ones on the current sysplex root file system. You can set them up either (1) manually or (2) by using the **pax** shell command to populate the new sysplex root file system using the existing sysplex root as a source. To do it manually, create a mount point in the existing sysplex root (for example, /newroot) and mount the new sysplex root file system in the MODE(RDWR) on that mount point. After mounting the new sysplex root file system, manually issue MKDIRS and ln -s to create the mount point directories and symbolic links similar to the existing sysplex root file system. Note that the new sysplex root file system must contain all active mount points and symbolic links exactly as on the existing sysplex root file system.
 - c. Use the **pax** shell command to populate the new file system, using the existing sysplex root as a source.

Example:

```
cd /  
pax -wr -pe -XCM ./ /newroot
```

For more information about using **pax** to copy data from an HFS file system to a zFS file system, see *z/OS Distributed File Service zFS Administration*.

- d. Unmount the new zFS file system.
3. On any system in the shared file system configuration, issue:

```
F OMVS,NEWROOT=new.root.file.system.name,COND=<Yes|No>
```

- YES** Proceed conditionally. The system checks for active usage in the current sysplex root file system and reports the active usage in a BPXF245I message. If file activity is found, the command fails with EBUSY return code and JrActivityFound reason code. If file activity is not found, the command continues processing to replace the sysplex root. YES is the default.
- NO** Proceed unconditionally. The system checks for active usage in the current sysplex root file system and reports the active usage in a BPXF245I message. Replacement of the sysplex root file system will continue.

The migration of the sysplex root file system will begin. During the migration, active connections to files and directories in the current sysplex root file system are broken.

After the migration completes:

- The root CWD('/') is updated on all systems in the sysplex to point to the new sysplex root file system.
- New opens go to the new sysplex root file system. The current sysplex root for the root directory is replaced for all processes in all systems. The current directory for root directory is replaced for any processes using it

- Old connections in the previous sysplex root file system might get EIO errors.
4. Update the TYPE parameter and name of the sysplex root file system in the BPXPRMxx member of SYS1.PARMLIB. Because the DDNAME() keyword of the BPXPRMxx ROOT and CMOUNT statements is not supported by zFS, change these statements to use the FILESYSTEM(name) keyword instead.

Reference information

For more information, see the following references:

- For more information about the HFS and zFS file systems, see *z/OS UNIX System Services Command Reference*.
- To read about setting up zFS, see *z/OS Distributed File Service zFS Administration*.
- For information about the pax command, see *z/OS UNIX System Services Command Reference*.

Determine whether your system has z/OS UNIX program files with certain attributes

Description

Before z/OS V2R2 and without the PTFs for APAR OA45793 installed, the sticky attribute was honored when either the set-user-id or set-group-id attributes were set. Starting with z/OS V2R2, APAR OA45793 changes the behavior of the exec (BPX1EXC or BPX4EXC) and spawn (BPX1SPN or BPX4SPN) interfaces when the user-specified path name resolves to a file that has the sticky attribute and either the set-user-id or set-group-id attributes. The exec and spawn services now ignore the sticky attribute unless a new RACF FACILITY class profile indicates that the usage is acceptable. Ignoring the sticky attribute means that the MVS program search order will not be used to locate the target program; only the z/OS UNIX program file that is identified by the user-specified path name is used.

EC6 abends with reason code xxxxE055 occur if the program is found in the MVS program search and no matching FACILITY class profile is found. If the program is not found in the MVS program search order, the z/OS UNIX file is run, which is the current behavior of exec and spawn.

Table 176 provides more details about this migration action. Use this information to plan your changes to the system.

Table 176. Information about this migration action

Element or feature:	z/OS UNIX
When change was introduced:	z/OS V2R1, z/OS V1R13, and z/OS V1R12, all with APAR OA45793 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13 both without APAR OA45793 applied.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you have a program that fits the criteria in the Steps to take section.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Migration actions from z/OS V2R1: z/OS UNIX

Steps to take

Follow these steps:

1. Determine whether any of your program files have the sticky attribute and either the set-user-id or set-group-id attributes. For each program file that has the sticky attribute and either the set-user-id or set-group-id attribute, select one of the following actions:

- If you do not want the exec and spawn services to use the MVS search order to locate programs, you do not need to take any action.
- If you want the exec and spawn services to always use the MVS search order for certain programs, then specify:

```
BPX.STICKYSUG.YOURPGM  
BPX.STICKYSUG.MYPGM
```

- If you want the exec and spawn services to use the MVS search order for a group of commonly named programs, then define a generic profile:

```
BPX.STICKYSUG.MYP*
```

The exec and spawn services will use the MVS search order for any program that begins with the characters MYP. The minimum allowable generic file is BPX.STICKYSUG.*.

After you complete the steps, you have determined how program files that have the sticky attribute and either the set-user-id or set-group-id attributes are to be handled.

Reference information

For more information, see *z/OS UNIX System Services Programming: Assembler Callable Services Reference*.

z/OS UNIX actions to perform before the first IPL of z/OS V2R2

This topic describes z/OS UNIX migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Remove files and directories in /var/man

Description

Before z/OS V2R2, the /var/man directory was used by the **man** command. Starting with z/OS V2R2, the **man** command does not use this directory. Instead, it uses the /tmp directory on a per-user basis.

Table 177 provides more details about this migration action. Use this information to plan your changes to the system.

Table 177. Information about this migration action

Element or feature:	z/OS UNIX
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use the man command to view the man pages.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.

Table 177. Information about this migration action (continued)

System impacts:	For temporary directory considerations, see “Steps to take.”
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Remove the `/var/man` directory and all subdirectories and files on your z/OS V2R2 system. These files are no longer used for the z/OS V2R2 `man` command.
2. The z/OS V2R2 `man` command uses the temporary directory for caching man pages. Each user has their own man page cache in the temporary directory. This change might increase the size of the temporary directory, depending on how much man command usage there is on your system. Monitor space usage for the temporary directory to ensure that there is adequate space for users to issue the `man` command. The temporary directory can be the directory referred to by the `TMPDIR` environment variable, or `/tmp` if `TMPDIR` is not defined.

Reference information

For more information about the `man` command, see *z/OS UNIX System Services Command Reference*.

z/OS UNIX actions to perform after the first IPL of z/OS V2R2

This topic describes z/OS UNIX migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

Migration actions from z/OS V2R1: z/OS UNIX

Chapter 4. Migration from z/OS V1R13

Chapter 4 describes those actions for anyone who is migrating from z/OS V1R13.

Sysplex migration actions

This topic summarizes actions for you to take if you are migrating systems that are members of a base sysplex or Parallel Sysplex configuration.

Sysplex actions related to hardware upgrades

Title of migration action	Page or topic
"Migrate to an IBM z13 or IBM z13s server" on page 43	"Migrate to an IBM z13 or IBM z13s server" on page 43
"Migrate to an IBM zEnterprise EC12 or IBM zEnterprise BC12 server" on page 60	"Migrate to an IBM zEnterprise EC12 or IBM zEnterprise BC12 server" on page 60
"Migrate to an IBM zEnterprise z196 or z114 server" on page 72	"Migrate to an IBM zEnterprise z196 or z114 server" on page 72
"Update your CFRM policy with coupling facility structure size changes" on page 89	"Update your CFRM policy with coupling facility structure size changes" on page 89
"Relocate Cross System Extended Services (XES) component trace buffers" on page 113	"Relocate Cross System Extended Services (XES) component trace buffers" on page 113
"Consider the new COUPLExx CFRMTAKEOVERCF(NO) default" on page 128	"Consider the new COUPLExx CFRMTAKEOVERCF(NO) default" on page 128

Sysplex actions to perform before installing z/OS V2R2

Element or feature	Title of migration action	Page or topic
Multiple	"Install coexistence and fallback PTFs" on page 6	"Install coexistence and fallback PTFs" on page 6
BCP	"Use LOGR Couple Data Set at format level HBB7705" on page 95	"Use LOGR Couple Data Set at format level HBB7705" on page 95
DFSMSdfp	"DFSMSdfp: Back up SMS control data sets" on page 168	"DFSMSdfp: Back up SMS control data sets" on page 168

Sysplex actions to perform before the first IPL of z/OS V2R2

Element or feature	Title of migration action	Page or topic
BCP	"Format the ARM couple data set for long symbol table support" on page 105	"Format the ARM couple data set for long symbol table support" on page 105
BCP	"Relocate Cross System Extended Services (XES) component trace buffers" on page 113	"Relocate Cross System Extended Services (XES) component trace buffers" on page 113
BCP	"Consider the new COUPLExx CFRMTAKEOVERCF(NO) default" on page 128	"Consider the new COUPLExx CFRMTAKEOVERCF(NO) default" on page 128

Sysplex actions to perform after the first IPL of z/OS V2R2

None.

BCP migration actions

This topic describes migration actions for the base element BCP (Base Control Program).

BCP actions to perform before installing z/OS V2R2

This topic describes BCP migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Evaluate your stand-alone dump data set allocations and your IPCS processing of them

Description

As your applications grow in size and use greater amounts of storage, you should evaluate whether the DASD allocated for your stand-alone dump data continues to be adequate.

In z/OS V1R6, support was introduced for extended-format sequential data sets, a form of data set that is SMS-managed and can occupy more than 64 K tracks per volume. In z/OS V1R7, this support was supplemented with support for large format sequential data sets (DSNTYPE=LARGE), a form of data set that is essentially the same as conventional sequential data sets except that more than 64 K tracks may be spanned per volume. If your stand-alone dump data sets are spread over more volumes than you want, both types of support can help you gain better control over the number of volumes used for each stand-alone dump data set.

Table 44 on page 92 provides more details about the migration action. Use this information to plan your changes to the system.

Table 178. Information about this migration action

Element or feature:	BCP.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.

Table 178. Information about this migration action (continued)

Is the migration action required?	No, but recommended because of changes that have been made to stand-alone dump processing (that reorder dump records with the intent of recording more important data early), and especially recommended if you deploy any LPARs with significantly more main storage than previously used.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Use multivolume stand-alone dump data sets. Adjust the number of volumes and their separation to achieve tolerable stand-alone dump capture times.
- Use extended-format sequential data sets or large format sequential data sets. Copy their contents to an extended-format, compressed, striped data set using the IPCS COPYDUMP subcommand before analysis. Use the same or a larger striping factor than you used for your stand-alone dump data sets. Dump data sets to which stand-alone dump can write may be neither compressed nor striped, but both attributes are advantageous for the target of the copy operation. Starting with z/OS V1R12, stand-alone dump data sets can be placed in track-managed space as well as cylinder-managed space on Extended Address Volumes (EAV).
- Use a large CISIZE and striping for IPCS dump directories, and use blocking, striping, and compression for the stand-alone dump data set. Very large stand-alone dumps might require that you define your directory with the extended addressing attribute, allowing it to hold more than 4 GB.

Tip: Control interval sizes less than 24K have been shown to be more vulnerable to fragmentation when used as IPCS dump directories, and IPCS performance can be degraded when such fragmentation occurs. In this background, warning message BLS21110I will be issued and you might recreate the DDIR by using the CLIST BLSCDDIR.

BLS21110I CISIZE(cisize) is less than 24K. It may degrade IPCS performance

Reference information

For more information, see the following references:

- For information about dump data set allocation, extended format sequential data sets, large format sequential data sets, and multivolume dump data sets, see *z/OS MVS Diagnosis: Tools and Service Aids*.
- For stand-alone dump procedures, see *z/OS V2R2 Problem Management*.

AMBLIST uses the system-determined block size for SYSPRINT Description

With APAR OA46441 applied, the AMBLIST utility uses the system determined block size when it creates the SYSPRINT data set. Before APAR OA46441, AMBLIST used (by default) a block size equal to the record length for allocating the SYSPRINT data set, if the block size was not specified or was specified as 0.

Migration actions from z/OS V1R13: BCP

Table 45 on page 94 provides more details about this migration action. Use this information to plan your changes to the system.

Table 179. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V2R1 and z/OS V1R13, both with APAR OA46441 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA46441.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you expect the SYSPRINT data set that is created by AMBLIST to have a block size other than the system determined block size.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	If a program opens the SYSPRINT data set created by AMBLIST with DCB RECFM=FA or RECFM=FA, LRECL=121 parameters, the program is abended with message IEC141I 013-60.
Related IBM Health Checker for z/OS checks:	None.

Steps to take

Check for JCL and programs that use the AMBLIST utility to write SYSPRINT output to a sequential data set, and ensure that block sizes are specified explicitly where appropriate. For example, suppose that a program that refers to the SYSPRINT data set expects a new SYSPRINT data set to have a block size of 121 (BLKSIZE=121). If so, you must specify this value explicitly in the SYSPRINT DD statement when you run the AMBLIST utility. For any programs that open the SYSPRINT data set with the DCB parameters RECFM=FA or RECFM=FA, LRECL=121, remove the RECFM and LRECL parameter from the DCB macro. Or, change the record format value to FBA (RECFM=FBA).

Reference information

For more information about the AMBLIST utility, see *z/OS MVS Diagnosis: Tools and Service Aids*.

Plan to move from SHARED mode to DISTRIBUTED mode for consoles

Description

z/OS V2R2 is the last release in which the SHARED console mode is supported. You must migrate to DISTRIBUTED mode, which was introduced in z/OS V1R10.

Table 46 on page 94 provides more details about the migration action. Use this information to plan your changes to the system.

Table 180. Information about this migration action

Element or feature:	BCP
When change was introduced:	See <i>Statement of direction: IBM z/OS IBM United States Software Announcement 212-086 April 11, 2012</i>
Applies to migration from:	z/OS V2R1 and z/OS V1R13.

Table 180. Information about this migration action (continued)

Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended if you are using SHARED console mode. When shared mode is removed, you are required to move to DISTRIBUTED mode.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	Fallback considerations exist; see topic on migration and fallback considerations in <i>z/OS MVS Planning: Operations</i> .
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	Use check IBM CNZ,CNZ_CONSOLE_OPERATING_MODE to determine whether your installation is operating in the DISTRIBUTED console mode, which is preferred.

Steps to take

Move from SHARED mode to DISTRIBUTED mode for your console environment. Note that the default changed from SHARED to DISTRIBUTED mode in z/OS V1R13.

Tip: You can check the current mode by using the command **DISPLAY OPDATA,MODE**.

Reference information

For more information, see the following references:

- *Statement of direction: IBM z/OS IBM United States Software Announcement 212-086 April 11, 2012.*
- For DISTRIBUTED mode, see *z/OS MVS Planning: Operations*

Make accommodations for RACROUTE AUTH check for SLIP command Description

As of z/OS V2R1, a RACROUTE AUTH check is performed for a SLIP command that is issued with action of REFAFTER or REFBEFOR. This change might affect your installation, depending on the security product you are using.

Table 181 provides more details about this migration action. Use this information to plan your changes to the system.

Table 181. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V2R1
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you are use a SLIP command with Action of REFAFTER or REFBEFOR and are using a security product that is affected by the additional RACROUTE AUTH check.
Target system hardware requirements:	See "Steps to take" on page 254.
Target system software requirements:	None.

Migration actions from z/OS V1R13: BCP

Table 181. Information about this migration action (continued)

Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you use the z/OS RACF security product, there is no action to take. If you use another security product, contact your vendor to see if there is any support or changes that you need to make.

Reference information

For more information, see *z/OS MVS System Commands*.

Remove the REPORTCOMPLETIONS option from the IEAOPTxx member Description

As of z/OS V1R13, support for the REPORTCOMPLETIONS=YES|NO option in the IEAOPTxx parmlib member is removed. This option was introduced with APAR OA34801 on November 24, 2010, and removed with APAR OA35428 on July 7, 2011. The setting REPORTCOMPLETIONS=YES was intended to provide a system-wide option for installations with a single large production environment, where all regions were exempted from being managed towards response time goals and you wanted to obtain response time statistics with different granularity through service and report classes. In all other cases, the usage of this option was not recommended.

The REPORTCOMPLETIONS=YES option was superseded by the “Manage Region Using Goal Of Both” option on the classification rule that allows to manage CICS Terminal Owning Regions (TORs) in a granular manner.

Table 182 provides more details about this migration action. Use this information to plan your changes to the system.

Table 182. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V1R13 with the PTF for APAR OA35428.
Applies to migration from:	z/OS V1R13 without the PTF for APAR OA35428.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended to avoid the information message, if you ever used the REPORTCOMPLETIONS parameter.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

To clean up the IEAOPTxx parmlib member, remove the REPORTCOMPLETIONS option. Otherwise, the REPORTCOMPLETIONS option is ignored with the following message:

```
IRA800I OPT MEMBER IEAOPTxx KEYWORD ReportCompletions IGNORED, NO LONGER USED
```

Reference information

For more information, see the documentation for APAR OA34801 and APAR OA35428.

Move BCPii API calls into your application instead of in BCPii ENF exits

Description

As stated in various IBM publications, non-SRB ENF exits need to avoid time-consuming processing. Coding an HWIEVENT ENF exit to execute BCPii APIs might result in multiple problems, such as delays with BCPii event notification processing when BCPii services are simultaneously being invoked. As of APAR OA38117 on z/OS V1R11, V1R12, and V1R13, BCPii enforces this restriction, and BCPii API calls made from within a BCPii ENF exit are now rejected with the return code HWI_UNSUPPORTED_ENVIRONMENT.

Table 183 provides more details about this migration action. Use this information to plan your changes to the system.

Table 183. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V1R11, V1R12, and V1R13 with APAR OA38117.
Applies to migration from:	z/OS V1R13 without the PTF for APAR OA38117 applied.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you have coded a BCPii API call from your ENF exit.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	BCPii API calls made from within a BCPii ENF exit are now rejected with return code HWI_UNSUPPORTED_ENVIRONMENT.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you have coded a BCPii API call from your ENF exit, move the BCPii API call into your application and have the BCPii ENF exit post the application when the event occurs. Your application program may now issue the BCPii API call from the user's thread.

For an example of how to code a BCPii ENF exit, see the sample ENF event exit HWIXMCX1 in SYS1.SAMPLIB.

Note: The sample ENF event exit HWIXMCX1 was corrected by APAR OA43767 for z/OS V2R1 and V1R13.

Migration actions from z/OS V1R13: BCP

Reference information

For more information, see *z/OS MVS Programming: Callable Services for High-Level Languages*.

Remove policies for the PFA_FRAMES_AND_SLOTS_USAGE check

Description

The PFA_FRAMES_AND_SLOTS_USAGE check no longer exists in Predictive Failure Analysis (PFA). Remove any policies you have in place for the PFA_FRAMES_AND_SLOTS_USAGE check.

Table 184 provides more details about this migration action. Use this information to plan your changes to the system.

Table 184. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V1R13 with APAR OA40065.
Applies to migration from:	z/OS V1R13 without APAR OA40065.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you have any policies in place for the PFA_FRAMES_AND_SLOTS_USAGE check.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Failure to remove some types of customization for the PFA_FRAMES_AND_SLOTS_USAGE check results in error messages.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Remove all IBM Health Checker for z/OS policy and non-policy statements in HZSPRMxx that refer to the PFA_FRAMES_AND_SLOTS_USAGE check.

Reference information

For more information, see *z/OS V2R2 Problem Management*.

Update code that invokes the IOSSPOF macro in a PSW key of 0-7

Description

The IOSSPOF macro changed to conditionally obtain the returned SPOFAREA in a different subpool depending on the caller's PSW key. This may cause the caller, depending on their current PSW key, to be required to change to a different PSW key if they want to update the storage. In addition, certain PSW key callers can no longer rely on the storage automatically being freed when the task ends. The subpool number continues to be returned in the SPOFAREA_SUBPOOL so that it can be used when the storage is freed.

The specific changes are:

- Key 0-7 callers: The returned SPOFAREA mapped by IOSDSPOF is obtained in subpool 252, which is key 0 storage, non-fetch-protected, and is associated with the jobstep task.

- Key 8-15 callers: The returned SPOFAREA mapped by IOSDSPOF continues to be obtained in subpool 1, which is fetch-protected storage with a key equal to the TCB key and is associated with the issuing task.

The specific restrictions are:

- Key 0-7 callers cannot rely on the SPOFAREA storage automatically being freed when the task ends. The area must now be explicitly freed and the caller must meet the state, key, and APF-authorization requirements for freeing from subpool 252.
- Key 1-7 callers must change to Key 0 in order to update the returned SPOFAREA storage.
- Key 8-15 callers must be in the PSW key of the TCB in order to access the SPOFAREA storage.

Table 185 provides more details about this migration action. Use this information to plan your changes to the system.

Table 185. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R1, and on z/OS V1R13 and z/OS V1R12 with APAR OA37035.
Applies to migration from:	z/OS V1R13 without APAR OA37035 applied.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you have code that invokes the IOSSPOF macro in a PSW key of 0-7.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

For any program that invokes the IOSSPOF macro in a PSW key of 0-7, ensure the following restrictions are followed:

- Key 0-7 callers: Because the subpool used for the SPOFAREA has changed from being associated with the issuing task to being associated with the jobstep task, be sure to free the storage if your task is not the jobstep task. In addition, make sure your storage-free invocation meets the state, key, and APF-authorization requirements for freeing from subpool 252.
- Key 1-7 callers: If the program attempts to write to the returned SPOFAREA, the program must switch to key 0 to update the area.

Reference information

For more information, see *z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG*.

Use LOGR Couple Data Set at format level HBB7705

Description

IBM recommends that you use the highest format level LOGR couple data set (CDS) that can be used by the lowest system release level in your sysplex. This will allow for the latest system logger features to be available, given the sysplex configuration. Currently, the highest LOGR CDS format level is HBB7705

Migration actions from z/OS V1R13: BCP

(introduced in z/OS V1R2). This format level is established by providing the ITEM NAME(SMDUPLEX) NUMBER(1) specification in the IXCL1DSU couple data set format utility program.

Table 47 on page 95 provides more details about the migration action. Use this information to plan your changes to the system.

Table 186. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V1R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended to allow for the latest system logger features to be available, given the sysplex configuration. If your LOGR couple data sets are already at HBB7705 level, this migration action does not apply to you.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	System Logger does not allow the introduction of an alternate LOGR CDS that is formatted at a lower-level than the primary.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Determine your current LOGR couple data set level. Use the **D XCF,C,TYPE=LOGR** command. If your LOGR couple data sets are at level HBB7705, you do not need to perform this migration action.
2. Use the IXCL1DSU (format couple data set utility) and include the ITEM NAME(SMDUPLEX) NUMBER(1) specification to obtain at least two LOGR CDSs at the HBB7705 format level, with:
 - LOGR CDS *primarydsname* on volume *primaryvolume*
 - LOGR CDS *alternatedsname* on volume *alternatevolume*

Note: SMDUPLEX item NUMBER(1) is the default value when you run the IXCL1DSU utility on z/OS V2R2.

3. After you create the HBB7705 format-level LOGR CDSs, you can dynamically bring them into your existing sysplex with these SETXCF commands:
 - SETXCF COUPLE,TYPE=LOGR,ACOUPL=(*primarydsname,primaryvolume*)
 - SETXCF COUPLE,TYPE=LOGR,PSWITCH
 - SETXCF COUPLE,TYPE=LOGR,ACOUPL=(*alternatedsname,alternatevolume*)
4. Remember to also specify, in your COUPLExx member of SYS1.PARMLIB, these two LOGR CDSs as the primary and alternate for any future sysplex IPLs:

```
DATA
TYPE(LOGR)
PCOUPLE(primarydsname,primaryvolume)
ACOUPLE(alternatedsname,alternatevolume)
```

Note: If you did not bring the newly formatted HBB7705 LOGR CDSs into the sysplex (with the SETXCF commands in the Step 3) prior to the first z/OS system that IPLs into the sysplex using the COUPLExx member identifying the newly formatted LOGR CDSs, then there will be no persistent logger data from before the IPL. Therefore, no log stream data exists when this first system IPLs.

Reference information

For more information, see the following references:

- For information about using the IXCL1DSU format couple data set utility for system logger, see the "LOGR parameters for format utility" section of *z/OS MVS Setting Up a Sysplex*.
- For considerations on the system logger functions that are supported using the different LOGR CDS format levels, see the "LOGR couple data set versioning - new format levels" section of *z/OS MVS Setting Up a Sysplex*.
- For details on the SETXCF command, see *z/OS MVS System Commands*.
- For information about the COUPLExx SYS1.PARMLIB member, see *z/OS MVS Initialization and Tuning Reference*.

Update Capacity Provisioning Manager parameters to use CIM Client for Java Version 2 Description

z/OS V2R1 was the last release to include Version 1 of the Standards Based Linux Instrumentation for Manageability (SBLIM) CIM client for Java. Version 1 support for SourceForge open source project was discontinued in 2010. Version 2 of the SBLIM client, which is designed to be a JSR48-compliant implementation, was included in z/OS V1R13 and z/OS V2R1. Users of SBLIM Version 1 must convert to Version 2.

Table 48 on page 97 provides more details about the migration action. Use this information to plan your changes to the system.

Table 187. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use SBLIM Version 1.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. The Provisioning Manager user CPOSRV needs READ access to CIM Client for Java Version 2 **sblim-cim-client.jar**. This access usually by default should be sufficient. If it is not, you must set the "other" READ access file permissions using the z/OS UNIX command **chmod** (for example, **chmod o+r/usr/lpp/wbem/jclient/sblim-cim-client2.jar**). Note that this command must be issued by a user with the appropriate authorization.

Migration actions from z/OS V1R13: BCP

2. If your CIM installation directory is not at the default location, you need to add the location of the CIM Client for Java Version 2 `slim-cim-client2.jar` to the CLASSPATH entry. If you have already specified the location of a previous version of the CIM Client Java, you need to add the location of CIM Client for Java Version 2 before the location of the previous version of CIM Client for Java. the CLASSPATH is specified in the ENV member of the Provisioning Manager runtime environment data set with prefix.PARM. The prefix for the data set name is the high-level qualifier of the Capacity Provisioning Manager parameters data set and the name of the domain managed by the Capacity Provisioning Manager. For example, with default values, the data set name is CPO.DOMAIN1.PARM.

Reference information

For more information, see *z/OS MVS Capacity Provisioning User's Guide*.

Update a Capacity Provisioning Manager parameter to avoid a defined capacity WTOR

Description

In z/OS V2R2, the Provisioning Manager can detect when a manual change to defined capacity or group capacity would interfere significantly with Capacity Provisioning management. In such cases, the Provisioning Manager suspends its management of defined capacity or group capacity and issues one of the following write-to-operator-with-reply (WTOR) messages:

CPO4218I

New DC for *systemName/sysplexName*. Previous base *previousLimit* MSU. Enter 1 to set base to *currentLimit* or 2 to set to *newLimit* MSU

CPO4219I

New GC for *groupName/CPCname*. Previous base *previousLimit* MSU. Enter 1 to set base to *currentLimit* or 2 to set to *newLimit* MSU.

In response, the operator can choose to reinitialize the capacity management by setting the management base to the new capacity value and its managed capacity to 0, or continue the capacity management by adapting the management base to the manual change.

If you want the Provisioning Manager to continue managing the defined capacity or group capacity, regardless of manual changes, you can suppress the WTOR by setting the key

DefinedCapacity.BaseToleration to 100 in the Capacity Provisioning Manager parameter file.

In z/OS V2R2, the default value of this key is 15, meaning that while Capacity Provisioning is managing a defined capacity, any concurrent manual reduction in defined capacity by more than 15% causes the WTOR to be issued.

Table 49 on page 98 provides more details about the migration action. Use this information to plan your changes to the system.

Table 188. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use Capacity Provisioning for managing defined capacity or group capacity and you want to avoid a WTOR for large manual reductions of defined capacity or group capacity.
Target system hardware requirements:	None.

Table 188. Information about this migration action (continued)

Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Add the entry `DefinedCapacity.BaseToleration=100` to the Capacity Provisioning parameter file. By default, the parameter file is named `CPO.DOMAIN1.PARM(PARM)`.

Reference information

For information about how to define the new key to the Capacity Provisioning Manager parameters, see *z/OS MVS Capacity Provisioning User's Guide*.

BCP actions to perform before the first IPL of z/OS V2R2

This topic describes BCP migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Create IPL text

Description

IPL text is bootstrap information required for IPL, such as the location of the nucleus library. You must create IPL text by running ICKDSF against the system residence volume.

Table 50 on page 99 provides more details about the migration action. Use this information to plan your changes to the system.

Table 189. Information about this migration action

Element or feature:	BCP.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

Migration actions from z/OS V1R13: BCP

- Update and run the IPLTEXT job to write a new copy of the IPL text. If you install z/OS with a ServerPac, an installation dialog job is provided to perform this action. If you install z/OS with a CBPDO, instructions to perform this action are provided in *z/OS Program Directory* at the z/OS installation related information website.

Tip: With ICKDSF R17 APAR PM42057, a new parameter called REMOVEIPLTXT has been added to the REFORMAT command that allows you to remove IPL text from the volume.

Note: When the IPLTXTEXTIST parameter (which was introduced by ICKDSF R17 APAR PK16403) is specified with the REFORMAT command using the IPLDD parameter, WTOR message ICK21836D is suppressed if IPL text already exists.

Reference information

For a sample IPLTEXT job, see *z/OS Program Directory* at the z/OS installation related information website. ServerPac provides a similar job for accomplishing this task; see *ServerPac: Installing Your Order*.

Review the list of WTORS in parmlib member AUTOR00 Description

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.

Table 51 on page 100 provides more details about the migration action. Use this information to plan your changes to the system.

Table 190. Information about this migration action

Element or feature:	BCP.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use the auto reply facility of z/OS, which is enabled by default when the AUTOR00 member is found in the parmlib concatenation, as of z/OS V1R12.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- 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.

Note: The IBM-shipped data set SYS1.IBM.PARMLIB contains the AUTOR00 member. So, if you specify it within the PARMLIB concatenation and will not intend to activate the auto reply functionality, you need to specify AUTOR=OFF in the IEASYSxx parmlib member.

Reference information

For more information, see the following references:

- For more information about the AUTORxx and IEASYSyy parmlib members, see *z/OS MVS Initialization and Tuning Reference*
- For the contents of AUTOR00, see *z/OS MVS Planning: Operations*.

Reassemble the stand-alone dump program Description

The stand-alone dump program produces a dump of storage that is occupied by a system that failed or a stand-alone dump program that failed. You must reassemble the stand-alone dump program each release. When the stand-alone dump program is properly created on a DASD residence volume, it resides in the SYS1.PAGEDUMP.Vvolser data set.

Table 52 on page 101 provides more details about the migration action. Use this information to plan your changes to the system.

Table 191. Information about this migration action

Element or feature:	BCP.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Reassemble the stand-alone dump program. If you install z/OS with a ServerPac, an installation dialog job is provided to perform this action. If you install z/OS with a CBPDO, instructions to perform this action are provided in *z/OS MVS Diagnosis: Tools and Service Aids*.

Reference information

For more information, see the following references:

- *ServerPac: Installing Your Order*
- *z/OS MVS Diagnosis: Tools and Service Aids*

Migration actions from z/OS V1R13: BCP

Plan for HWIREXX helper program restriction for z/OS BCPii

Description

Starting with z/OS V2R1, users of the z/OS BCPii System REXX helper program HWIREXX are required to have at least READ authority to the FACILITY class resource HWI.HWIREXX.execname as defined in the security product. This function is provided in APAR OA45932 with PTF UA75120.

Table 53 on page 101 provides more details about the migration action. Use this information to plan your changes to the system.

Table 192. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R1 with APAR OA45932.
Applies to migration from:	z/OS V2R1 without APAR OA45932 applied, and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use the BCPii helper program HWIREXX.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	The security product definitions as described need to be implemented to restrict use of the HWIREXX helper program.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- To allow you to run your BCPii System REXX exec using the HWIREXX helper program, you must have at least READ authority to the FACILITY class resource HWI.HWIREXX.execname, where *execname* specifies a 1 to 8 character System REXX exec to be executed by the HWIREXX helper application. Also, BCPii requires the FACILITY class to be RACLIST-specified.

The RACF syntax is as follows:

```
RDEFINE FACILITY HWI.HWIREXX.execname UACC(NONE)
PERMIT HWI.HWIREXX.execname CLASS(FACILITY) ID(userid) ACCESS(READ)
SETROPTS RACLIST(FACILITY) REFRESH
```

If the caller does not have sufficient SAF authorization to run the HWIREXX program, HWIREXX return code 112 (in decimal) is returned.

Reference information

For more information, see *z/OS MVS Programming: Callable Services for High-Level Languages*.

Move from the console tracking facility to the Generic Tracker

Description

Before z/OS V2R1, the console tracking facility was used to track use of system functions; however, it had some limitations. Starting with z/OS V2R1, the console tracking facility is being replaced with a new enhanced Generic Tracker. As of z/OS V2R1, support for the console tracking facility parmlib member,

CNIDTRxx, is no longer provided. The Generic Tracker accepts GTZPRMxx parmlib members, and a tool to convert CNIDTRxx to the Generic Tracker GTZPRMxx is also provided.

Table 193 provides more details about this migration action. Use this information to plan your changes to the system.

Table 193. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have started or customized the console tracking facility.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	It is assumed that the retired console tracking facility commands are typically issued manually and for diagnostic purposes only, not in any scripts or automation tools. The callable service CNZTRKR, compiled into executable programs, continues to be supported and the internal routing of any data passed to CNZTRKR and the Generic Tracker will be transparent to the existing CNZTRKR caller.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Replace the use of any console tracking facility commands. Use COMMNDxx, automation scripts, or manually enter the commands on the console command line with their corresponding Generic Tracker (GTZ) counterparts. You can use the following mapping as a quick reference:
 - Instead of using COMMNDxx to start the console tracking facility, use the new system parameter GTZ (in IEASYSxx) to specify a GTZPRMxx member that specifies the SETGTZ TRACKING=ON command.
 - Instead of the DISPLAY command, consider using utility GTZPRINT or a user-written program with the service GTZQUERY to retrieve, store, and process current tracking data.
 - Instead of SETCON TRACKING={ON|OFF}, use SETGTZ TRACKING={ON|OFF}
 - Instead of SETCON TRACKING=ONWITHABEND, use SETGTZ DEBUG(ACTION=ABEND...)
 - Instead of DISPLAY OPDATA,TRACKING, use DISPLAY GTZ command, the GTZPRINT tool, or the GTZQUERY macro service.
 - Instead of SET CNIDTR=xx, use SET GTZ=xx or system parameter GTZ in IEASYSxx
- Instead of having any SETGTZ commands in COMMNDxx, consider putting them into GTZPRMxx parmlib members. You can use the SET GTZ command or the GTZ system parameter in IEASYSxx to select and execute the content of those GTZPRMxx.
- For any new applications use macro GTZTRACK instead of macro CNZTRKR. Consider converting any existing use of CNZTRKR to GTZTRACK.
- Convert existing CNIDTRxx parmlib members to GTZPRMxx. See the sample GTZCNIDJ for how the GTZCNIDT conversion tool can help you automate this conversion.

Migration actions from z/OS V1R13: BCP

Reference information

For more information, see the following references:

- For details about SETGTZ, SET GTZ, DISPLAY GTZ, see *z/OS MVS System Commands* .
- For details about GTZTRACK and GTZQUERY, see *z/OS MVS Programming: Assembler Services Reference ABE-HSP*.
- For details about GTZPRMxx and IEASYSxx GTZ=, see *z/OS MVS Initialization and Tuning Reference*.

Convert your existing IBM Health Checker for z/OS setup for automatic start-up Description

Before z/OS V2R1, IBM Health Checker for z/OS users had to perform a set up procedure and start manually. As of z/OS V2R1 the system starts IBM Health Checker for z/OS automatically.

Table 194 provides more details about the migration action. Use this information to plan your changes to the system.

Table 194. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you are currently using the IBM Health Checker for z/OS and wish to continue to use it as you have customized it. This migration action is strongly recommended for those that have not used the IBM Health Checker for z/OS on each system yet.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	If you have not started IBM Health Checker for z/OS before, you will probably see exception messages. For information about how to handle the exceptions, see <i>IBM Health Checker for z/OS User's Guide</i>
Related IBM Health Checker for z/OS check:	None.

Steps to take

For first time users of IBM Health Checker for z/OS, follow the steps for optimizing IBM Health Checker for z/OS in *IBM Health Checker for z/OS User's Guide*.

For users with existing IBM Health Checker for z/OS setup, use the following migration actions to convert systems to the IBM Health Checker for z/OS automatic start-up:

1. Make sure the system knows the name of your HZSPROC procedure if you renamed it from the default HZSPROC: The start-up procedure for IBM Health Checker for z/OS is called HZSPROC, by default. If you customized your hzsproc name, you must specify it to the system, using the new HZSPROC system parameter in IEASYSxx.
2. Remove any existing START HZSPROC invocations that start IBM Health Checker for z/OS and rely on the automatic start-up: Because IBM Health Checker for z/OS now starts automatically, you must

look for instances of START HZSPROC invocations in your installation. For example, look for START HZSPROC invocations in the COMMNDxx, parmlib member.

After the system brings IBM Health Checker for z/OS up automatically, the system rejects any attempt to bring up a second instance. The system issues one of the two following warning messages:

```
HZS0101I - ...HEALTH CHECKER... IS ALREADY ACTIVE
```

or if the automatically started IPL-time instance is still initializing:

```
HZS0116I - ...HEALTH CHECKER... START PENDING
```

3. Change the way you specify the HZSPRMxx parmlib members you want the system to use: Before z/OS V2R1, users typically specified the HZSPRMxx parmlib members for IBM Health Checker for z/OS in the HZSPROC procedure. Now starting with z/OS V2R1, IBM recommends that you do the following to tell the system which members of HZSPRMxx to use:

- a. Specify the HZSPRMxx parmlib members for your installation in the new HZS system parameter of IEASYSxx. This provides the default for the automatic start of IBM Health Checker for z/OS at IPL-time.
- b. In your hzsproc procedure, default to or define HZSPRM='PREV':

```
//HZSPROC PROC HZSPRM='PREV'
//HZSSTEP EXEC PGM=HZSINIT,REGION=0K,TIME=NOLIMIT,
//          PARM='SET PARMLIB=&HZSPRM'
//*HZSPDATA DD DSN=SYS1.&SYSNAME..HZSPDATA,DISP=OLD
//          PEND
//          EXEC HZSPROC
```

- c. HZSPRM='PREV' specifies the following:

- For the initial automatic start, the system will use the HZSPRMxx suffixes listed in the HZS system parameter.
- For manual restarts after the initial automatic start, IBM Health Checker for z/OS initially uses the HZSPRMxx parmlib members that were in effect just before the previous Health Checker instance was stopped. This action will in particular include any parmlib members specified through a MODIFY HZSPROC,ADD,PARMLIB or MODIFY HZSPROC,REPLACE,PARMLIB command, while this first instance was running.

For example, assume HZSPRM=PREV was specified when that first instance was started and system parameter HZS was set to (00,01). Then this first instance would have initially used HZSPRM00 and HZSPRM01.

Now assume a MODIFY HZSPROC,ADD,PARMLIB=(02,03) was specified and then later this first instance is stopped. A manual restart, still with HZSPRM=PREV, will initially use HZSPRM00, HZSPMR01, HZSPRM02, and HZSPRM03, as in the previous instance before it was stopped.

If MODIFY HZSPROC,REPLACE,PARMLIB=(02,03) is used instead, the secondary instance initially only uses HZSPRM02 and HZSPRM03.

Specifying HZSPRM='PREV' makes occasional manual restarts (after applying service, for example) easy and consistent.

4. Optionally specify an HZSPDATA data set for persistent data in the HZSPRMxx parmlib member: Before z/OS V2R1, you could only specify the HZSPDATA in the HZSPROC startup procedure. Now you can define your HZSPDATA data set in either the HZSPROC startup procedure or on the HZSPDATA parameter of the HZSPRMxx parmlib member.

Reference information

For more information, see the following references:

- For system parameters HZS and HZSPROC, see IEASYSxx (system parameter list) in *z/OS MVS Initialization and Tuning Reference*.
- For information about specifying the HZSPRMxx parmlib members to be used, see *IBM Health Checker for z/OS User's Guide*.

Migration actions from z/OS V1R13: BCP

- For information about the HZSPROC procedure, see *IBM Health Checker for z/OS User's Guide*.
- For information about specifying the HZSPDATA data set for persistent data, see *IBM Health Checker for z/OS User's Guide*.

Consider the new default value for the LOADxx DYNCPADD keyword that indicates how many CPUs z/OS is prepared to dynamically add

Description

Before z/OS V2R1, through PARMLIB member LOADxx you could enable that CPUs be added to the configuration over the life of the IPL if the hardware supported such addition. The default was for all CPUs that could be configured to the LPAR, which was the minimum supported by the z/OS release (for example, 100) and the machine (for example, 80), and which could be asked for explicitly by DYNCPADD ENABLE. In z/OS V2R1, the LOADxx keyword DYNCPADD now supports a 1-4 character decimal value nnnn that indicates how many CPUs z/OS is able to dynamically add over the life of the IPL. The default has changed to 16.

Table 195 provides more details about this migration action. Use this information to plan your changes to the system.

Table 195. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the LOADxx DYNCPADD value is omitted (defaulted) and the default number of CPUs (16) z/OS will be able to dynamically add over the life of the IPL is not sufficient. Recommended, if you specify DYNCPADD ENABLE, which provides maximum flexibility but also results in maximum storage usage and overhead.
Target system hardware requirements:	All system z hardware (z10 EC/BC and later hardware) that supports dynamic CPU addition.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	When specifying the maximum number of CPs that z/OS can dynamically add with LOADxx DYNCPADD <i>nnnn</i> , this LOADxx cannot be shared with pre-V2R1 systems; that is, the <i>nnnn</i> parameter of DYNCPADD is not recognized by pre-V2R1 systems.
Restrictions:	None.
System impacts:	Specifying DYNCPADD <i>nnnn</i> or taking the DYNCPADD 16 default allows z/OS to determine the number of CPUs that z/OS must be prepared to be dynamically added for the life of the IPL. Because z/OS can know the maximum CPU id that can be dynamically added for the life of the IPL at IPL, z/OS can obtain CPU array related storage based on the maximum number of CPUs that can be activated for the life of the IPL.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. If the default limit of 16 CPUs that can be dynamically added is not sufficient, then indicate on your LOADxx DYNCPADD the number you desire. The maximum number of CPUs that can be added over the life of the IPL will be capped by the minimum between the highest CPU id hardware and the z/OS release supports.
2. Review the changed messages associated with two digit CP IDs. Update any necessary automation or operator procedures to accommodate the two digits. Before z/OS V2R1, there was only one digit used for CP IDs. The messages that will now contain 2 byte CP ids are the following:
 - BLW007W MULTIPLE ACR ATTEMPTS BY CPU id
 - IEA020W AN FRR STACK POINTER FOR CPU xxxx IS DAMAGED, THE ERROR MASK IS abcdefghijklmnopqrst
 - IEA796E ACR HAS TAKEN CPU x [LOGICALLY] OFFLINE BECAUSE *text*
text inserts that are updated include:
 - CPU x CHECKSTOPPED.
 - CPU x REACHED ITS *vv* MACHINE-CHECK THRESHOLD.
 - CPU x'S TOD CLOCK COULD NOT BE SYNCHRONIZED.
 - CPU x'S CLOCK COULD NOT BE SYNCHRONIZED TO THE ETR
 - IEE178I AUTOMATIC RECOVERY IS IN PROGRESS. NO OPERATOR ACTION IS REQUIRED.
 - [PROCESSOR (*y*) DETECTED AN EXCESSIVE DISABLED SPIN LOOP WAITING FOR event FROM PROCESSOR (*x*)]
 - [An event OCCURRED WHEN PROCESSOR (*y*) TRIED TO SIGNAL PROCESSOR (*x*)]
 - IEE331A PROCESSOR (*y*) IS IN AN EXCESSIVE DISABLED SPIN LOOP WAITING FOR *event*. REPLY U OR SPIN TO CONTINUE SPIN, REPLY ABEND TO TERMINATE WORK ON PROCESSOR (*x*) WITH RETRY REPLY TERM TO TERMINATE WORK ON PROCESSOR (*x*) WITHOUT RETRY OR STOP PROCESSOR (*x*) AND REPLY ACR
 - ISN011I CPU nnnn HAS BEEN ADDED

Reference information

For more information, see the following references:

- *z/OS MVS Initialization and Tuning Reference*
- The appropriate *z/OS MVS System Messages* volume for a description of the messages:
 - *z/OS MVS System Messages, Vol 3 (ASB-BPX)*
 - *z/OS MVS System Messages, Vol 6 (GOS-IEA)*
 - *z/OS MVS System Messages, Vol 7 (IEB-IEE)*

Plan for the increase of the maximum number of supported CPUs to 256

Description

In z/OS V2R2, z/OS CPU infrastructure supports up to a maximum of 256 CPUs (CPU IDs 0-255). Earlier releases of z/OS support up to 100 CPUs (CPU IDs 0-99). Components or products allocating storage for CPU related arrays or bitmasks might require changes to support the V2R2 CPU infrastructure.

Allocating CPU related arrays or bitmasks on a per CPU basis is done using one of the following:

- Runtime fields in the z/OS CVT (mapped by CVT) and ECVT (mapped by IHAECVT) control blocks representing the maximum CPU ID a z/OS image can use for the life of the IPL. Products using runtime fields do not require changes to support the V2R2 CPU infrastructure.

Migration actions from z/OS V1R13: BCP

- Compile-time or assemble time constants in the z/OS ECVT control block or within the product itself representing the maximum CPU ID the z/OS CPU infrastructure supports. Products using compile-time or assemble time constants need to recompile at a minimum, and might require code changes to support the V2R2 CPU infrastructure.

All products running on z/OS V2R2 must prepare to support all CPUs supported by the z/OS V2R2 CPU infrastructure (up to 256 CPUs with CPU IDs 0-255). Products that support the z/OS V2R2 CPU infrastructure will be able to run on earlier z/OS releases whose CPU infrastructure supports a smaller number of CPUs.

Table 196 provides more details about this migration action. Use this information to plan your changes to the system.

Table 196. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2
Is the migration action required?	Yes, for programs using local constants or the z/OS constants for the number of CPUs the z/OS CPU infrastructure supports at the current or a specific level of z/OS
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Programs that do not support up to the maximum number of CPUs the z/OS infrastructure supports might not be able to work with all CPUs on the z/OS image. The system impacts are program dependent.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Scan your code for all of the constants in the ECVT control block that have a prefix of ECVT_max_* or ECVT_zOSR11_*. These fields are all related to the maximum CPU ID the current or a specific z/OS release supports.
- Scan your code for compile-time or assemble-time constants in your product for constants related to the maximum CPU ID that the current or a specific z/OS release supports. Also scan your product for constants related to the maximum number of CPUs the current or a specific z/OS release supports.

If you use ECVT constants with a prefix of ECVT_max_* or ECVT_zOSR11_* , the product will require the following changes:

- If the ECVT_zOSR11_highestCPUID or ECVT_max_highestCPUID constants are in use:, consider upgrading your code to use the run-time field CVTMAXMP (for allocating CPU related arrays) or ECVT_Installed_CPU_HWM (for traversing CPU related arrays).
- If ECVT compile-time or assemble-time constants with a prefix of ECVT_max_* are in use, recompile/reassemble all appropriate parts with the z/OS V2R2 IHAECVT macro.

- If ECVT compile-time or assemble-time constants with a prefix of ECVT_zOSR11_* are in use, consider converting constants with a prefix of ECVT_zOSR11_* to the ECVT_max_* analog. Otherwise change ECVT_zOSR11_* to the new ECVT_zOSV2R2 analog.

If your code has its own local declares for compile-time or assembler-time constants, update your code to use the z/OS run-time fields or the z/OS compile-time or assemble-time constants. Do the following:

1. Allocate CPU bit masks at compile-time or assemble-time using ECVT_max_CPUMaskSizeInBits or ECVT_max_CPUMaskSizeInBytes.
2. Convert to using run-time fields like CVTMAXMP to allocate your local CPU related arrays. If using run-time fields is undesirable, allocate CPU arrays using the compile-time or assemble time constants ECVT_max_* or ECVT_zOSV2R2_* fields

Reference information

For more information, see *z/OS MVS Data Areas* in the z/OS Internet library (www.ibm.com/systems/z/os/zos/library/bkserv).

Plan for the new default TRACKDIRLOAD in PROGxx Description

Before z/OS V2R1, the system-wide tracking of directed load modules was not enabled. As of z/OS V2R1, you can control the enablement or disablement of this function in PROGxx, with the default being TRACKDIRLOAD (to enable system-wide tracking).

Table 197 provides more details about this migration action. Use this information to plan your changes to the system.

Table 197. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of V2R2.
Is the migration action required?	No. If you used the old default value of NOTRACKDIRLOAD and you want to retain it, you must explicitly specify NOTRACKDIRLOAD in PROGxx.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None expected. Using TRACKDIRLOAD might cause extra but generally beneficial overall processing.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you want to use the old default value, specify NOTRACKDIRLOAD in PROGxx. As a result, you will see CSV567I TRACKDIRLOAD IS NOT IN EFFECT.

Reference information

For more information, see *z/OS MVS Initialization and Tuning Reference*.

Migration actions from z/OS V1R13: BCP

Update automation that handles messages IEE302I, IEE303I, IEE1302I, IEE1303I, and IOS566I

Description

Starting in z/OS V2R1, the following messages have changed message text:

- Messages IEE302I, IEE303I, IEE1302I, and IEE1303I are changed from including ESCM in the message text to including CONFIG MANAGER in the message text.
- Message IOS566I is changed from including SYSTEM AUTOMATION in the message text to including CONFIG MANAGER in the message text.

Table 198 provides more details about this migration action. Use this information to plan your changes to the system.

Table 198. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use automation programs or other procedures to handle messages IEE302I, IEE303I, IEE1302I, IEE1303I, and IOS566I.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Modify automated actions for IEE302I, IEE303I, IEE1302I, IEE1303I, and IOS566I so they now work with the updated message text.

Reference information

For information about messages IEE302I, IEE303I, IEE1302I, and IEE1303I, see *z/OS MVS System Messages, Vol 7 (IEB-IEE)*. For information about message IOS566I, see *z/OS MVS System Messages, Vol 9 (IGF-IWM)*.

Plan for new entries AXRINIT and AXRRXTSS in the program properties table

Description

In z/OS V1R13 and earlier there were no entries in the program properties table for AXRINIT and AXRRXTSS to indicate that these programs needed to run privileged, so you had to manually add PPT entries for AXRINIT and AXRRXTSS into SCHEDxx parmlib members. In z/OS V2R1, these entries are now included in the IBM supplied default program properties table, and you can remove the SCHEDxx PPT specifications for AXRINIT and AXRRXTSS.

Table 199 on page 273 provides more details about this migration action. Use this information to plan your changes to the system.

Table 199. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V2R1
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	No, but recommended to avoid an unintended override of the IBM shipped default PPT.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Remove the PPT specifications of AXRINIT and AXRRXTSS in SCHEDxx parmlib member.

Note: The recommended action described in DOC APAR OA40519 is no longer needed as of z/OS V2R1.

Reference information

For more information, see *z/OS MVS Initialization and Tuning Reference*.

Plan for security changes to EXECIO restricting the REXX exec for allocating an internal reader

Description

In z/OS V1R13 and earlier for a REXX exec that was running under System REXX (TSO=YES), the exec was able to allocate an internal reader and subsequently invoke EXECIO to submit JCL. As of z/OS V2R1, this function is restricted if the security product (RACF or equivalent) indicates that the invoker does not have authority to the entity JCL.

Table 200 provides more details about this migration action. Use this information to plan your changes to the system.

Table 200. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V2R1
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the invoker of the System REXX exec wants to invoke EXECIO to submit JCL.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Migration actions from z/OS V1R13: BCP

Table 200. Information about this migration action (continued)

Related IBM Health Checker for z/OS check:	None.
--	-------

Steps to take

Permit access to allow the System REXX exec that uses EXECIO to submit JCL for allocating an internal reader. The System REXX exec runs under the security environment as specified by the SECURITY keyword on the AXREXX invocation; the default is the invoker of the AXREXX macro. The invoker of the System REXX exec must have access to the JCL resource in the TSOAUTH resource class.

Reference information

For more information, see *z/OS Security Server RACF Security Administrator's Guide*.

Accommodate increase in nucleus size

Description

With the introduction of the z/OS V1R13 RSM Enablement Offering web deliverable, the nucleus will increase in size by approximately 380K above the 16MB line. Because of this increase, the available private storage might affect the way your applications run on your system.

Table 201 provides more details about this migration action. Use this information to plan your changes to the system.

Table 201. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V1R13 RSM Enablement Offering Web deliverable.
Applies to migration from:	z/OS V1R13 without the z/OS V1R13 RSM Enablement Offering web deliverable.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the increase in nucleus size will affect the private storage available to applications on your system above the 16MB line.
Target system hardware requirements:	None. The migration action is relevant on all servers.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Failure to have sufficient private storage available might result in errors that affect the running of your applications.
Related IBM Health Checker for z/OS check:	VSM_CSA_CHANGE. You can use this health check to identify changes in the size of CSA or private (including the extended areas) since the last IPL.

Steps to take

Review your current available private storage usage above the 16MB line using reports from RMF or an equivalent product. Ensure that an increase of 380K for the nucleus above the 16 MB line will not adversely affect your system. Adjust values accordingly.

Reference information

For more information, see the following references:

- “Verify that virtual storage limits are set properly” on page 23
- *z/OS MVS Initialization and Tuning Guide*
- *z/OS MVS Initialization and Tuning Reference*.

Accommodate increase in ESQA Description

With the introduction of the z/OS V1R13 RSM Enablement Offering Web deliverable, there is an increased allocation of 24K (6 pages) in ESQA per CPU per LPAR. This increased allocation in ESQA per CPU includes general purpose CPs, zIIPs, and zAAPs regardless of the status (online, offline, configured, stand-by, and so forth) of the hardware. Because of this increase in ESQA, if you change the ESQA size, the available private storage may affect application execution on your system.

Table 202 provides more details about this migration action. Use this information to plan your changes to the system.

Table 202. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V1R13 RSM Enablement Offering Web deliverable.
Applies to migration from:	z/OS V1R13 without the z/OS V1R13 RSM Enablement Offering Web deliverable.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the increase in ESQA usage might cause you to run out of ESQA storage.
Target system hardware requirements:	The migration action is relevant on all servers.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Failure to have sufficient private storage available might result in errors that affect the running of your applications. The following messages might be issued: IRA103I SQA/ESQA HAS EXPANDED INTO CSA/ECSA BY xxxx PAGES IRA104I SQA/ESQA EXPANSION INTO CSA/ECSA HAS BEEN RELIEVED
Related IBM Health Checker for z/OS check:	VSM_CSA_CHANGE. You can use this health check to identify changes in the size of CSA or private (including the extended areas) since the last IPL.

Steps to take

Review your ESQA specification in IEASYSxx, to ensure that an ESQA increased allocation of 24K per CPU used on the LPAR will not adversely affect your system. If you need to increase your ESQA specification, you should also review the effects on your current available private storage usage above the 16 MB line using reports from RMF or an equivalent product. Adjust values accordingly.

Note: On a z13 server, z/OS can use symmetric multi-threading (SMT) if parmlib member LOADxx specifies PROCVIEW CORE. Here, the system defines 2 threads for every core (including CPs and zIIPs).

Migration actions from z/OS V1R13: BCP

For example, with 1 general purpose CP core and 1 zIIP core, z/OS allocates 2 CP threads and 2 zIIP threads, which results in 24K times 4 CPUs, for a total increased allocation of 96K.

Reference information

For more information, see the following references:

- “Verify that virtual storage limits are set properly” on page 23
- *z/OS MVS Initialization and Tuning Guide*
- *z/OS MVS Initialization and Tuning Reference*.

Format the ARM couple data set for long symbol table support Description

z/OS V2R2 systems require an ARM couple data set (CDS) that is formatted for long symbol table support. Otherwise, V2R2 systems can join the sysplex, but are not ARM-capable. You can establish this format level by using the z/OS V2R2 level of the IXCL1DSU format utility (either from a z/OS V2R2 system or with a STEPLIB to a z/OS V2R2 MIGLIB) to format the CDS.

Table 56 on page 105 provides more details about the migration action. Use this information to plan your changes to the system.

Table 203. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if systems are intended to use ARM functions.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None required. Systems at lower-level releases can use an ARM CDS formatted for long symbol-table support. However, a DISPLAY XCF,COUPLE,TYPE=ARM command from a down-level system cannot indicate that the HBB77A0 level of symbol table is in use unless you apply the PTFs for OA46977. With the PTFs for OA46977 applied, the response message IXC358I contains the text HBB77A0 SYMBOL TABLE SUPPORT.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Use the IXCL1DSU (format couple data set utility) at the z/OS V2R2 level to obtain at least two ARM CDSs at the HBB77A0 format level, with:
 - ARM CDS *primarydsname* on volume *primaryvolume*
 - ARM CDS *alternatedsname* on volume *alternatevolume*
2. After you create the HBB77A0 format-level ARM CDSs, you can dynamically bring them into your existing sysplex with these SETXCF commands:
 - SETXCF COUPLE,TYPE=ARM,ACOUPL=(*primarydsname,primaryvolume*)

- SETXCF COUPLE,TYPE=ARM,PSWITCH
 - SETXCF COUPLE,TYPE=ARM,ACOUPL=(*alternatedsname,alternatevolume*)
3. Remember to also specify, in your COUPLExx member of SYS1.PARMLIB, these two ARM CDSs as the primary and alternate for any future sysplex IPLs :

```
DATA
  TYPE(ARM)
  PCOUPLE(primarydsname,primaryvolume)
  ACOUPLE(alternatedsname,alternatevolume)
```

Reference information

For more information, see the following references:

- For information about the SETXCF command, see *z/OS MVS System Commands*.
- For information about the COUPLExx SYS1.PARMLIB member, see *z/OS MVS Initialization and Tuning Reference*.

Ensure that PARMDD or REGIONX are not used as job statement symbols

Description

z/OS V2R1 adds PARMDD and z/OS V2R2 adds REGIONX as new keywords on the JCL EXEC statement and PROC statement. Because JCL keyword names are reserved, you must ensure that your jobs do not use symbols with these same names. That is, if a job contains the symbolic parameter name PARMDD or REGIONX on the EXEC or PROC statement, you must edit the job to use an alternatively named symbol. Otherwise, the job can fail with a JCL error.

Table 57 on page 106 provides more details about the migration action. Use this information to plan your changes to the system.

Table 204. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V2R2 (REGIONX) and z/OS V2R1 (PARMDD).
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you used symbol names REGIONX or PARMDD on EXEC or PROC statements in jobs.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Jobs that use PARMDD or REGIONX as an EXEC or PROC statement symbol name will fail with a JCL error.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Search for a symbol named PARMDD or REGIONX in all libraries that contain JCL, such as procedure libraries. Specifically, search for the following occurrences:

- PROC statements that contain a symbolic parameter named PARMDD or REGIONX.

Examples:

```
//PROC1 PROC PARMDD=ABC
//PROC1 PROC REGIONX=ABC
```

Migration actions from z/OS V1R13: BCP

- EXEC statements that contain a symbolic parameter named PARMDD or REGIONX.

Examples:

```
//JSTEP1 EXEC PROC1,PARMDD=ABC  
//JSTEP1 EXEC PROC1,REGIONX=ABC
```

- EXEC statements that contain a '®IONX' PARM or '&PARMDD' parameter value string.

Examples:

```
//STEP1 EXEC PGM=MYPROG,PARM='&PARMDD'  
//STEP1 EXEC PGM=MYPROG,PARM='&REGIONX'
```

For any occurrences that you find, change the PROC or EXEC statement to refer to another symbolic parameter name.

Reference information

For information about JCL statements, see *z/OS MVS JCL Reference*.

Examine your IEFUSI exit routine for possible changes

Description

z/OS V2R2 includes a number of functional enhancements to support improved region management, including:

REGIONX keyword

New JCL keyword for the JOB and EXEC statements. JCL programmers can use REGIONX to explicitly request precise below-the-line and above-the-line storage amounts.

SMFLIMxx parmlib member

New parmlib member. Your installation can use SMFLIMxx to set rules for the REGION and MEMLIMIT values in job steps, or cancel job steps that violate the rules.

These changes include new parameter input fields for the IEFUSI exit routine. If your installation uses an IEFUSI exit routine to control job region size, it is recommended that you examine the routine for possible changes that you might need to make.

Note the following changes in the exit input parameter list:

- If the REGIONX keyword is used, the "region requested" value in sub-word 2 (as pointed to by word 5) is updated to contain a value based on the two values that were supplied on the REGIONX keyword. This change allows an existing exit routine to continue to receive the total amount of storage that was requested by the job step. Specifically, the value now contains either of the following values:
 - A value of 0 when the REGIONX second parameter is 0M, 0K, or 0G
 - The larger of the specified values when the REGIONX second parameter is not 0M, 0K, or 0GIf the REGIONX keyword is not used, the IEFUSI input parameter list contains one "region requested" value in sub-word 2. This behavior is the same as in previous releases of z/OS.
- For job steps that include the REGIONX keyword, sub-word 1, bit 3 (as pointed to by word 5), indicates that separate values are also available. Here, two more words are provided, sub-word 7 and 8 (as pointed to by word 5), which provide the below-the-line and above-the-line values on the REGIONX keyword.

If the total size indicated in sub-word 2 is not specific enough for your purposes, you can have your exit routine use the values in sub-word 7 and 8 to set the existing below- and above-the-line output fields in sub-words 2, 3, 4, and 5, as pointed to by word 5 of the input parameter list.

No additions or changes to the output parameter list are needed for REGIONX-related processing. The output parameter list allows for specifying separate above- and below-the-line values, as in previous releases of z/OS.

After the IEFUSI exit routine runs, the system checks the SMFLIMxx member for rules that might override region limits. This processing allows the existing IEFUSI exit to continue to set region and MEMLIMIT values for its various functions, including functions that are not supported by SMFLIMxx, such as setting limits on data space blocks. The SMFLIMxx member can be used to set values for new work or to override IEFUSI values for changes to existing work, thus reducing the need for more IEFUSI exit code changes.

In some cases, however, your installation might require that the IEFUSI exit routine make the final determination. If so, the exit routine can set a new flag (sub-word 1, bit 4, as pointed to by word 5) to bypass the SMFLIMxx rules. This bit essentially disables the SMFLIMxx processing for the current job step.

Note: A sample IEFUSI exit routine is provided in SYS1.SAMPLIB in member IEEUSI. For more information about changes that might be needed, see the commented sections in the sample IEFUSI exit routine.

Table 58 on page 108 provides more details about the migration action. Use this information to plan your changes to the system.

Table 205. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	No, but recommended to ensure that users who specify a REGIONX value in their JCL receive the correct storage allocation, according to your installation's requirements.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- If your installation uses an IEFUSI exit routine, examine it to determine whether changes are required for the REGIONX keyword and SMFLIMxx member processing.

It is possible that no action is needed, if the decisions made by the exit routine are generic, such as setting the region above-the-line value 128 MB for all job steps. If the exit sets storage values using sub-word 2 (as pointed to by word 5) and a job uses REGIONX, the exit continues to set the desired value. Here, the REGIONX value is ignored and the IEFUSI selected storage value is used.

SMFLIMxx processing, if activated by specifying SMFLIM= as part of IPL parameters or through the SET SMFLIM= operator command, overrides the IEFUSI exit-returned values, if environmental conditions match the job step's current environment.

- If you determine that your IEFUSI exit routine requires updating, you can modify your routine by using the new values in the input parameter list. For example, you can have your exit routine do the following:

Migration actions from z/OS V1R13: BCP

- Use the new REGIONX values for below- and above-the-line storage for region size determinations. These values are provided in sub-word 7 and 8 (as pointed to by word 5), when sub-word 1, bit 3 is set to 1.
- Bypass SMFLIMxx processing for certain jobs by setting sub-word 1, bit 4 (as pointed to by word 5).
Or, you can remove all region and MEMLIMIT processing from your routine, and create SMFLIMxx statements to limit the REGION and MEMLIMIT values. Here, you might retain your routine to perform other types of processing, such as setting limits on data space blocks.

Reference information

For more information, see *z/OS MVS Installation Exits*.

Accommodate system symbol names that contain underscores

Description

z/OS V2R2 enhances the use of system symbols in the following ways:

- Longer system symbol names (up to 16 characters) and longer symbol substitution values
- Underscores (_) can be specified in any character position other than the first one.

System symbols are typically used in started procedures and jobs, parmlib members, and other objects. Information about using system symbols is provided in *z/OS MVS Initialization and Tuning Reference*.

For objects that undergo system symbol substitution, be aware that the use of underscores in symbol names can result in an incompatibility if a symbol reference is followed immediately by an underscore (that is, without a symbol-delimiting period). For example, in previous releases, specifying &SYM_A in a file would match the symbol &SYM and add "_A". In z/OS V2R2, this specification can match the symbol &SYM or the symbol &SYM_A. Here, a match is attempted first for &SYM_A (with the underscore). If no match is found, an attempt is made to match &SYM.

Note: As of z/OS z/OS 2.1, underscores can be specified in JES symbol names. Thus, this migration action does not apply to JES symbol names.

Table 55 on page 104 provides more details about the migration action. Use this information to plan your changes to the system.

Table 206. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have situations in which a symbol name might be followed immediately by an underscore.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	In a sysplex of mixed releases of z/OS systems, if you use symbol names with underscores, you must ensure that earlier systems can handle the symbol names. Install the toleration PTF for APAR OA46739 on the earlier systems. The PTFs for this APAR are identified with the SMP/E FIXCAT IBM.Coexistence.z/OS.V2R2.
Restrictions:	None.
System impacts:	None.

Table 206. Information about this migration action (continued)

Related IBM Health Checker for z/OS check:	None.
--	-------

Steps to take

In z/OS V2R2, IBM provides a REXX exec, ASASYMUN, to help you locate data that might encounter unexpected results if symbol names have underscores. You can run the exec on z/OS V2R2 and older systems.

ASASYMUN scans a PDS or PDSE for situations where a symbol name that contains an underscore might cause different results than expected. For example, it checks for a symbol (an ampersand followed by other characters) followed immediately by an underscore with no delimiting period. Change these lines to add a period before the underscore to delimit the symbol.

ASASYMUN is supplied by IBM in the SBLSCLI0 data set. To use ASASYMUN, you must invoke it from an ISPF environment.

Follow these steps:

1. From the ISPF command line, run the exec as follows:

```
TSO EXEC execdsn(ASASYMUN) 'scandsn'
```

Where:

execdsn

is the cataloged data set containing the ASASYMUN exec. Use 'execdsn(ASASYMUN)' if the data set name is fully qualified. You can use alternative forms of execdsn(ASASYMUN) if the data set is in the SYSEXEC or SYSPROC concatenation of the user. For example, you might be able to specify just (ASASYMUN).

scandsn

is the PDS or PDSE you want to scan. Specify a data set contain statements subject to symbol substitution, like JCL or parmlib statements. If the data set name is fully qualified, double the quotations around the name in addition to the single quotation marks that surround the parameter. For example, specify '''fully.qual.dsn''' for a fully qualified data set.

2. For any references you find that were intended to be resolved by a symbol, add a period before the underscore to delimit the symbol. For example:

```
&SYM._A
```

Reference information

For information about specifying system symbols, see *z/OS MVS Initialization and Tuning Reference*.

Adjust parameters to start IOSHMCTL in TPC-R Basic Hyperswap environment

Description

With APAR OA40866 applied (with one of the following PTFs: UA71220 for z/OS V2R1, or UA71219 for z/OS V1R13), parameters supplied in the JCL to start PGM=IOSHMCTL may be rejected. APAR OA40866 introduced new function which caused JCL parameter checking to now be enforced. As a result, unsupported parameters will be rejected and IOSHMCTL will not start due to JCL failures.

For example:

```
ASA101I SYNTAX ERROR: MODE=EXT, WAS SEEN, WHERE ONE OF
(SOCKPORT=)
WOULD BE CORRECT.
DETECTING MODULE IS IOSHMCTL
```

Migration actions from z/OS V1R13: BCP

Prior to APAR OA40866, unsupported parameters would be ignored and IOSHMCTL would start without any JCL failures.

Note: This problem is a documentation error where some examples of JCL to start the Basic HyperSwap address space used incorrect parameters. At this time with Basic HyperSwap Sockets Server APAR OA40866 applied, the only parameter allowed to the IOSHMCTL program is 'SOCKPORT=*port_num*'. Any other parameters are rejected.

Table 54 on page 103 provides more details about the migration action. Use this information to plan your changes to the system.

Table 207. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R1 and z/OS V1R13, both with APAR OA40866 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA40866 applied.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have unsupported parameters specified to start the Basic HyperSwap address space.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- When applying the PTF for APAR OA40866, make sure that any HSIB procedures to start IOSHMCTL do not include unsupported parameters. For example, the following JCL may be used:

```
//HSIB JOB MSGLEVEL=(1,1),TIME=NOLIMIT,REGION=0M  
//IEFPROC EXEC PGM=IOSHMCTL
```

Tip: Some older publications, including Redpapers, might have documented incorrect parameters on the PARM statement used in the examples of suggested procedures for starting IOSHMCTL. It is best to refer to the latest TPC-R publications for current supported parameters.

Reference information

For more information, see APAR OA46189, which describes the potential JCL failures after installing PTFs for APAR OA40866.

Assess the use of the INCLUDE1MAFC keyword on the LFAREA parameter in IEASYSxx

Description

Prior to z/OS V2R2, the default was for RSM not to include 1 M fixed frames in the available frame count (RCEAFC). APAR OA41968 added the INCLUDE1MAFC keyword on the LFAREA parameter in the IEASYSxx member of parmlib to cause RSM to include 1 M fixed frames in the available frame count. This results in the following system behavior:

- RSM performs less paging when there is an abundance of available 1 M fixed frames in the system.
- RSM is more likely to break up 1 M fixed frames to satisfy 4 K page demand. Although RSM attempts to coalesce broken up 1 M fixed frames when there is fixed 1 M page demand, there is no guarantee that coalescing will be successful, especially if any of the 4 K frames making up the fixed 1 M page is fixed long term.

Starting with z/OS V2R2, RSM includes 1 M fixed frames in the available frame count by default; you no longer need to specify INCLUDE1MAFC to do this. Furthermore, the syntax of the INCLUDE1MAFC keyword has been extended to include a YES or NO option. The former INCLUDE1MAFC keyword syntax is still valid and can now also be specified as INCLUDE1MAFC(YES).

IBM recommends that you accept the default (or specify INCLUDE1MAFC or INCLUDE1MAFC(YES)). However, if you have a need to retain the old default behavior (that is, to exclude 1 M fixed frames from the available frame count), you must specify INCLUDE1MAFC(NO).

Table 59 on page 109 provides more details about the migration action. Use this information to plan your changes to the system.

Table 208. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you did not specify the INCLUDE1MAFC keyword on the LFAREA parameter in IEASYSxx prior to z/OS V2R2 and you want to continue excluding 1 M fixed frames from the available frame count.
Target system hardware requirements:	None.
Target system software requirements:	RMF APAR OA42066 for z/OS V2R1 RMF APAR OA42510 for z/OS V1R13
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Check the LFAREA parameter specification in the IEASYSxx member on your pre-z/OS V2R2 system.
 - If you specified the INCLUDE1MAFC keyword on the LFAREA parameter after APAR OA41968, and you want to continue with that setting on your z/OS V2R2 system, you can do any of these things:
 - Leave the INCLUDE1MAFC keyword as it is.
 - Remove the INCLUDE1MAFC keyword, as it is now the default.
 - Change INCLUDE1MAFC to INCLUDE1MAFC(YES).
 - If you did not specify the INCLUDE1MAFC keyword on the LFAREA parameter and you want to retain the old default behavior, you must now specify INCLUDE1MAFC(NO).
- Check any application programs that use the STGTEST SYSEVENT to determine if any changes need to be made. The STGTEST event returns information about the amount of storage available in the system,

Migration actions from z/OS V1R13: BCP

which includes the LFAREA when INCLUDE1MAFC(YES) is specified or defaulted. Application programs can check the RCEINCLUDE1MAFC bit to determine the setting of INCLUDE1MAFC in the LFAREA specification.

Reference information

For information about the LFAREA parameter and the INCLUDE1MAFC keyword in IEASYSxx, see *z/OS MVS Initialization and Tuning Guide*.

Plan for the use of freemained frames

Description

To enhance system performance on the IBM z13, there might be cases where the system does not free the real frame that is backing a virtual page following a FREEMAIN, that is, when the page no longer contains any GETMAIN-assigned storage ranges. If so, the system will clear or “dirty” the frame to ensure that sensitive information is removed. Such a frame is referred to as a *freemained frame*. Freemained frames do not cause the count of frames owned by the address space (RAXFMCT) to be decremented (as they would have previously), nor do they cause the count of available frames within the system (RCEAFC) to be incremented (as they would have previously). Instead, the system uses a new counter, RAX_FREEMAINEDFRAMES, to keep track of the number of frames backing freemained pages in the address space with which the RAX is associated.

This feature is active by default on the IBM z13 and only applies to region private “low” storage (below 2GB), which is defined as subpools 0-127, 129-132, 240, 244, 250-252. Storage subpools define the characteristics of virtual storage below 2 GB and are discussed in detail in *z/OS MVS Diagnosis: Reference*.

The SYSEVENT STGTEST API reports on the current usage of real storage, returning a three-word value:

Word 1

Use of this number affects system performance very little, if at all.

Word 2

Use of this number affects performance to some degree.

Word 3

Use of this number may substantially affect performance.

To maintain compatibility with prior releases, SYSEVENT STGTEST will include most of Rce_FreemainedFrames in word 1 and all of it in words 2 and 3 for z/OS V2R1 (HBB7790) and z/OS V1R13 (JBB778H). For z/OS V2R2 (HBB77A0), SYSEVENT STGTEST is changed to exclude Rce_FreemainedFrames from word 1.

Programs that reference or issue TPROT instructions against region private storage that is not GETMAIN assigned might not experience an 0C4 system abend nor get a non-zero condition code where they previously would have. This applies to the subpools listed earlier.

The following new parameters in the DIAGxx member of parmlib allow you to disable this feature, if necessary:

FREEMAINEDFRAMES(NO)

Disables the freemained frames feature on a system-wide basis.

FREEMAINEDFRAMES(YES) [EXCLUDEJOBLIST(job1[,job2,...])]

Enables the freemained frames feature, except for the specified jobs. Up to eight job names may be specified. The job names may include the * and ? wildcard characters, where the * character is allowed in any position.

Reissuing the SET DIAG command with different EXCLUDEJOBLIST values will *not* increase the total number of excluded jobs; the last EXCLUDEJOBLIST specification overrides any previous specifications.

Disabling this feature for selected jobs will cause performance degradation for the entire system, not just for the specified jobs.

You can use the DISPLAY DIAG command to verify that the system is using the requested FREEMAINEDFRAMES statement.

Note: The DISPLAY DIAG command does not report the default value. The FREEMAINEDFRAMES statement only appears in the IGV007I message when it has been specified in the DIAGxx member. Therefore, you can use the DISPLAY DIAG command to verify that the system is using the specified FREEMAINEDFRAMES statement.

Table 60 on page 111 provides more details about the migration action. Use this information to plan your changes to the system.

Table 209. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2. z/OS V2R1 and z/OS V1R13 (with the RSM web deliverable), both with APAR OA46291 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13 (with the RSM web deliverable).
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	<p>Yes, unless you disable this feature. Otherwise, installations that use software tools that monitor real storage usage must install updates to accommodate the advent of freemained frames.</p> <p>Applications that invoke the TPROT instruction to determine whether pages of region private storage have been GETMAIN assigned should change to use the VSMLOC or VSMLIST services. The IARQDUMP service may also be applicable in some cases.</p> <p>If none of these services meet the performance requirements of the application, then the application should use the new IARBRVER and IARBRVEA services provided with APAR OA46291 and z/OS V2R2.</p>
Target system hardware requirements:	IBM z13.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	<ul style="list-style-type: none"> • Address spaces may appear to be using more storage than before the feature is enabled or by default. • The system may appear to have less available storage than before the feature is enabled or by default. • References to non-GETMAIN assigned storage may not result in a 0C4 system abend. • The TPROT instruction may not return a condition code of 3 in cases where it previously would have done so.
Related IBM Health Checker for z/OS check:	None.

Migration actions from z/OS V1R13: BCP

Steps to take

Follow these steps:

- Verify that the value of RceOA46291Applied is B'1' before using any other new fields in the RCE or RAX data areas, as the new fields are not guaranteed to be initialized otherwise.
- Programs that reference RAXFMCT can subtract Rax_FreemainedFrames to determine how much real storage the address space is currently using.
- Programs that reference RCEAFC can add RCE_FreemainedFrames to determine how much storage is not currently in use. If an application is referencing RCEAFC to determine how much storage is available to be used by the application, a better solution is to use SYSEVENT STGTEST.
- If an application needs to determine whether a virtual address range is GETMAIN assigned, it should use the VSMLOC or VSMLIST services, instead of using the LLAG or TPROT assembly language instructions. These services are documented in *z/OS MVS Programming: Authorized Assembler Services Reference SET-WTO* and can be invoked regardless of whether the caller is running in a cross-memory environment (although they would only be applicable to the primary address space).

The IARQDUMP callable service can be used to determine whether there is some virtual storage backing a given page and is documented in *z/OS MVS Programming: Authorized Assembler Services Guide*.

If neither of these approaches are feasible, perhaps due to concerns about performance, the following new callable services provide the same results as the TPROT instruction while also taking freemained frames into account:

- IARBRVER takes in general purpose register (GPR) 1 the virtual address of the page and returns one of the following codes in GPR 15:

Code	Meaning
------	---------

- | | |
|---|--|
| 0 | Caller has write access to the data. |
| 1 | Caller has Read-only access (no write access) to the data. |
| 2 | Caller has neither read nor write access to the data. |
| 3 | The page either cannot be translated or is backed by a freemained frame. |

- IARBRVEA is similar to IARBRVER except that it is invoked in AR mode and access register (AR) 1 contains the ALET associated with the virtual address to be tested. This entry should be used when the page to be tested does not reside in the primary address space.

These services are available when the value of RceOA46291Applied is B'1' and can be invoked on all supported hardware, not just the z13.

Reference information

The documentation updates for APAR OA46291 are described in the file, OA46291.PDF, which is available at: <http://publibz.boulder.ibm.com/zoslib/pdf/OA46291.pdf> .

The following table provides a list of references for various aspects of the freemained frames feature.

Table 210. Reference information for freemained frames

For information about...	See...
User region private storage and the freemained frames feature	<i>z/OS MVS Initialization and Tuning Guide</i>
The FREEMAINEDFRAMES parameter in DIAGxx	<i>z/OS MVS Initialization and Tuning Reference</i>
The IARQDUMP service	<i>z/OS MVS Programming: Authorized Assembler Services Guide</i>
The IARBRVEA and IARBRVER services	<i>z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG</i>
The VSMLOC and VSMLIST services	<i>z/OS MVS Programming: Authorized Assembler Services Reference SET-WTO</i>

Table 210. Reference information for freemained frames (continued)

For information about...	See...
The PVT, RAX, and RCE data areas	<i>z/OS MVS Data Areas</i> in the z/OS Internet library (www.ibm.com/systems/z/os/zos/library/bkserv)

Relocate Cross System Extended Services (XES) component trace buffers

Description

In z/OS V2R2, the Cross System Extended Services (XES) buffers for component tracing are moved from a common area data space (CADS) to a 4 GB memory object in 64-bit common high virtual (HVCOMMON) storage. During system initialization, XES obtains a 4 GB memory object and manages the virtual storage for global and connection CTRACE buffers. This change allows the GLOBAL trace buffer to be increased from 16 MB to 32 MB (fixed), which reduces the possibility of buffer wrapping. It also increases the available address range for connector trace buffers, which decreases the possibility of a connector running without component tracing.

In previous releases, the XES CTRACE buffers resided in a CADS object named IXLCTCAD, which limited the buffers to a 2 GB range of addresses. In z/OS V2R2, XES no longer creates the IXLCTCAD object.

Notes:

1. The 4 GB memory object is a fixed size area that is obtained by XES; the size cannot be modified.
2. The IXLBCCAD object is not affected by this migration action.

Table 62 on page 114 provides more details about the migration action. Use this information to plan your changes to the system.

Table 211. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use coupling facilities in your sysplex or have references to the XES CTRACE CADS ('IXLCTCAD') on the DSPNAME parameter of the DUMP and SLIP commands or in automated parse routines.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Eliminating the XES CADS decreases the number of common area data spaces that are created in the system.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Ensure that enough 64-bit common storage (HVCOMMON) storage is allocated by the system, so that the additional 4 GB request by XES does not cause shortages for other components and elements. The amount of 64-bit common storage is controlled by the HVCOMMON parameter in the IEASYSxx

Migration actions from z/OS V1R13: BCP

parmlib member. Review the value that is specified on the HVCOMMON parameter to determine whether it must be increased. You can use the MVS operator command **D VIRTSTOR,HVCOMMON** to display information about the current use of the HVCOMMON storage on your system.

For example:

```
IAR019I 06.55.51 DISPLAY VIRTSTOR
SOURCE = DEFAULT
TOTAL 64-BIT COMMON = 66G
64-BIT COMMON RANGE = 1982G-2048G
64-BIT COMMON ALLOCATED = 4171M
```

- To accommodate the allocation of a 4 GB XES CTRACE buffer, add 4 gigabytes (4G) to the HVCOMMON value in the IEASYSxx parmlib member.
- Check for references to the IXLCTCAD object, which is no longer created in z/OS V2R2. Specifically, check for references to 'IXLCTCAD' on the DSPNAME parameter of the **DUMP** and **SLIP** commands (that is, DSPNAME=('XCFAS'.IXLCTCAD)) and on any automated parse routines.
- Ensure that SDATA=XESDATA is specified on any **DUMP** or **SLIP** commands where the IXLCTCAD name was removed. This setting causes the XES CTRACE 64-bit common storage to be included in an SVC dump.

Failure to remove the IXLCTCAD references can result in an error message, such as ASA104. This error, however, does not stop the running process.

If XES cannot obtain a 4 GB memory object, message IXL017I is issued. The system continues to process XES requests normally, but SYSXES CTRACE data is not be available in dumps for analysis under IPCS.

Reference information

For more information, see the following references:

- For information about the HVCOMMON system parameter, see *z/OS MVS Initialization and Tuning Reference*.
- For information about CTRACE, see *z/OS MVS Diagnosis: Tools and Service Aids*.

MVS SLIP command change for MODE=HOME

Description

When a **SLIP** command is issued for a PER trap with **MODE=HOME** specified, but without **JOBNAME** and **ASID** specified, the system issues message IEE088D to prompt the operator for a reply (continue or cancel).

The **JOBNAME**, **ASID**, and **MODE** parameters for a **SLIP** command work together to control the cross memory environment for a PER interrupt. Specifying **MODE=HOME** indicates that the SLIP trap matches only when the command is running in the home address space. When **MODE=HOME** is specified, more processing is used to monitor for the correct environment. When **MODE=HOME** is specified with the **JOBNAME** or **ASID** parameter, this monitoring is limited to the specified address spaces.

However, if **MODE=HOME** is specified without **JOBNAME** and **ASID**, the monitoring occurs for every address space on the system, which can impact performance significantly. As a warning, the system issues message IEE088D with either of the following text strings:

```
IEE088D SLIP COMMAND SPECIFIES MODE=HOME WITHOUT JOBNAME AND ASID. SPECIFY 'OK' OR 'CANCEL'
IEE088D SLIP ID=xxxx SPECIFIES MODE=HOME WITHOUT JOBNAME AND ASID. SPECIFY 'OK' OR 'CANCEL'
```

Note: When this capability was introduced in z/OS V2R1 with APAR OA45297 and even after APAR OA45912, you enabled it by specifying the option TRAPS NAME(IeaSlipConfirm) in the DIAGxx parmlib member. However, in z/OS V2R2, this capability is enabled automatically; you no longer need to specify it explicitly. If you do so in z/OS V2R2, the explicit specification is ignored without an error.

Table 63 on page 115 provides more details about the migration action. Use this information to plan your changes to the system.

Table 212. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use any IEASLPxx parmlib member or program that issues a SLIP command for a PER trap with MODE=HOME specified, but without JOBNAME and ASID specified.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

For any IEASLPxx parmlib member or program that issues a **SLIP** command for a PER trap with **MODE=HOME** specified, but without **JOBNAME** and **ASID** specified, verify your use of **MODE=HOME** to determine whether changes are needed.

Follow these steps:

- If a **SLIP** command includes **MODE=HOME**, ensure that it also includes **JOBNAME** or **ASID**, or both. Or, if you require the SLIP trap to be set this way, include the **OK** parameter to avoid message IEE088D.
- If you already include the **OK** parameter on the **SLIP** command for another purpose, verify that the **MODE=HOME** parameter is required. Previously, you might have specified the **OK** parameter to avoid receiving the following message:

```
IEE831D SLIP TRAP ID=0001 PER RANGE (00000000_00000000,00000000_01000000)
EXCEEDS 1M OR WRAPS. SPECIFY 'OK' OR 'CANCEL'
```

For example, if you have a SLIP trap that is defined as follows, verify that **MODE=HOME** is required:

```
SLIP SET,IF,RA=(0,1000000),MODE=HOME,OK,END
```

Reference information

For more information, see the following references:

- For the SLIP command, see *z/OS MVS System Commands*.
- For the IEE088D message, see *z/OS MVS System Messages, Vol 7 (IEB-IEE)*.

Define a SAF profile for the log stream subsystem exits

Description

As of APAR OA51174, a log stream subsystem exit routine name is used only when it is one of the IBM-defined names, or the exit name is allowed through a SAF profile. Otherwise, z/OS does not invoke the exit routine name. Instead, z/OS issues message IXG507I and returns a failure indication to the log stream subsystem function (either converter or allocation).

Migration actions from z/OS V1R13: BCP

Currently, log stream users can specify a log stream subsystem exit routine name to receive control for reading log data. Users can use either of the following methods to specify the exit routine names:

- On the JCL DDNAME statement, on the keyword SUBSYS=(LOGR,*exit_routine_name*,...)
- On a dynamic allocation request that includes a text unit value for key DALSSPRM (*exit routine name*)

With APAR OA51174, this behavior is changed. To continue to specify an exit routine name as described here, your installation must protect the resource IXLGLOGR.SUBSYS.LSEXIT.*exit_routine_name*, where *exit_routine_name* identifies the name of the log stream subsystem exit routine.

If your installation uses RACF as its security management product, your security administrator can protect the resource by defining a profile in the FACILITY class. If your installation uses a security management product other than RACF, your security administrator can refer to this topic for reference when creating an equivalent protection in the security management product on your system.

The exception to this requirement is if your installation uses the following IBM-defined names for the exit routines. If so, you have no migration action to perform.

- IXGSEXIT
- IFASEXIT
- IFBSEXIT
- DFHLGCNV

This table provides more details about the migration action. Use this information to plan your changes to the system.

Element or feature:	BCP
When change was introduced:	z/OS V2R2, z/OS V2R1, and z/OS V1R13, all with PTFs for APAR OA51174 applied.
Applies to migration from:	z/OS V2R2, z/OS V2R1, and z/OS V1R13, all without PTFs for APAR OA51174 applied.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if both of the following conditions are true: <ul style="list-style-type: none">• Your installation has a log stream subsystem exit routine that is specified through the SUBSYS=(LOGR,...) keyword on a DDNAME JCL statement or on a dynamic allocation request that includes a text unit value for key DALSSPRM• Exit routine name is not one of the following IBM-defined names: IXGSEXIT, IFASEXIT, IFBSEXIT, or DFHLGCNV.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Jobs or dynamic allocation requests that specify a log stream exit routine name might fail with an authorization error.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If your installation does not use any log stream subsystem exit routines, or if your installation uses only the IBM-defined names for the log stream subsystem exit routine names, you have no migration action to perform.

Otherwise, if your installation uses or plans to use log stream subsystem exit routine names other than the IBM-defined names, you must perform the following steps:

- Define a discrete profile IXGLOGR.SUBSYS.LSEXIT.*exit_routine_name* for the FACILITY class, where *exit_routine_name* is the name of the log stream subsystem exit routine. Your security administrator can use this profile to audit access failures and grant users READ access. For example:

```
RDEFINE FACILITY IXGLOGR.SUBSYS.LSEXIT.exit_routine_name UACC(READ) AUDIT(FAILURES(READ))
```

- If you need to allow for exit routine names that might not be explicitly known on your system, consider also defining the generic profile IXGLOGR.SUBSYS.LSEXIT.* in the FACILITY class. Include the WARNING attribute in the profile definition (to issue a warning message, but allow access). This profile protects resources that are associated with the log stream subsystem exit routines. For example:

```
RDEFINE FACILITY IXGLOGR.SUBSYS.LSEXIT.* UACC(NONE) WARNING
```

When this generic profile is used to cover the authorization check for the resource IXGLOGR.SUBSYS.LSEXIT.*exit_routine_name*, if the check fails, RACF issues the appropriate warning message to the user, logs the access attempt, and allows the user to access the resource.

Using a generic profile is recommended only as a temporary means for gathering information on the possible exit routine names on your system that require protection. When the exit routine names are identified, you can define the appropriate discrete profiles. After you protect the known exit routine names with discrete profiles, delete the generic profile.

Note: If you do not define profiles as described here, but instead, define a generic profile that protects the resource IXGLOGR.SUBSYS.LSEXIT.*exit_routine_name*, the generic profile attributes are used to determine the following behaviors:

- Outcome of the authorization checking
- Logging
- Whether the exit routine is invoked.

Reference information

For information about defining RACF profiles in the FACILITY class, see *z/OS Security Server RACF Security Administrator's Guide*.

Update Capacity Provisioning to use Java 7.1 or higher Description

Starting with z/OS V2R2, the Provisioning Manager component of Capacity Provisioning supports Java V7.1. If the references in the ENV member of the Provisioning Manager parameters data set specify the location of an earlier version of Java, you must update the LIBPATH environment variable.

Table 64 on page 118 provides more details about the migration action. Use this information to plan your changes to the system.

Table 213. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use Capacity Provisioning.
Target system hardware requirements:	IBM 31-bit SDK for z/OS, Java Technology Edition, V7.1 (5655-W43).
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.

Migration actions from z/OS V1R13: BCP

Table 213. Information about this migration action (continued)

Restrictions:	Levels prior to z/OS V2R2 Capacity Provisioning Manager are not compatible with IBM 31-bit SDK for z/OS V7.1, Java Technology Edition. The support for Java V7.1 is found in z/OS V2R2 Capacity Provisioning Manager. Thus, you cannot use Java V7.1 with pre-z/OS V2R2 Capacity Provisioning Manager levels.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Install IBM 31-bit SDK for z/OS, Java Technology Edition, V7.1 (5655-W43).
- Change the LIBPATH variable in the ENV member of your Provisioning Manager PARM data set to refer to the installation directories of your Java V7 installation. For example:
`LIBPATH=/usr/lpp/cpo/lib:/usr/lib:/usr/lpp/java/a71/J7.1/bin:/usr/`

Reference information

For information about how to adapt the Provisioning Manager parameters, see *z/OS MVS Capacity Provisioning User's Guide*.

Modify the UPDATE statement for the PFA date change Description

Before z/OS V2R2, Predictive Failure Analysis (PFA) checks had a **DATE** value that reflected the current parameters and values.

Beginning with z/OS V2R2, the **DATE** value in each PFA check changed because new parameters are added to all checks. The existing **UPDATE** statements in HZSPRMxx parmlib members fail unless the **DATE** parameter is set to use ('20140313') or later.

New parameters are added to all PFA checks. If you want to use the new PFA enhancements, or you want to use a value other than the default, you must create an HZSPRMxx parmlib member or modify the existing one.

Table 65 on page 119 provides more details about this migration action. Use this information to plan your changes to the system.

Table 214. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have updated PFA checks in HZSPRMxx.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.

Table 214. Information about this migration action (continued)

Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Determine whether you are using an HZSPRMxx parmlib member that contains the **UPDATE** statements for one or more PFA checks.
2. If you have an **UPDATE** statement for any PFA check, the **DATE** parameter must be changed to **DATE('20140313')** or later, or the **UPDATE** fails.
3. Determine whether you want to change the value of any of the new parameters. If you want to change the values, add the parameters and new values to the **UPDATE** command.
4. If you do not want to change any of the other parameter values, PFA uses the value that was last set. When a value is never set, PFA uses the default.
5. If you specify WTOTYPE for the PFA_COMMON_STORAGE_USAGE check and want to use the new enhancement for dynamic severity for that check, remove WTOTYPE from the **UPDATE** statement.

For example, the following **UPDATE** statement changes for the PFA_JES_SPOOL_USAGE check changes:

- **DATE** to ('20140313').
- **EXCDIRDAYS** to **30** days.
- **FORCEMODEL** time to **5:00** A.M.
- **COLLUPTIME** to **3** hours.

```
UPDATE CHECK(IBM PFA,PFA_JES_SPOOL_USAGE)
ACTIVE
SEVERITY(MEDIUM)
INTERVAL(ONETIME)
PARMS=('COLLECTINT(5)', 'MODELINT(720)', 'STDDEV(3)', 'DEBUG(0)', 'COLLECTINACTIVE(1)'
, 'EXCEPTIONMIN(10)', 'EXCDIRDAYS(30)', 'FORCEMODEL(5:00)', 'COLLUPTIME(180)')
DATE(20140313)
REASON('To detect a damaged address space by comparing the amount of
change in the size of the JES spool to the expected value.')
```

Reference information

For more information about PFA, see *z/OS V2R2 Problem Management*.

Review PFA check values

Description

Before z/OS V2R2, Predictive Failure Analysis (PFA) defined the following default values for the checks listed:

- TRACKEDMIN(3) for PFA_SMF_ARRIVAL_RATE and PFA_MESSAGE_ARRIVAL_RATE.
- STDDEVLOW(4) in PFA_ENQUEUE_REQUEST_RATE.

In z/OS V2R2, changes were made to the algorithm that PFA uses, and to the default PFA check values, to work more accurately with the algorithm changes. The changes are intended to accomplish the following goals:

- Increase the accuracy of the PFA checks
- Reduce false positives while still issuing valid exceptions.
- Choose which address spaces to track more accurately.

Migration actions from z/OS V1R13: BCP

Table 66 on page 120 provides more details about this migration action. Use this information to plan your changes to the system.

Table 215. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you are using PFA and not satisfied with the results.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Determine whether you are using a HZSPRMxx parmlib member that contains one or more of the following checks, or if you manually change the parameters for these PFA checks by using the **MODIFY** command supplied by IBM Health Checker for z/OS:
 - PFA_ENQUEUE_REQUEST_RATE
 - PFA_SMF_ARRIVAL_RATE
 - PFA_MESSAGE_ARRIVAL_RATE.
2. If you are changing values for any or all of the checks, determine whether the following parameters are being set for the checks in your HZSPRMxx parmlib member, and if the value set is anything other than the following value:
 - PFA_ENQUEUE_REQUEST_RATE: STDDEVLOW(8)
 - PFA_MESSAGE_ARRIVAL_RATE: TRACKEDMIN(2)
 - PFA_SMF_ARRIVAL_RATE: TRACKEDMIN(2)
3. If yes, remove the change to those values from the HZSPRMxx parmlib member. Do not change them using the **MODIFY** command.
4. Restart PFA to begin by using the new default values.
5. After PFA runs for more than a week, if the current default values are not sufficient for your installation, consider changing them based on the results from that period.

Reference information

For more information about the checks, see *z/OS V2R2 Problem Management*.

Ensure that PFA finds the configuration file

Description

Before z/OS V2R2, Predictive Failure Analysis (PFA) required that you run the install script, AIRSHREP.sh, to create the new directory structure, copy the ini file, and create the default EXCLUDED_JOBS file. Beginning with z/OS V2R2, there is no need to run the install script. Everything previously done by the install script is now done when PFA starts. Also, the only ini file that PFA uses is the /etc/PFA/ini file. The install of PFA requires that any values in the /etc/PFA/ini file are correct.

Table 67 on page 121 provides more details about this migration action. Use this information to plan your changes to the system.

Table 216. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the <code>/etc/PFA/ini</code> file does not exist or if the values for JAVAPATH , PATH , and LIBPATH are not correct.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Before you begin, ensure that the PFA user has READ access to the `/etc/PFA/ini` file. Also, the operator must have proper authority to read or update the files, as needed.

When PFA is started, PFA attempts to use the values in the `/etc/PFA/ini` file.

Follow these steps:

1. If the `/etc/PFA/ini` file already exists, PFA uses the existing **JAVAPATH**, **PATH**, and **LIBPATH** that are in the file. Update the values as necessary.
2. If the `/etc/PFA/ini` file does not exist, PFA attempts to create the `/etc/PFA/ini` file from an existing check, or it uses the values defined in the `/usr/lpp/bcp/samples/PFA/ini` file. To ensure that the **JAVAPATH**, **PATH**, and **LIBPATH** values are correct for your installation before PFA starts, copy `/usr/lpp/bcp/samples/PFA/ini` into `/etc/PFA/ini` and update the values as necessary.

For example, check the values for the **JAVAPATH**, **PATH**, and **LIBPATH** to be certain they are at the correct level for PFA. In z/OS V2R2, PFA uses a minimum level of Java 7.1 (31-bit) as in the following examples for the **PATH** and **LIBPATH**:

```
PATH= /usr/lpp/java/J7.1/lib/s390/classic:/usr/lpp/java/J7.1/lib/s390
```

```
LIBPATH=/usr/lpp/java/J7.1/lib/s390:/usr/lpp/java/J7.1/lib/s390/classic:/lib:/usr/lib:
```

If the values are not correct, PFA either fails to start or can have processing errors.

Reference information

For information about installing PFA, see *z/OS V2R2 Problem Management*.

Update PFA to use Java 7.1 or higher Description

Before z/OS V2R2, Predictive Failure Analysis (PFA) used a minimum level of IBM 31-bit SDK for z/OS Java Technology Edition version 6.0.0. Beginning with z/OS V2R2, PFA uses a minimum level of IBM 31-bit SDK for z/OS Java Technology Edition version 7.1.0 or later.

Migration actions from z/OS V1R13: BCP

Table 68 on page 122 provides more details about this migration action. Use this information to plan your changes to the system.

Table 217. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you are using PFA.
Target system hardware requirements:	None.
Target system software requirements:	IBM 31-bit SDK for z/OS Java Technology Edition version 7.1.0 or later.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Before you begin, ensure that the PFA user must have READ access to the `/etc/PFA/ini` file. When PFA is started, PFA attempts to use the values in the `/etc/PFA/ini` file.

Follow these steps:

1. If the `/etc/PFA/ini` exists, update the **PATH=** and **LIBPATH=** statements to point to IBM 31-bit SDK for z/OS Java Technology Edition version 7.1.0 or higher.
2. If the `/etc/PFA/ini` file does not exist, copy it from `/usr/lpp/bcp/samples/PFA/ini`. If the path to the JDK for your installation is not the same as the path in the ini file, update it so that both the **PATH=** and **LIBPATH=** statements point to IBM 31-bit SDK for z/OS Java Technology Edition version 7.1.0 or higher.
3. If the `/etc/PFA/ini` file does not exist and you do not copy the sample file, when PFA starts, it attempts to copy the ini file from an existing PFA check directory. If no ini files exists in any of the PFA check directories, PFA copies the sample file that specifies the default path for Java 7.1. If the path to the JDK for your installation is the same as the default, PFA starts. If the path to the JDK for your installation is not the same as the default, PFA issues a message, and then either fails to start or can have processing errors.

The following example is the default **PATH** and **LIBPATH** for PFA:

```
PATH= /usr/lpp/java/J7.1/lib/s390/classic:/usr/lpp/java/J7.1/lib/s390
LIBPATH=/usr/lpp/java/J7.1/lib/s390:/usr/lpp/java/J7.1/lib/s390/classic:/lib:/usr/lib:
```

Reference information

For more information about PFA, see *z/OS V2R2 Problem Management*.

Ensure that the IWM4HLTH service is used properly Description

As of z/OS V2R2, the minimum authorization requirements for callers of the Workload Management service, IWM4HLTH (setting the server health indicator), are changed. Problem state with any PSW key is sufficient only for setting the health indicator for the home address space of the calling application.

To set the health indicator for another address space, the caller must have at least one of the following authorizations:

- Supervisor state
- Program key mask (PKM) with at least one of the keys 0 - 7
- UPDATE authority to the resource IWM.SERVER.HEALTH in the FACILITY class.

Also, callers of the IWM4HLTH service are recommended to avoid setting the health value to less than 100 for any purposes other than for server health. In z/OS V2R2, a server health value of less than 100 can result in false positives, as follows:

- Runtime Diagnostics creates a diagnostic event for each address space with a server health value less than 100, regardless of the reason. Events that are created for reasons other than server health might be considered as false events by the user of Runtime Diagnostics.
- Predictive Failure Analysis (PFA) issues exceptions for Runtime Diagnostics events that are received for server health values less than 100. PFA exceptions that are issued for these events might be considered as false positive exceptions by the user of PFA.

Table 69 on page 123 provides more details about this migration action. Use this information to plan your changes to the system.

Table 218. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2, z/OS V2R1, and z/OS V1R13, all with APAR OA46280.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA46280.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have <ul style="list-style-type: none"> • Unauthorized applications that call this service • Callers that set health values of less than 100 for reasons other than server health
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

To identify unauthorized callers of the IWM4HLTH service who set the health indicator for an address space other than the caller's home address space, you can temporarily define the resource profile IWM.SERVER.HEALTH with the parameter WARNING. After the first IPL of z/OS V2R2, RACF issues the following warning message for callers of the service with insufficient authorization:

```
ICH408I USER(user) IWM.SERVER.HEALTH CL(FACILITY)
WARNING: INSUFFICIENT AUTHORITY - TEMPORARY ACCESS ALLOWED
```

Take one of the following steps for unauthorized callers:

- Change the program so that it no longer calls the IWM4HLTH service or no longer runs the program.
- Change the caller authorization to supervisor state or PKM, with at least one of the keys 0-7.
- Give the user ID associated with the program UPDATE authority to the resource profile IWM.SERVER.HEALTH or an appropriate generic profile when generic profile checking is active.

Migration actions from z/OS V1R13: BCP

After the necessary steps are taken, modify the resource profile and specify NOWARNING. Or, if there are no unauthorized callers of the IWM4HLTH service, delete the profile.

Also, ensure that callers of the IWM4HLTH service do not set health values of less than 100 for reasons other than server health.

Reference information

For more information, For more information, see *z/OS MVS Programming: Workload Management Services*.

Identify unauthorized callers of the IWMSRDRS and IWMSRSRG services

Description

With z/OS V2R2, the minimum authorization requirements for the callers of Workload Management services IWMSRDRS (Deregister a server for sysplex routing) and IWMSRSRG (Register a server for sysplex routing) are changed.

- Problem state with any PSW key if the server address space to be registered or deregistered is the home address space. If resource BPX.WLMSEVER is defined in the FACILITY class, an unauthorized caller requires access authority to this resource or the IWM.SERVER.REGISTER resource in the FACILITY class.
- If the server to be registered or deregistered is not the home address, one of the following:
 - Supervisor state
 - Program key mask (PKM) allowing at least one of the keys 0-7
 - The caller has at least READ authority to the resource IWM.SERVER.REGISTER in the FACILITY class. If this resource is not defined, READ authority to the FACILITY class resource BPX.WLMSEVER is required.

Table 70 on page 125 provides more details about this migration action. Use this information to plan your changes to the system.

Table 219. Information about this migration action

Element or feature:	BCP
When change was introduced:	z/OS V2R2, z/OS V2R1, and z/OS V1R13, all with APAR OA46405.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA46405.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have unauthorized applications that invoke one of these services and resource BPX.WLMSEVER in the FACILITY class is not defined.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If RACF resource BPX.WLMSEVER is defined in the FACILITY class, unauthorized callers of WLM services IWMSRDRS and IWMSRSRG already have access authority and no further steps are necessary.

If the resource is not defined, it is recommended that you identify unauthorized callers that use the IWMSRDRS and IWMSRSRG services to register or deregister an address space other than the caller's home address space. To do so, you can temporarily define the IWM.SERVER.REGISTER resource profile with the WARNING parameter. After the first IPL of z/OS V2R2, RACF issues the following warning message for callers of the macro with insufficient authorization:

```
ICH408I USER(user) IWM.SERVER.REGISTER CL(FACILITY)
WARNING: INSUFFICIENT AUTHORITY - TEMPORARY ACCESS ALLOWED
```

For unauthorized callers, take one of the following steps:

- Change the program so that it no longer calls the IWMSRDRS or IWMSRSRG macro or no longer runs the program.
- Change the caller's authorization to supervisor state or PKM allowing at least one of the keys 0-7.
- Give the user ID associated with the program access authority to the resource profile IWM.SERVER.REGISTER or an appropriate generic profile when generic profile checking is active.

After all necessary steps have been taken, modify the resource profile and specify NOWARNING. Or, delete the resource profile if there are no unauthorized callers of the IWMSRDRS or IWMSRSRG macro.

Reference information

For more information, see *z/OS MVS Programming: Workload Management Services*.

Ensure that authorizations are correct for callers of WLM services

Description

With z/OS V2R2, the minimum authorization requirements for the callers of following Workload Management services are changed:

- IWMDEXTR – Extract WLM service definition
- IWMDINST – Install a service definition
- IWMPACT – Activate service policy.

Resource MVSADMIN.WLM.POLICY in the FACILITY class is mandatory. Callers of IWMDEXTR must have READ access and callers of IWMDINST and IWMPACT must have UPDATE authority. Appropriate access authorities are also required when using the WLM ISPF Application to install or extract a service definition or activate a service policy.

In previous releases, MVSADMIN.WLM.POLICY was optional. If you did not define this resource (or a generic one), any user could invoke IWMDEXTR, IWMDINST, and IWMPACT.

Table 71 on page 126 provides more details about this migration action. Use this information to plan your changes to the system.

Table 220. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the resource MVSADMIN.WLM.POLICY in the FACILITY class is not already defined.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.

Migration actions from z/OS V1R13: BCP

Table 220. Information about this migration action (continued)

Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Define resource MVSADMIN.WLM.POLICY in the FACILITY class. Then, provide read access or update authority to users according to their needs.

Reference information

For more information, see the following references:

- *z/OS MVS Programming: Workload Management Services*
- *z/OS MVS Planning: Workload Management*

BCP actions to perform after the first IPL of z/OS V2R2

This topic describes BCP migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

Accommodate the SETLOAD xx,IEASYM command to update system symbols Description

Before z/OS V2R1, the downloadable SYMUPDTE routine and the IEASYMUP module in SYS1.SAMPLIB were provided as mechanisms to update system symbols without initiating an IPL. Starting with z/OS V2R1, the SETLOAD xx,IEASYM command is available to perform this task. In z/OS V2R1, the IEASYMUP module in SAMPLIB is updated to return with a RC=X'FFF', not having done the requested function. However, unless this IEASYMUP module is rebound, there is no way to prevent the usage of an old copy, or detect an update because of use of an old copy of the tool.

In z/OS V2R2 you should stop using the downloadable SYMUPDTE routine or the IEASYMUP module from samplib in your earlier release. Note that use of SYMUPDTE or IEASYMUP might produce incorrect results when used in conjunction with the SETLOAD xx,IEASYM command. The SYS1.LINKLIB program IEASYMU2 is instead provided via APAR OA42569 as a replacement for the function provided by IEASYMUP / SYMUPDTE on previous z/OS releases. IEASYMU2 is a supported program in z/OS, and has considerations when used with SETLOAD xx, IEASYM.

Table 221 provides more details about this migration action. Use this information to plan your changes to the system.

Table 221. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you are currently using the IEASYMUP module provided in SYS1.SAMPLIB or the SYMUPDTE routine to update system symbols.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.

Table 221. Information about this migration action (continued)

Restrictions:	If you continue to use the SYMUPDTE routine or the IEASYMUP module, or if you use the IEASYMU2 program, system symbols will be updated and the system will continue to function properly until the SETLOAD xx,IEASYM command is used. Once SETLOAD xx,IEASYM has been issued, updates introduced by those other programs will be lost. You may continue to use the IEASYMU2 program again, even after a SETLOAD xx,IEASYM has been issued, but the same considerations will be in effect.
System impacts:	<p>Note:</p> <ul style="list-style-type: none"> • Updates to the system symbol table through the SETLOAD xx,IEASYM command will occur only on the system issuing the command. • When a SETLOAD command is issued and fails, messages issued by IEFPRMLB (logical parmlib service) that contain <i>jobname</i> and <i>stepname</i> will contain the master <i>jobname</i> and <i>stepname</i> of the last step that ran under master because the SETLOAD command runs under master but does not run as its own step. In this case, the error is related to the SETLOAD processing and NOT the step whose name appears in the message.
Related IBM Health Checker for z/OS check:	SUP_SYSTEM_SYMBOL_TABLE_SIZE. This code checks if the size of the static system symbol table has exceeded the threshold. This check is initially run once and is also run when the SETLOAD xx,IEASYM command is successfully processed.

Steps to take

Follow these steps:

- Rebind the IEASYMUP module from the z/OS V2R2 SAMPLIB to disable the code or simply remove it from LINKLIB or your LNKLST library.
- If you have used the downloadable SYMUPDTE routine, remove it from your LINKLIB or your LNKLST library. Begin using SETLOAD xx,IEASYM command instead of these obsolete modules. Or change your JCL to use IEASYMU2 instead of IEASYMUP (and remove any joblib/steplib specification). IEASYMU2 verifies access through the same profile of IEASYMUP.* in the FACILITY class that IEASYMUP did, so there are no security definition changes from using IEASYMUP to IEASYMU2.

Reference information

For more information, see the following references:

- SETLOAD command description in *z/OS MVS Planning: Operations*
- System symbols description in *z/OS MVS Initialization and Tuning Reference*

Plan for the new default format level of HBB7705 in the IXCL1DSU utility Description

Starting in z/OS V2R2, system logger uses a new default NUMBER() value for the SMDUPLEX item when using the XCF couple data set format utility (IXCL1DSU) to format a LOGR CDS.

The SMDUPLEX item NUMBER(1) is now the default value when running the IXCL1DSU utility on a z/OS V2R2 or higher release level and results in a LOGR CDS format level of HBB7705.

Migration actions from z/OS V1R13: BCP

The LOGR CDS format level is managed as follows:

HBB7705

Indicates that the LOGR CDS was formatted at one of the following sets of release level ranges and options:

- z/OS V2R2 or later when the ITEM NAME(SMDUPLEX) specification is not provided
- z/OS V1R2 or later with option NUMBER(1) specified for item name SMDUPLEX

HBB6603

Indicates that the LOGR CDS was formatted at one of the following sets of release level ranges and options:

- OS/390 V1R3 or later, through OS/390 V2R10 and z/OS V1R1
- z/OS V1R2 or later, through z/OS V2R1, without option NUMBER(1) for item name SMDUPLEX
- z/OS V1R2 or later with option NUMBER(0) specified for item name SMDUPLEX

HBB5520

Indicates that the LOGR CDS was formatted at a release level before OS/390 V1R3.

Table 72 on page 127 provides more details about this migration action. Use this information to plan your changes to the system.

Table 222. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you intend on using the IXCL1DSU format couple data set utility on any z/OS V2R2 level systems.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Plan to make use of the default HBB7705 LOGR CDS format level or take steps to format a different LOGR CDS level.

Reference information

For more information, see the following references:

- For information about using the IXCL1DSU format couple data set utility for system logger, see the "LOGR parameters for format utility" section of *z/OS MVS Setting Up a Sysplex*.
- For considerations on the system logger functions that are supported using the different LOGR CDS format levels, see the "LOGR couple data set versioning - new format levels" section of *z/OS MVS Setting Up a Sysplex*.

Use the z/OSMF Capacity Provisioning task to define policies

Description

z/OS V1R13 was the last release to provide the Windows-based Capacity Provisioning Control Center (CPCC) function for use with z/OS MVS Capacity Provisioning. Starting with z/OS V2R1, IBM provides the z/OSMF based Capacity Provisioning task as an alternative means to define Capacity Provisioning policies and to allow you to control your Capacity Provisioning function.

Table 223 provides more details about this migration action. Use this information to plan your changes to the system.

Table 223. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R1 with partial support rolled back in the z/OSMF APAR PM74519.
Applies to migration from:	z/OS V1R13 without the z/OSMF APAR PM74519.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you are using Capacity Provisioning.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Use the Capacity Provisioning task in z/OSMF V2R2 as the replacement for the former Capacity Provisioning Control Center. When you have set up z/OSMF, you can import your previous Domain Configurations and Capacity Provisioning Policies into the z/OSMF Capacity Provisioning task using the Import from File or Import from Domain actions.

Reference information

For more information about using the z/OSMF Capacity Provisioning task, see the following publication and the z/OSMF online help: *z/OS MVS Capacity Provisioning User's Guide*.

Consider the new COUPLExx CFRMTAKEOVERCF(NO) default

Description

z/OS V2R2 introduces a new COUPLExx parmlib member keyword: CFRMTAKEOVERCF. Specifying CFRMTAKEOVERCF(NO) enables CF gain ownership processing enhancements that might prevent a sysplex outage by avoiding operator errors. CFRMTAKEOVERCF(NO) is also the default for z/OS V2R2. To have your z/OS V2R2 system to prompt the operator as it did in prior releases, specify CFRMTAKEOVERCF(PROMPT).

When CFRMOWNEDCFPROMPT(YES) is specified by the COUPLExx parmlib member of a down-level system (prior to z/OS V2R2), the z/OS V2R2 default of CFRMTAKEOVERCF(NO) is not compatible with the configuration.

When CFRMOWNEDCFPROMPT(YES) is used by a down-level system, that system clears the CF authorities saved in the CFRM CDS during CFRM and sysplex initialization (that is, a sysplex-wide IPL).

Migration actions from z/OS V1R13: BCP

When that occurs, an up-level system (z/OS V2R2) rejects the use of any CF that has a non-zero authority. However, CFRMTAKEOVERCF(NO) is not intended to reject the use of the CF when the old CF authority in the CFRM CDS matches the CF authority in the CF. If a down-level system is no longer in the sysplex, no system will perform the desired prompting.

When CFRMOWNEDCFPROMPT(NO) is specified (or defaulted) by the COUPLExx parmlib member of a down-level system, the z/OS V2R2 default of CFRMTAKEOVERCF(NO) is compatible with the configuration.

Table 73 on page 128 provides more details about the migration action. Use this information to plan your changes to the system.

Table 224. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you are currently using CFRMOWNEDCFPROMPT(YES) or if, for some reason, the new behavior of CFRMTAKEOVERCF(NO) is not desirable.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you specify CFRMOWNEDCFPROMPT(YES) in the COUPLExx parmlib member, follow these steps:

- Create a COUPLExx parmlib member for z/OS V2R2 systems with CFRMOWNEDCFPROMPT(YES) CFRMTAKEOVERCF(PROMPT) to obtain the old default behavior. After all of the systems are on z/OS V2R2, the COUPLExx parmlib member can be changed to CFRMOWNEDCFPROMPT(YES) CFRMTAKEOVERCF(NO) if the enhanced CF gain ownership processing of CFRMTAKEOVERCF(NO) is desired.
- To have your z/OS V2R2 system prompt the operator as it did in prior releases:
 - Copy the existing COUPLExx parmlib member into a new COUPLExx parmlib member.
 - Add the new CFRMTAKEOVERCF(PROMPT) statement after the COUPLE statement in the new COUPLExx parmlib member.
 - Ensure that the new COUPLExx parmlib member is used when you IPL z/OS V2R2.

If you specify or default to CFRMOWNEDCFPROMPT(NO), you have no migration action to perform.

Reference information

For more information, see the following reference:

- For the COUPLExx (cross-system coupling facility (XCF)) parmlib parameters, see *z/OS MVS Initialization and Tuning Reference*.

Evaluate the stand-alone dump default for large memory objects

Description

Before APAR OA47439, large memory objects were included in stand-alone dumps, which contributed to longer stand-alone dump times. With the PTF for APAR OA47439 applied, this default behavior is changed to improve stand-alone dump processing time.

As part of this support, a new keyword, `SADMP=DEFAULT|YES|NO`, is added to the IARV64 macro. This keyword is used to specify whether a memory object is to be included in a stand-alone dump by default.

The SADMP keyword is added to the IARV64 macro for the following options:

- IARV64 REQUEST=GETSTOR
- IARV64 REQUEST=GETCOMMON
- IARV64 REQUEST=GETSHARED

`SADMP=NO` is the default when `PAGEFRAMESIZE=2G` is specified on the IARV64 REQUEST=GETSTOR macro invocation. Previously, the default behavior was equivalent to specifying `SADMP=YES`. The new default behavior can help to reduce stand-alone dump capture times by avoiding the inclusion of large memory objects and their associated real storage in the dump. To have this type of memory object included in a stand-alone dump, you must allow it explicitly by specifying `SADMP=YES`.

Table 74 on page 129 provides more details about the migration action. Use this information to plan your changes to the system.

Table 225. Information about this migration action

Element or feature:	BCP.
When change was introduced:	z/OS V2R2, and z/OS V2R1 with APAR OA47439 applied.
Applies to migration from:	z/OS V2R1 (without APAR OA47439 applied) and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you want to continue capturing memory objects that are backed by 2G frames in stand-alone dumps.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	By default, not including memory objects in stand-alone dumps is expected to result in faster stand-alone dumps. If memory objects are included in stand-alone dumps, you can expect lengthened stand-alone dump times. The performance of stand-alone dump might be noticeably lengthened for z/OS systems that have a large amount of real memory (1 TB or greater) when memory objects are included.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Check for the IARV64 REQUEST=GETSTOR macro invocation with the PAGEFRAMESIZE=2G option specified.

Migration actions from z/OS V1R13: BCP

2. For memory objects that should not be included in a stand-alone dump, add `SADMP=NO` to the macro invocation (or accept the default).
3. Otherwise, for memory objects that contain data that should be captured in a stand-alone dump, add `SADMP=YES` to the `IARV64 REQUEST=GETSTOR` macro invocation, if `PAGEFRAMESIZE=2G` is specified.

Note: `SADMP` APAR OA44443 for z/OS V2R2 and V2R1 introduces the `SADMPNO` keyword, which can be used to capture memory objects that are created with the `SADMP=NO` attribute in specified address spaces.

Reference information

For information about creating large memory objects with the `IARV64` macro, see *z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG*.

BookManager BUILD migration actions

This topic describes migration actions for optional feature BookManager BUILD.

BookManager BUILD actions to perform before installing z/OS V2R2

This topic describes BookManager BUILD migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Accommodate the removal of BookManager BUILD Description

z/OS V2R1 is the last release that supported the optional feature BookManager BUILD of z/OS. As of z/OS V2R2, this optional feature has been removed.

Table 75 on page 131 provides more details about this migration action. Use this information to plan your changes to the system.

Table 226. Information about this migration action

Element or feature:	BookManager BUILD
When change was introduced:	z/OS V2R1
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use the optional feature BookManager BUILD.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Remove any usage of BookManager BUILD. Note that the z/OS base element BookManager READ is still available for reading existing BookManager books.

Reference information

None.

BookManager BUILD actions to perform before the first IPL of z/OS V2R2

This topic describes BookManager BUILD migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

None.

BookManager BUILD actions to perform after the first IPL of z/OS V2R2

This topic describes BookManager BUILD migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

CIM migration actions

This topic describes migration actions for the base element Common Information Model (CIM).

CIM actions to perform before installing z/OS V2R2

This topic describes CIM migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

**Prepare for the removal of the CIM Java Managed Provider Interface (JMPI)
Description**

z/OS V2R2 is planned to be the last release to support the Java Managed Provider Interface (JMPI) in Common Information Model (CIM). If your installation is using JMPI, IBM recommends that you migrate to a supported provider interface, such as the Common Manageability Programming Interface (CMPI).

Table 76 on page 132 provides more details about this migration action. Use this information to plan your changes to the system.

Table 227. Information about this migration action

Element or feature:	z/OS Common Information Model
When change was introduced:	See IBM United States Software Announcement 215-267 "IBM z/OS Version 2 Release 2—Fueling the new digital enterprise," dated July 28, 2015.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you are using the JMPI function.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Migration actions from z/OS V1R13: CIM

Table 227. Information about this migration action (continued)

Related IBM Health Checker for z/OS check:	None.
--	-------

Steps to take

Identify any provider that is using the JMPI function, and convert it to use a supported provider interface. Equivalent function is available through the Common Manageability Programming Interface (CMPI), which is a C language interface. Using the CMPI requires that the CIM provider be written in the C language.

Reference information

For information about CIM providers, see *z/OS Common Information Model User's Guide*.

CIM actions to perform before the first IPL of z/OS V2R2

This topic describes CIM migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

None.

CIM actions to perform after the first IPL of z/OS V2R2

This topic describes CIM migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

Update to SBLIM CIM Client for Java Version 2 Description

z/OS V2R1 is the last release to include Version 1 of the Standards Based Linux Instrumentation for Manageability (SBLIM) CIM client for Java. Version 1 support for the SourceForge open source project was discontinued after 2010. Version 2 of the SBLIM client, which is designed to be a JSR48- compliant implementation, is included in z/OS. Users of SBLIM Version 1 must convert to Version 2.

If you are using SBLIM Version 1, convert to Version 2, which has been included in z/OS since V1R13.

Table 77 on page 133 provides more details about this migration action. Use this information to plan your changes to the system.

Table 228. Information about this migration action

Element or feature:	z/OS Common Information Model
When change was introduced:	IBM United States Software Announcement 213-013, dated February 5, 2013. The removal occurs in z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you used SBLIM CIM Client for Java Version 1.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Table 228. Information about this migration action (continued)

Related IBM Health Checker for z/OS check:	None.
--	-------

Steps to take

Identify any non-IBM application that is using the SBLIM CIM Client for Java Version 1 (**sblimCIMClient.jar**) and contact the owner of the application to convert it to use SBLIM CIM Client for Java Version 2 (**sblim-cim-client2.jar**).

Reference information

For more information about the CIM client for Java, see *z/OS Common Information Model User's Guide* .

Communications Server migration actions

This topic describes migration actions for base element Communications Server.

Communications Server actions to perform before installing z/OS V2R2

This topic describes Communications Server migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Configuration assistant: Migrate to the Configuration Assistant for Communications Server in z/OSMF

Description

Starting with z/OS V2R1, IBM Configuration Assistant for z/OS Communications Server is no longer offered as a stand-alone application that runs on the Windows operating system. IBM Configuration Assistant for z/OS Communications Server is available as a fully supported task in the z/OSMF product. Use the task available in z/OSMF.

Table 229 provides more details about this migration action. Use this information to plan your changes to the system.

Table 229. Information about this migration action

Element or feature:	Communications Server.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if a Windows desktop version is being used.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Migration actions from z/OS V1R13: Communications Server

Steps to take

To use the IBM Configuration Assistant for z/OS Communications Server task, you need to take the following steps:

1. Configure z/OSMF.
2. Transfer your existing backing store files into the z/OSMF environment if desired.

Reference information

For more information, see the following references:

- For information about configuring z/OSMF, see *IBM z/OS Management Facility Configuration Guide*.
- For information about transferring Configuration Assistant backing store files to z/OSMF, see *IBM z/OS Management Facility Configuration Guide*.

IP Services: Permit intranode management network application to use OSM interfaces

Description

Beginning in z/OS V2R1, access to OSM interface information by using ioctls SIOCGIFNAMEINDEX, SIOCGHOMEIF6, and SIOCGIFCON6 has been restricted to applications with READ authorization to the EZB.OSM.sysname.tcpname resource.

Table 230 provides more details about this migration action. Use this information to plan your changes to the system.

Table 230. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you run an application that requires OSM interface information by using the ioctls.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

An applications that uses ioctls SIOCGIFNAMEINDEX, SIOCGHOMEIF6, or SIOCGIFCONF6 to retrieve OSM interface information requires authorization to the EZB.OSM.sysname.tcpname resource.

- If your security server is RACF, issue the following commands.

```
SETROPTS CLASSACT(SERVAUTH)
SETROPTS RACLIST (SERVAUTH)
RDEFINE SERVAUTH EZB.OSM.sysname.tcprocname
PERMIT EZB.OSM.sysname.tcpname CLASS(SERVAUTH) -
ID(userid) ACCESS(READ)
SETROPTS RACLIST(SERVAUTH) REFRESH
```
- If you use a different security server, perform the equivalent steps.

Reference information

For more information, see OSM access control in *z/OS Communications Server: IP Configuration Guide*.

IP Services: Ensure that FTP is listed in AUTHCMD and AUTHPGM NAMES

Description

Beginning with z/OS V2R1, the z/OS FTP client supports user exits. The FTP client invokes z/OS Dynamic Exit Services (DES) to determine whether you have installed FTP client user exit EZAFCCMD or EZAFCREP. To invoke DES successfully, the program FTP must be APF authorized. Therefore, if you want to use the z/OS FTP client user exits, you must add FTP to the AUTHCMD and AUTHPGM NAMES section of your IKJTSOxx member of SYS1.PARMLIB.

Note: Before applying the PTF of TCP/IP APAR PI05065, you will receive the following messages during the FTP Server initialization if you do not add the FTP program to the AUTHCMD and AUTHPGM NAMES section of your IKJTSOxx parmlib member.

```
EZA1555I CSVDYNEX DEFINE failed for user exit EZAFCCMD,
RETURN CODE x'08' REASON CODE x'00000804'
EZA1555I CSVDYNEX DEFINE failed for user exit EZAFCREP,
RETURN CODE x'08' REASON CODE x'00000804'
```

Table 231 provides more details about this migration action. Use this information to plan your changes to the system.

Table 231. Information about this migration action

Element or feature:	Communications Server.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	No, only if you want to use the z/OS FTP client user exits.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	The IKJTSOxx change cannot be shared between z/OS V2R2 systems and pre-z/OS V2R1 systems. That is, do not share the IKJTSOxx change for FTP between z/OS V2R2 and z/OS V1R13.
Restrictions:	None.
System impacts:	If you make the IKJTSOxx FTP change on your z/OS V1R13 system, you may see various ABENDs or problems. These problems may result in message IKJ56652I You attempted to run an authorized command or program. This is not supported under the dynamic TSO/E environment, or other related problems.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Add FTP in the AUTHCMD and AUTHPGM NAMES section of your IKJTSOxx member of SYS1.PARMLIB if you want to use the z/OS FTP client user exits.

Note: SYS1.SAMPLIB(IKJTSO00) member was updated with TSO/E APAR OA45541 to remove the FTP definitions in both the AUTHCMD and AUTHPGM NAMES sections, which were added in z/OS V2R1.

Migration actions from z/OS V1R13: Communications Server

Reference information

For more information, see the following references:

- FTP client user exits in *z/OS Communications Server: IP Configuration Reference*.
- TSO command authorization in *z/OS Communications Server: IP Configuration Guide*
- For a complete list of all the z/OS Communications Server commands and programs that need to be added to the AUTHCMD NAMES and AUTHPGM NAMES statements in your IKJTSOxx PARMLIB member, see the *z/OS Program Directory* at the z/OS installation related information website.

IP Services: Understand the change in the support for the DVIPSEC parameter Description

Before z/OS V2R1, the DVIPSEC parameter on the IPSEC statement in the TCP/IP profile enabled Sysplex-Wide Security Associations (SWSA) for IPv4 on a stack that had IPCONFIG IPSECURITY specified in the TCP/IP profile. Support for SWSA for IPv6 was not provided in these releases.

Beginning with z/OS V2R1, SWSA for IPv6 is supported. The DVIPSEC parameter on the IPSEC statement in the TCP/IP profile enables SWSA for IPv6 on a stack that has IPCONFIG6 IPSECURITY specified in the TCP/IP profile.

Table 232 provides more details about this migration action. Use this information to plan your changes to the system.

Table 232. Information about this migration action

Element or feature:	Communications Server.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if the TCP/IP profile for your stack specifies the IPSECURITY parameter on the IPCONFIG6 statement and also specifies the DVIPSEC parameter on the IPSEC statement.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- If you have both of the following specified in your TCP/IP profile, be aware that SWSA for IPv6 will be enabled on your stack:
 - The IPSECURITY parameter on the IPCONFIG6 statement
 - The DVIPSEC parameter on the IPSEC statement
- If you have IPv6 TCP traffic that is protected by an IPsec Security Association (SA) with an IPv6 DVIPA endpoint, you can see the following changes:

- When an IPv6 DVIPA is moved during a planned or unplanned DVIPA takeover, new SAs are automatically reestablished with the same security service characteristics as the SAs that existed on the host that owned the DVIPA.
- IPv6 TCP traffic that is protected by an IPSec SA with a sysplex-distributed DVIPA endpoint can be distributed to target hosts.
- Ensure that you configure the appropriate IP security policy on the backup and target hosts.

Reference information

For more information, see the topic on sysplex-wide security associations in *z/OS Communications Server: IP Configuration Guide*.

IP Services: Be aware of the enhancements to IP Fragment attack type of IDS Description

Beginning in z/OS V2R1, IP fragment attack type of the Intrusion Detection Services (IDS) is enhanced to monitor both IPv4 and IPv6 traffic for suspicious fragments. It is also enhanced further to check for overlays that change the data in the packet. Be aware that in z/OS V2R1, if you have the IP fragment IDS attack enabled, IPv6 traffic will now be monitored. In earlier releases, only IPv4 traffic was monitored.

Table 233 provides more details about this migration action. Use this information to plan your changes to the system.

Table 233. Information about this migration action

Element or feature:	Communications Server.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you are using IDS on a stack and the IP Fragment attack type is enabled.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you are using IDS on a stack and the IP Fragment attack type is enabled, be aware of the following information:

- Both IPv4 and IPv6 traffic are monitored for suspicious fragments.
- The IP Fragment attack type checking is enhanced to check for overlays that change the data in the packet, including changes to the length of the packet.

Reference information

For more information about IP fragments, see “Attack of IDS policy definition considerations” in *z/OS Communications Server: IP Configuration Guide*.

Migration actions from z/OS V1R13: Communications Server

IP Services: Relink NMI applications using the 64-bit TMI copy buffer function Description

Starting with z/OS V2R1, the interface between the 64-bit TMI copy buffer function (EZBTMIC4) and the TCP/IP stack is changed. Applications that use the real-time TCP/IP network monitoring network management interface (NMI) and statically link to this function must either relink or change to dynamic linking or loading of the function.

Table 234 provides more details about this migration action. Use this information to plan your changes to the system.

Table 234. Information about this migration action

Element or feature:	Communications Server.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if your application statically links to the 64-bit TMI copy buffer function (EZBTMIC4). No change is required for applications that use the 32-bit TMI copy buffer function (EZBTMIC1) or that dynamically link or load EZBTMIC4.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If your application statically links to the 64-bit TMI copy buffer function (EZBTMIC4), relink your application, or change your application to dynamically link to the 64-bit TMI copy buffer function (EZBTMIC4).

Reference information

For more information, see “EZBTMIC1 or EZBTMIC4: Copy TCP/IP Management Interface Data Buffer” in *z/OS Communications Server: IP Programmer’s Guide and Reference*

IP Services: Review XL C/C++ applications that use the GetProfile request of TCP/IP NMI Description

In z/OS V2R1, the definitions of some of the IPv6 address fields returned by the TCP/IP callable NMI GetProfile request were changed. The definitions for the following fields are corrected to specify a data type of `in6_addr` instead of a character string in the XL C/C++ header file `ezbnmmmpc.h`.

- NMTP_V6CFDynXcfAddr
- NMTP_IPA6Addr

If you have XL C/C++ applications that reference these fields, modify the applications before recompiling them with the updated XL C/C++ header file.

Table 235 provides more details about this migration action. Use this information to plan your changes to the system.

Table 235. Information about this migration action

Element or feature:	Communications Server.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you plan on recompiling your application with the updated XL C/C++ header file.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Review the references to the changed fields in your application program.
2. If you have XL C/C++ applications that reference these fields, you need to modify your application before recompiling it with the updated XL C/C++ header file.

Reference information

For more information about the GetProfile request, see “TCP/IP callable NMI (EZBNMIFR)” in *z/OS Communications Server: IP Configuration Guide*

IP Services: Prepare for the addition of IPv6 support for policy-based routing Description

As of z/OS V2R1, policy-based routing is enhanced to route IPv6 traffic. In earlier releases a policy-based routing rule that did not specify the source and destination IP addresses only applied to IPv4 packets. Starting in z/OS V2R1, that same policy-based routing rule applies to both IPv4 and IPv6 packets.

Table 236 provides more details about this migration action. Use this information to plan your changes to the system.

Table 236. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you are using policy-based routing on a stack that is being run as a dual-mode stack (IPv4 and IPv6).
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.

Migration actions from z/OS V1R13: Communications Server

Table 236. Information about this migration action (continued)

Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you have a policy-based routing rule that specifies neither source IP addresses nor destination IP addresses, the rule will apply to both IPv4 and IPv6 packets. If you want the rule to continue to apply to only IPv4 packets, modify the rule to specify either a source or destination IP address of 0.0.0.0/0.

Reference information

For more information, see the RoutingRule statement in *z/OS Communications Server: IP Configuration Reference*.

IP Services: Migrate from BIND 9.2.0

Description

z/OS V1R13 was the last release that supported the z/OS BIND 9.2.0 name server function. If you are using this function as a name server, you must find a replacement.

Table 237 provides more details about this migration action. Use this information to plan your changes to the system.

Table 237. Information about this migration action

Element or feature:	Communications Server
When change was introduced:	The removal of the BIND 9.2.0 function was first announced in February 2009. z/OS V1R13 was the last release that supported the z/OS BIND 9.2.0 name server function, as stated in the z/OS V1R13 preview announcement on February 11th, 2011.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you are using the BIND 9.2.0 function as a name server.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	ZOSMIGV1R11_CS_DSNBIND9.

Steps to take

Follow these steps:

- If you are using z/OS BIND 9.2.0 as a caching-only name server, use the z/OS resolver DNS caching function to cache DNS responses.
- If you are using z/OS BIND 9.2.0 as a primary or secondary authoritative name server, investigate using BIND on Linux for System z.

Migration actions from z/OS V1R13: Communications Server

- Update the NSINTERADDR statements in the resolver configuration file.
- If the z/OS BIND 9.2.0 name server is the only name server to be contacted in the NSINTERADDR list of name servers, replace the name server entry with one or more name server IP addresses.
- If more than one name server is in the NSINTERADDR list of name servers, delete the IP address of the z/OS BIND 9.2.0 name server.
- If the automated domain name registration(ADNR) application is being used, ensure the name server is configured to support ADNR. See *z/OS Communications Server: IP Configuration Guide* for configuring automated domain name registration.

Reference information

For more information about the resolver, see the following references:

- *z/OS Communications Server: IP Configuration Guide*
- *z/OS Communications Server: IP Configuration Reference*.

IP Services: Replace configuration of TCP/IP legacy device types

Description

Support for the DEVICE and LINK profile statements for the following TCP/IP legacy device types are removed from IBM Communications Server in z/OS V2R2:

- ATM
- CDLC
- CLAW
- HYPERchannel
- SNALINK (LU0 and LU6.2)
- X.25

Because support will be eliminated for the ATM device type, the following associated TCP/IP profile statements will no longer be supported:

- ATMARPSV
- ATMLIS
- ATMPVC
- TRANSLATE NSAP

Because support will be eliminated for the CDLC, SNALINK (both LU0 and LU6.2), and X.25 device types, the following server applications will no longer be supported:

- NCPROUTE
- SNALINK LU0
- SNALINK LU6.2
- X.25 NPSI

Because support will be eliminated for the CLAW and HCH device types, the following TCP/IP profile statement parameters will no longer be supported:

- IPCONFIG CLAWUSEDODUBLENOP and STOPONCLAWERROR
- TRANSLATE HCH

If you are using these legacy device type profile statements, migrate to a later interface type, such as OSA-Express QDIO or HiperSockets.

Note: This only affects device types that are configured to the TCP/IP stack.

As of z/OS V2R2, ZOSMIGV2R1_CS_LEGACYDEVICE migration health check is removed.

Table 78 on page 134 provides more details about this migration action. Use this information to plan your changes to the system.

Migration actions from z/OS V1R13: Communications Server

Table 238. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R2. This change was also announced in the Statement of direction: IBM zEnterprise System, z/OS, and z/VM enhancements shorten time to value, deliver enhanced security, and improve data access 114-009 February 24, 2014.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you are using any of these legacy device types, you must migrate from these device types to more recent types, such as OSA-Express QDIO and HiperSockets.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	TCP/IP configuration error messages are issued if any of the affected profile statements are configured to the TCP/IP stack.
Related IBM Health Checker for z/OS check:	<p>The ZOSMIGV2R1_CS_LEGACYDEVICE migration health check determines whether you are using any legacy device statements in your TCP/IP profile. This check is available on the following releases:</p> <ul style="list-style-type: none">• z/OS V1R13 with APARs PI12977 and OA44669 applied.• z/OS V2R1 with APARs PI12981 and OA44671 applied. <p>If any of these device type profile statements are processed, warning message EZZ0717I is issued.</p>

Steps to take

1. If your current configuration includes functions for which support has been eliminated, perform the following steps:
 1. Migrate to a later TCP/IP interface type, such as OSA-Express QDIO or HiperSockets.
 2. Review your TCP/IP IPCONFIG and TRANSLATE profile statements for unsupported parameters.
 3. Verify you are not using the unsupported server applications.
2. You should also remove any customization for the ZOSMIGV2R1_CS_LEGACYDEVICE health check in your IBM Health Checker for z/OS HZSPRMxx parmlib member.

Reference information

For information about configuring OSA-Express QDIO and HiperSockets interfaces, see Considerations for networking hardware attachment in *z/OS Communications Server: IP Configuration Guide*.

IP Services: Replace GATEWAY statements in the TCP/IP profile Description

As of z/OS V2R2, support for the GATEWAY statement in the TCP/IP profile is removed. You must migrate your static route configuration to the equivalent BEGINROUTES statements.

Also, the migration health check ZOSMIGV2R1_CS_GATEWAY is removed in z/OS V2R2.

Migration actions from z/OS V1R13: Communications Server

Table 79 on page 135 provides more details about this migration action. Use this information to plan your changes to the system.

Table 239. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you have defined static routes by using GATEWAY statements, you must migrate to the BEGINROUTES statements.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	TCP/IP configuration error messages are issued if a GATEWAY statement is configured to the TCP/IP stack.
Related IBM Health Checker for z/OS check:	ZOSMIGV2R1_CS_GATEWAY can help you determine if you are using any GATEWAY statements in your TCP/IP profile. This check is provided in z/OS V1R13 via VTAM APAR OA43345 and TCP/IP APAR PM96813. If the GATEWAY statement is processed, warning message EZZ0717I is issued.

Steps to take

You must migrate your static route configuration from GATEWAY statements to BEGINROUTES statements.

Follow these steps:

1. Obtain a dump of the TCP/IP stack address space from your z/OS V2R1 or V1R13 system.
2. Use the TCPIPCS PROFILE command against the dump. The command formats all configured static routes as BEGINROUTES profile statements.
3. Use the BEGINROUTES profile statements from the TCPIPCS PROFILE command output to replace the GATEWAY statements in your TCP/IP stack profile.

Remove any customization for the ZOSMIGV2R1_CS_GATEWAY health check in your HZSPRMxx parmlib member.

Reference information

For more information, see the following references:

- For more information about the TCP/IP profile BEGINROUTES statement, see BEGINROUTES statement in *z/OS Communications Server: IP Configuration Reference*.
- For more information on health check customization, see *IBM Health Checker for z/OS User's Guide*

SMTP: Prepare for the removal of SMTPD NJE Mail Gateway and Sendmail Description

z/OS V2R2 is the last release in which the Simple Mail Transport Protocol Network Job Entry (SMTPD NJE) Mail Gateway and Sendmail mail transports is planned to be supported. If you use the SMTPD NJE

Migration actions from z/OS V1R13: Communications Server

Gateway to send mail, IBM recommends that you use the CSSMTP SMTP NJE Mail Gateway instead. CSSMTP provides functional and performance improvements, and is designed so that application programming changes are not required.

No replacement functions are planned for the SMTPD or Sendmail listener support; these functions allow for receiving mail for delivery to local TSO/E or z/OS UNIX System Services user mailboxes, or for forwarding mail to other destinations.

Table 240 provides more details about this migration action. Use this information to plan your changes to the system.

Table 240. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	24 February 2014 in U.S. Announcement Letter 114-009.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended if you are using the SMTPD NJE Gateway function.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	<ul style="list-style-type: none">• ZOSMIGV2R2_Next_CS_SENDMAILDAEMN• ZOSMIGV2R2_Next_CS_SENDMAILCLIEN• ZOSMIGV2R2_Next_CS_SENDMAILMTA• ZOSMIGV2R2_Next_CS_SENDMAILMSA• ZOSMIGV2R2_Next_CS_SMTPDDAEMON• ZOSMIGV2R2_Next_CS_SMTPDMA

Steps to take

If you are using the SMTPD NJE Gateway, migrate to the existing CSSMTP SMTP NJE Mail Gateway.

Reference information

For more information, see *Statement of direction: IBM zEnterprise System, z/OS, and z/VM enhancements shorten time to value, deliver enhanced security, and improve data access 114-009 February 24, 2014.*

For information about the functions supported by CSSMTP, see the “Communications Server SMTP server” chapter of *z/OS Communications Server: IP Configuration Reference* and the “Mail on z/OS” chapter of *z/OS Communications Server: IP Configuration Guide*.

IP Services: Verify that the changed DHGroup default is acceptable

Description

In z/OS V2R2, the default value for the DHGroup parameter on the KeyExchangeOffer statement in the IPSec policy is changed from Group1 to Group2. If you have an IPSec policy, determine whether this change affects your policy. If you use the IBM Configuration Assistant for z/OS Communications Server to configure your IPSec policy, an explicit DHGroup value is generated on every KeyExchangeOffer statement. A default value is not used.

Migration actions from z/OS V1R13: Communications Server

Table 81 on page 137 provides more details about this migration action. Use this information to plan your changes to the system.

Table 241. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R2 and z/OS V2R1, both with APAR PI43832. z/OS V1R13 with APAR PI43833.
Applies to migration from:	z/OS V2R1 without APAR PI43832. z/OS V1R13 without APAR PI43833.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use an IPSec policy.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS checks:	None.

Steps to take

If your policy is not generated by IBM Configuration Assistant for z/OS Communications Server, search your IPSec policy files for any KeyExchangeOffer statements that do not specify a DHGroup parameter. If you find such a KeyExchangeOffer statement, your policy is effected. If you require the DHGroup value to continue to use the previous default of Group1, update your policy to explicitly set the DHGroup parameter to Group1. If you want to use the new default, you need to coordinate with the owners of each remote IKE peer that is associated with the z/OS policy changes to ensure that the remote peer's policy is compatible with the z/OS changes. If the z/OS policy changes so that it is incompatible with the remote peer's policy, the IKE daemons will no longer be able to successfully negotiate IPSec tunnels.

Note: Diffie-Hellman group 1 is considered a weak algorithm and is not recommended.

Reference information

For more information about the KeyExchangeOffer statement in the IPSec policy, see *z/OS Communications Server: IP Configuration Reference*.

IP Services: Replace configuration of additional z/OS legacy device types

Description

- | TCP/IP DEVICE and LINK profile statements for the following legacy device types will not be supported in a future release of IBM z/OS Communications Server:
 - | • FDDI and Token Ring (LCS with LINKs FDDI and IBMTR)
 - | • Token Ring (MPCIPA with LINK IPAQTR)
 - | • Ethernet and FDDI (MPCOSA with LINKs OSAENET and OSAFDDI)
- | If you are currently using these profile statements, migrate to a supported interface type, such as OSA-Express QDIO or HiperSockets. For more information about using OSA-Express QDIO or HiperSockets interfaces, see Considerations for networking hardware attachment in z/OS Communications Server: IP Configuration Guide.

Migration actions from z/OS V1R13: Communications Server

Table 82 on page 138 provides more details about this migration action. Use this information to plan your changes to the system.

Table 242. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	This change was announced in IBM United States Hardware Announcement 215-267 dated July 28, 2015.
Applies to migration from:	z/OS V1R13 and z/OS V2R1.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended because these TCP/IP device types will not be supported in a future release of IBM z/OS Communications Server.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	ZOSMIGV2R2_NEXT_CS_LEGACYDEVICE can help you determine whether you are using any legacy device statements in your TCP/IP profile. This check is provided in z/OS V2R1 and V2R2 with TCP/IP APAR PI49962 and SNA APAR OA49071 applied.

Steps to take

Use a supported TCP/IP interface type, such as OSA-Express QDIO or HiperSockets.

Reference information

For information about configuring OSA-Express QDIO and HiperSockets interfaces, see Considerations for networking hardware attachment in *z/OS Communications Server: IP Configuration Guide*.

IP Services: Prepare for the removal of the TFTPDP function

Description

z/OS V2R2 is planned to be the last release to include the Trivial File Transfer Protocol Daemon (TFTPDP) function in z/OS Communications Server. If you are using the TFTPDP function, IBM recommends that you migrate to a supported file transfer protocol, such as FTP.

Table 83 on page 139 provides more details about this migration action. Use this information to plan your changes to the system.

Table 243. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	See IBM United States Software Announcement 215-267 "IBM z/OS Version 2 Release 2—Fueling the new digital enterprise," dated July 28, 2015.
Applies to migration from:	z/OS V1R13 and z/OS V2R1.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended if you are using the TFTPDP function.

Table 243. Information about this migration action (continued)

Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you are using the TFTP function, IBM recommends that you migrate to a supported file transfer protocol, such as FTP.

Reference information

For information about the trivial file transfer protocol (TFTP) and the TFTP daemon, see *z/OS Communications Server: IP Configuration Reference*.

Communications Server actions to perform before the first IPL of z/OS V2R2

This topic describes Communications Server migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

IP Services: Allow the IKE daemon and the NSS daemon access to the CSFIQF resource of the CSFSERV class if ICSF is to be used with IP security Description

Starting in z/OS V2R1, the Internet Key Exchange daemon (IKED) and the NSS daemon perform additional status queries to ICSF. If ICSF is active and the CSFSERV class is active, the user IDs associated with IKED and NSSD must have READ access to the CSFIQF resource of the CSFSERV class. This access will allow IKED and NSSD to query ICSF.

Table 244 provides more details about this migration action. Use this information to plan your changes to the system.

Table 244. Information about this migration action

Element or feature:	Communications Server.
When change was introduced:	z/OS V2R1
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the IKE daemon or the NSS daemon will be started.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Migration actions from z/OS V1R13: Communications Server

Steps to take

If the CSFSERV class is active, give READ access to the user IDs associated with IKED and NSSD to the CSFIQF resource within the CSFSERV class.

Reference information

For more information, see “Steps for preparing to run IP security” in Appendix E in *z/OS Communications Server: IP Configuration Guide*.

IP Services: Allow users of AT-TLS access to CSFIQA and CSFRNG resources of the CSFSERV class if ICSF will be used with AT-TLS

Description

Starting in z/OS V2R1, System SSL will attempt to use ICSF services if ICSF is active during AT-TLS group initialization. If ICSF is active and the CSFSERV class is active, the userid associated with TCP/IP stack should have READ access to the CSFIQA and CSFRNG resources of the CSFSERV class. This will allow System SSL to be aware of the hardware available with ICSF and use ICSF to generate random numbers during initialization. Application userids using AT-TLS groups should also be given READ access to the CSFRNG resource of the CSFSERV class.

Table 245 provides more details about this migration action. Use this information to plan your changes to the system.

Table 245. Information about this migration action

Element or feature:	Communications Server
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. If the CSFSERV class is active, give READ access to the userid associated with the TCP/IP stack and any application userid using the TTLGroup to the CSFRNG resource within the CSFSERV class.
2. If the CSFSERV class is active, give READ access to the userid associated with the TCP/IP stack to the CSFIQA resource within the CSFSERV class.

Reference information

For more information, see “Chapter 3. Using Cryptographic Features with System SSL” in *z/OS Cryptographic Services System SSL Programming*.

IP Services: Ensure ICSF is active before starting the NSS daemon in FIPS 140 mode

Description

As of z/OS V2R1, FIPS 140 support now requires ICSF services. If the NSS daemon is configured in FIPS 140 mode, the daemon will fail to activate if ICSF is not active. Ensure that ICSF is started before starting the NSS daemon if it is configured in FIPS 140 mode.

Table 246 provides more details about this migration action. Use this information to plan your changes to the system.

Table 246. Information about this migration action

Element or feature:	Communications Server.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the NSS daemon is configured in FIPS 140 mode.
Target system hardware requirements:	None.
Target system software requirements:	ICSF must be active.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	The NSS daemon will fail to initialize.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If the NSS daemon is configured in FIPS 140 mode, ensure that ICSF is active prior to starting the NSS daemon.

Reference information

For more information, see “Steps for preparing the z/OS system for IP security” and “Steps for configuring IP security to support FIPS 140 mode” in Chapter 19 “IP Security” in *z/OS Communications Server: IP Configuration Guide*.

IP Services: Ensure ICSF is active before starting the IKE daemon in FIPS 140 mode

Description

As of z/OS V2R1, FIPS 140 support now requires ICSF services. If the Internet Key Exchange (IKE) daemon is configured in FIPS 140 mode, the daemon will fail to activate if ICSF is not active. Ensure ICSF is started before starting the IKE daemon if it is configured in FIPS 140 mode.

Table 247 provides more details about this migration action. Use this information to plan your changes to the system.

Table 247. Information about this migration action

Element or feature:	Communications Server.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.

Migration actions from z/OS V1R13: Communications Server

Table 247. Information about this migration action (continued)

Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the IKE daemon is configured in FIPS 140 mode.
Target system hardware requirements:	None.
Target system software requirements:	ICSF must be active.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	The IKE daemon will fail to initialize.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If the IKE daemon is configured in FIPS 140 mode, ensure ICSF is active prior to starting the IKE daemon.

Reference information

For more information, see “Steps for preparing the z/OS system for IP security” and “Steps for configuring IP security to support FIPS 140 mode” in Chapter 19 in *z/OS Communications Server: IP Configuration Guide*

IP Services: Ensure ICSF is active before starting the Policy Agent when AT-TLS groups are configured in FIPS 140 mode

Description

As of z/OS V2R1, FIPS140 support now requires ICSF services. Ensure ICSF is started before starting AT-TLS groups with FIPS140 support enabled. ICSF services will be used for random number generation and for Diffie Hellman support for generating key parameters, key pairs and key exchanges.

Table 248 provides more details about this migration action. Use this information to plan your changes to the system.

Table 248. Information about this migration action

Element or feature:	Communications Server
When change was introduced:	z/OS V2R1
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if AT-TLS groups are configured in FIPS 140 mode.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	The AT-TLS group will be installed but inactive.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Ensure ICSF is active before starting AT-TLS groups configured to support FIPS140-2
2. If the CSFSERV class is defined, give READ access to the userid associated with the TCPIP stack and any application userid using the TTLSGroup to the CSFRNG resource within the RACF CSFSERV class.
3. If the CSFSERV class is defined and Diffie Hellman is being used, give READ access to the application userid to the CSF1TRC, CSF1DVK, CSF1GKP, CSF1GSK, CSF1GAV, and CSF1TRD resources within the RACF CSFSERV class.

Reference information

For more information, see “FIPS 140-2 support” in *z/OS Communications Server: IP Configuration Guide*.

IP Services: Update automation on D TCPIP,tnproc,<Telnet>,CONN for the expanded EN TY column in message EZZ6064I Description

Message EZZ6064I, which is issued in response to a **D TCPIP,tnproc,<Telnet>,CONN** command, is expanded by two bytes to show a four byte cipher value when the connection is secured with AT-TLS. As a result of this change, the previous column header of EN TY has been changed to ENCR TYPE. The cipher value can be up to four bytes in length. Cipher values less than four bytes are padded with blanks.

Table 249 provides more details about this migration action. Use this information to plan your changes to the system.

Table 249. Information about this migration action

Element or feature:	Communications Server
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if automating on the D TCPIP,tnproc,<Telnet>,CONN command message EZZ6064I.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Be aware of the changes in message EZZ6064I.
- Update any automation on message EZZ6064I.

Migration actions from z/OS V1R13: Communications Server

Reference information

For an example of the updated **D TCPIP, tnproc, <Telnet>, CONN** output, see *z/OS Communications Server: IP System Administrator's Commands* .

IP Services: Update automation to monitor resolver address space initialization completion messages

Description

In releases before z/OS V2R1, the resolver address space initialization failed if errors were detected in the setup file. Beginning with z/OS V2R1, the resolver processes the entire resolver setup file during resolver address space initialization. When the resolver detects syntax errors or when it does not recognize the resolver setup statement, the resolver ignores the setup file statement and the resolver initialization completes successfully with warning messages. Ignoring the setup file statement might result in the resolver using default settings for some resolver setup statements if the statement was specified with errors.

If the resolver issues warning messages during address space initialization, the resolver issues message EZD2038I instead of message EZZ9291I when the initialization completes.

Table 250 provides more details about this migration action. Use this information to plan your changes to the system.

Table 250. Information about this migration action

Element or feature:	Communications Server
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you customize the resolver and want to correct any errors that the resolver finds in the resolver setup file.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	The resolver might initialize with the incorrect configuration because of errors in the setup file, which might cause applications issuing resolver API calls to get erroneous results.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you customize the resolver and want to detect when the resolver ignores errors in the resolver setup file during address space initialization, do the following:

- Monitor resolver address space initialization for message EZD2038I RESOLVER INITIALIZATION COMPLETED WITH WARNINGS.
- Issue the MODIFY RESOLVER,DISPLAY command after system initialization completed to determine if the following message has been issued in the display output:
EZD2039I WARNINGS ISSUED DURING RESOLVER INITIALIZATION

If the resolver issues the message EZD2038I or EZD2039I, do the following:

Migration actions from z/OS V1R13: Communications Server

1. Collect the system console messages that are issued by the resolver during resolver address space initialization.
2. Contact the system programmer. The system programmer needs to use the resolver warning messages to correct the errors in the resolver setup file.
3. When the errors are corrected, the network operator needs to issue a MODIFY RESOLVER,REFRESH,SETUP=setup_file command to correct the resolver configuration.

Reference information

For more information about the resolver, see “Customizing the resolver” in *z/OS Communications Server: IP Configuration Guide*.

IP Services: Update OMPROUTE configuration procedures for OMPROUTE_OPTIONS

Description

Before z/OS V2R1, the OMPROUTE_OPTIONS environment variable was used by OMPROUTE to set various controls for OMPROUTE processing and only the hello_hi option was supported. The hello_hi option optimized the processing of OSPF Hello packets in OMPROUTE to minimize the potential adjacency failures with neighbors.

Beginning with z/OS V2R1, the OMPROUTE_OPTIONS environment variable is ignored and will not be supported in a future release. The optimization function for OSPF Hello packets is always enabled

If the environment variable, OMPROUTE_OPTIONS, is configured then the following message will be issued to the console or hardcopy log:

```
EZZ8172I jobname IGNORING ENVIRONMENT VARIABLE OMPROUTE_OPTIONS WHICH WILL BE  
RETIRED IN A FUTURE RELEASE
```

Table 251 provides more details about this migration action. Use this information to plan your changes to the system.

Table 251. Information about this migration action

Element or feature:	Communications Server.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	No, but recommended if the environment variable OMPROUTE_OPTIONS=hello_hi is coded.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you want to suppress the warning message that the environment variable OMPROUTE_OPTIONS is to be retired in a future release, remove the environment variable from the OMPROUTE environment variable file.

Migration actions from z/OS V1R13: Communications Server

Reference information

For more information, see “Steps for Configuring OMPROUTE” in *z/OS Communications Server: IP Configuration Guide*.

IP Services: Check the values specified for TCP related configuration statements Description

As of z/OS V2R1 the default values for TCPCVBUFRSIZE and TCPSENBUFFERSIZE parameters on the TCPCONFIG statement have been increased from 16K to 64K. Increasing the receive or send buffer size does not in itself allocate or consume any additional storage. The receive and send buffer sizes determine the amount of data that can be buffered by TCPIP for the application. The increase in the default values can allow more data to be buffered and consequently, more storage to be used.

The default value for the SOMAXCONN statement has increased from 10 to 1024. The SOMAXCONN value limits what a server application can specify for its listening backlog.

The amount of time a connection remains in FINWAIT2 has been changed to use the value specified on the TCPCONFIG parameter FINWAIT2. Previously, an additional seventy five seconds was added to the time specified on the FINWAIT2 parameter before the connection was dropped.

Table 252 provides more details about this migration action. Use this information to plan your changes to the system.

Table 252. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, for one of the following conditions: <ul style="list-style-type: none">• If the potential increase in the size of the send and receive buffers is likely to cause a storage shortage• If you used the current defaulted value of SOMAXCONN to limit applications from specifying a listening backlog larger than 10• If you require the additional seventy-five seconds before the connection is dropped
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If needed, do the following:

- Change the TCPCVBUFRSIZE and TCPSENBUFFERSIZE values to 16K.
- Change the SOMAXCONN value to 10.
- Increase the FINWAIT2 value by 75 seconds.

Reference information

For more information about configuration statements in z/OS Communications Server, see *z/OS Communications Server: IP Configuration Reference*.

IP Services: Make changes for Netstat enhancements

Description

The Netstat command displays the status of a local host. In each release of z/OS, the Netstat reports can change in ways that can affect automation or front-end programs.

Table 85 on page 141 provides more details about this migration action. Use this information to plan your changes to the system.

Table 253. Information about this migration action

Element or feature:	Communications Server
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the changed or removed settings affect either automation that uses the Netstat report output or front-end programs that invoke the Netstat command.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Accommodate the Netstat changes in your automation and front-end programs. You can begin by reviewing the ways in which the displays are updated in each release. For details about the changes for each Netstat report, see *z/OS Summary of Message and Interface Changes*. However, you must run the commands to know with certainty what changes to make after IPL on a z/OS V2R2 system.

Reference information

For more information, see the following references:

- For information about using the Netstat command, see *z/OS Communications Server: IP System Administrator's Commands*
- For information about the Netstat report changes, see *z/OS Summary of Message and Interface Changes*.

IP Services: Use the new maximum segment size adjustments if required

Description

New function is introduced in z/OS V2R2 to automatically adjust the Maximum Segment Size (MSS) that is used on a TCP connection to avoid fragmentation. This function is turned on by default. If you need to continue using your existing setting for the MSS, see “Steps to take” on page 148.

Table 92 on page 148 provides more details about this migration action. Use this information to plan your changes to the system.

Migration actions from z/OS V1R13: Communications Server

Table 254. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you do not want the automatic reduction of MSS.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	A performance degradation can result if the MSS is not configured to avoid fragmentation.
Related IBM Health Checker for z/OS check:	None.

Steps to take

To disable the auto-adjusting function and continue using your existing setting for the MSS from the prior release, specify the subparameter `ADJUSTVIPAMSS NONE` on the parameter `GLOBALCONFIG`.

Reference information

For more information, see *z/OS Communications Server: IP Configuration Reference*.

IP Services: Check code that automates on IKE daemon syslogd messages Description

Scalability enhancements in z/OS V2R2 Communications Server introduce a new internal thread pool to the Internet Key Exchange (IKE) daemon. As part of this change, all of the IKED messages that are written through syslogd will contain the thread identifier in the syslogd header, which precedes the message identifier. In addition, messages from different IKED threads might be interleaved. These changes might affect the automation code that parses these IKED messages:

- If the automation code parses individual IKED messages in syslogd destinations based on any sort of position-based logic (for example, counting blanks delimiters, relying on a specific column), you need to update to account for the new thread id field.
- If the automation code parses individual IKED messages based on message content (for example, searching the string for specific message identifiers), no change is needed.
- If the automation code depends on the order of the IKED messages, you might need to update to take the thread id field into account so that the code ignores messages from other threads that are interleaved with the messages of interest.

IKED messages are those in the ranges EZD0902I - EZD1160I, EZD1751I - EZD1800I, and EZD1901I - EZD1925I as well as EZD2017I, EZD2019I, EZD2025I and EZD2027I.

The following example shows a small excerpt of messages from z/OS V2R1 and the equivalent messages from z/OS V2R2 with the imbedded thread identifiers:

```
V2R1:
Jul 28 11:39:26 mvs046 IKE: EZD1061I IKE connecting to PAGENT
Jul 28 11:39:26 mvs046 IKE: EZD1062A IKE retrying connection to PAGENT
Jul 28 11:39:34 mvs046 IKE: EZD0923I IKE has received the STOP command
Jul 28 11:39:34 mvs046 IKE: Message instance 0: EZD0967I IKE release
CS V2R1 Service Level CS130924 Created on Sep 24 2013
Jul 28 11:39:34 mvs046 IKE: Message instance 14: EZD1116I IKE detected
```

Migration actions from z/OS V1R13: Communications Server

an NAPT in front of the remote security endpoint while initiating a new phase 1 tunnel

V2R2:

Jul 28 15:10:47 mvs046 IKE: (00000001) EZD1061I IKE connecting to PAGENT

Jul 28 15:10:47 mvs046 IKE: (00000001) EZD1062A IKE retrying connection to PAGENT

Jul 28 15:11:06 mvs046 IKE: (00000003) EZD0923I IKE has received the STOP command

Jul 28 15:11:06 mvs046 IKE: Message instance 0: (00000001) EZD0967I IKE release

CS V2R2 Service Level CS140728 Created on Jul 28 2014

Jul 28 15:11:06 mvs046 IKE: Message instance 14: (00000007) EZD1116I IKE detected

an NAPT in front of the remote security endpoint while initiating a new phase 1 tunnel

Table 93 on page 149 provides more details about this migration action. Use this information to plan your changes to the system.

Table 255. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use the z/OS IKE daemon and you have code that automates on IKED messages written through syslogd.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Change the code that automates on IKED messages written through syslogd to account for the thread identifier that is added to the header area preceding the IKED message number.

Reference information

None.

IP Services: Decide whether to accept the new FIXED CSM default Description

In z/OS V2R2, the default amount for communications storage manager (CSM) fixed storage for buffers is increased from 100 MB to 200 MB. Your installation can specify a value for the CSM fixed storage amount on the FIXED statement in the IVTPRM00 parmlib member.

Table 94 on page 150 provides more details about this migration action. Use this information to plan your changes to the system.

Table 256. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R2.

Migration actions from z/OS V1R13: Communications Server

Table 256. Information about this migration action (continued)

Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use the default CSM FIXED MAX value of 100M and you do not want to use the new default of 200M.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you did not previously code a value for FIXED in IVTPRM00 and you do not want the new default, specify FIXED MAX(100M) 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.

Reference information

For information about the IVTPRM00 parmlib member, see the IVTPRM00 parmlib member in *z/OS Communications Server: New Function Summary*.

IP Services: Update /etc configuration files Description

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.

Table 86 on page 142 provides more details about this migration action. Use this information to plan your changes to the system.

Table 257. Information about this migration action

Element or feature:	Communications Server.
When change was introduced:	Various releases. See Table 87 on page 142.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have customized a configuration file (listed in Table 87 on page 142) that IBM has changed.

Migration actions from z/OS V1R13: Communications Server

Table 257. Information about this migration action (continued)

Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you added installation-dependent customization to any of the IBM-provided configuration files listed in Table 87 on page 142, make the same changes in the new versions of the files by copying the IBM-provided samples to the files shown in the table and then customizing the files.

Table 258. Changed Communications Server configuration files

Utility	IBM-provided sample file	Target location	What changed and when
Communications Server z/OS UNIX applications	SEZAINST(SERVICES)	/etc/services	In z/OS V2R2, the NCPROUT entry is removed because NCPROUTE is no longer supported. If you update /etc/services, ensure that you also update the ETC.SERVICES data set.
DCAS	No sample provided	/etc/dcas.conf	In z/OS V2R2, a new TLSV1ONLY keyword is provided to configure SSLv3 protocol for connections secured using the DCAS SSL support.
File Transfer Protocol Daemon (FTPD)	SEZAINST(FTPDATA)	/etc/ftp.data	In z/OS V2R1, a configuration statement was provided to specify that a type 119 SMF record of subtype 71 is collected for the FTP daemon configuration information when the FTP daemon starts.
FTP Server and Client	SEZAINST(FTCDATA) for the client and (FTPDATA) for the server	/etc/ftp.data	In z/OS V2R2, a new SSLV3 keyword is provided to configure SSLv3 protocol for connections secured using the FTP TLS support.
Internet Key Exchange Daemon(IKED)	/usr/lpp/tcpip/samples/iked.conf	/etc/security/iked.conf	In z/OS V2R2, a new log level is added for the IKE daemon.
Policy agent	/usr/lpp/tcpip/samples/pagent.conf	/etc/pagent.conf	In z/OS V2R2, a new ServerSSLv3 keyword is provided to configure SSLv3 protocol for the policy client connecting to the server.
Sendmail	/usr/lpp/tcpip/samples/sendmail/cf/zOS.cf	/etc/mail/zOS.cf	In z/OS V2R2, a new SSLV3 keyword is provided to configure SSLv3 protocol for connections secured using System SSL.

Migration actions from z/OS V1R13: Communications Server

Table 258. Changed Communications Server configuration files (continued)

Utility	IBM-provided sample file	Target location	What changed and when
SNMP agent	/usr/lpp/tcpip/samples/osnmpd.data	/etc/osnmpd.data	Every release, the value of the sysName MIB object is updated to the current release.
SNMP agent	/usr/lpp/tcpip/samples/snmpd.conf	/etc/snmpd.conf	In z/OS V2R2, a new privacy protocol value AESCFB128 can be specified on a USM_USER statement to request AES 128-bit encryption.
z/OS UNIX snmp command	/usr/lpp/tcpip/samples/snmpv2.conf	/etc/osnmp.conf	In z/OS V2R2, a new privacy protocol value AESCFB128 can be specified on a statement for an SNMPv3 user to request AES 128-bit encryption.

Reference information

For more information about Communications Server configuration files, see *z/OS Communications Server: IP Configuration Guide*.

IP Services: Verify z/OS UNIX file permission settings Description

As of z/OS V2R2, z/OS UNIX file security is enhanced to include additional restrictions for some of the z/OS UNIX files that belong to z/OS Communications Server functions. Table 89 on page 144 lists the affected z/OS UNIX files. For any existing file that does not comply with the restrictions, take the following steps:

- If the file is not a symbolic link or hard link, delete the file.
- If the file is a symbolic link or hard link, change the incorrect permissions of the file or directory, and the owning information if any.

Table 88 on page 144 provides more details about this migration action. Use this information to plan your changes to the system.

Table 259. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R1 with APAR PI16886, and z/OS V1R13 with APAR PI17084.
Applies to migration from:	z/OS V2R1 without APAR PI16886, and z/OS V1R13 without APAR PI17084.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if any files you have are affected by the restrictions in Table 89 on page 144.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Verify whether the z/OS UNIX files in Table 89 on page 144 comply with the restrictions. To conform with the restrictions, correct any discrepancies that are found.

Table 260. Affected z/OS UNIX files.

Function	File name	Restrictions
DCAS	/tmp/dcas.tcpname_or_INET.pid	1,2,3
IKED	/var/ike/iked.pid	1,2,3
Network SLAPM2 subagent	/tmp/nslapm2.tcpname.pid	1,2,3
Policy Agent	<ul style="list-style-type: none"> • /tmp/tcpname.Pagent.tmp • /tmp/pagent.pid 	1,2,3
Popper	user bulletin and maildrop files in directory /usr/mail	1,2
RSVP	/tmp/rsvpd.pid.imagename	1,2,3
SNTP	/etc/sntpd.pid	1,2,3
Syslog	<ul style="list-style-type: none"> • /etc/syslog.pid • /etc/syslog_net.pid 	1,2,3
TCP/IP stack	/tmp/tcpname.Pagent.tmp	1,2

Restrictions:

1. If the file is a symbolic link, it must have an owning UID or GID that matches the EUID or EGID that is assigned to the listed function.
2. If the file is a hard link or the target of a hard link, users that are outside the owner or group of the directory in which the file is stored cannot have write access to the directory.
3. Additionally, write access to the file must be limited to the owning UID or group, for example, --w--w---- permissions.

Reference information

None.

IP Services: Enable SSLv3 for z/OS components if required

Description

In z/OS V2R2, Communications Server changed its default protocol support for components that use SSL/TLS natively or through AT-TLS. SSLv3 is now disabled by default, which can affect the usage of AT-TLS, the FTP client and server, the TN3270 server, the DCAS server, Policy Agent, and sendmail. For any exploiters (installations and applications) that must continue to use SSLv3, you can explicitly enable this protocol.

Table 90 on page 145 provides more details about this migration action. Use this information to plan your changes to the system.

Table 261. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R1 with APAR PI28679, and z/OS V1R13 with APAR PI28678.
Applies to migration from:	z/OS V2R1 without APAR PI28679 and z/OS V1R13 without APAR PI28678.

Migration actions from z/OS V1R13: Communications Server

Table 261. Information about this migration action (continued)

Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have applications that use SSLv3.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Review each of the Communications Server components that follow to determine whether you are affected. Make changes as directed. For applications that are protected by AT-TLS and that require SSLV3, evaluate their usage and change them to use TLS protocols, if possible. TLS addresses many security deficiencies that exist in the prior SSLv2 and SSLv3 protocols. For applications that must continue to use SSLv3, you can explicitly enable this protocol, as described in the sections that follow.

AT-TLS

AT-TLS is modified to disable SSLv3 by default. Any applications that are protected by AT-TLS default to SSLv3 Off.

If SSLv3 is explicitly enabled in your policy, no action is required. However, it is recommended that you evaluate whether applications can be updated to use a more secure protocol version, such as TLSv1, TLSv1.1, or TLSv1.2.

Applications that require SSLv3, and for which this protocol is not explicitly enabled in the policy, rely on AT-TLS defaults. For these applications, you can enable SSLv3 at the environment or connection level by specifying the parameter SSLV3 on the relevant TTLSEnvironmentAdvancedParms or TLSConnectionAdvancedParms policy statement with a value of ON. For Configuration Assistant users, you can enable SSLv3 in the **name** tab of the Modify Security Level dialog under the AT-TLS perspective.

FTP client and server

The FTP client and FTP server are modified to disable SSLv3 by default when TLSMECHANISM FTP is specified. In this mode, the FTP client or server uses System SSL APIs natively for SSL/TLS protection, rather than AT-TLS.

Because the z/OS FTP client and server enabled SSLv3 by default, evaluate whether either of the following conditions are true:

- Your server is supporting clients that require SSLv3
- Your client is connecting to a server that requires SSLv3

If so, you can enable SSLv3 by specifying the new parameter SSLV3 in the relevant FTP configuration data set FTP.DATA with a value of TRUE.

If TLSMECHANISM ATTLS is specified, the FTP client or server is protected by AT-TLS; the changes that are described for the AT-TLS function apply.

TN3270 server

The TN3270 server is modified to disable SSLv3 by default when SECUREPORT is specified. In this mode, the TN3270 server uses System SSL APIs natively for SSL/TLS protection, rather than AT-TLS.

Because the TN3270 server enabled SSLv3 by default, determine whether your server is supporting clients that require SSLv3. If so, you can enable SSLv3 by specifying the new statement SSLV3 in the relevant TN3270 profile data set and refreshing the configuration by using the command **VARY TCP/IP, tnproc, OBEYFILE**.

Migration actions from z/OS V1R13: Communications Server

If `TTLSPORT` is specified, the TN3270 server is protected by AT-TLS; the changes that are described for the AT-TLS function apply.

DCAS server

The DCAS server is modified to disable SSLv2 and SSLv3 by default when `TLSMECHANISM DCAS` is specified. In this mode, the DCAS server uses System SSL APIs natively for its SSL/TLS protection, rather than AT-TLS.

Because the DCAS server enabled SSLv2 and SSLv3 by default, evaluate whether your server is supporting clients that require SSLv2 or SSLv3. If so, you can enable SSLv2 and SSLv3 by specifying the new parameter `TLSV10ONLY` in your DCAS configuration file with a value of `FALSE` and restarting DCAS.

If `TLSMECHANISM ATTLS` is specified, the DCAS server is protected by AT-TLS; the changes that are described for the AT-TLS function apply.

Policy Agent

The Policy agent, when it operates as a policy client, is modified to disable SSLv3 by default. Because the policy client enabled SSLv3 by default, evaluate whether your policy server supports SSLv3 only. If so, you can enable SSLv3 by specifying the new parameter `ServerSSLv3` on the `ServerSSL` substatement of the `ServerConnection` statement with a value of `ON` in the policy agent main configuration file. Then, update the policy agent configuration by using the command **MODIFY pagent,UPDATE**.

Sendmail

Sendmail, which operates as both a client and server, is modified to disable SSLv3 by default. Because the z/OS sendmail program enabled SSLv3 by default, evaluate whether either of the following conditions is true:

- Your server is supporting clients that require SSLv3
- Your client is connecting to a server that requires SSLv3

If so, you can enable SSLv3 by specifying the parameter `SSLV3` in the `zOS.cf` configuration file with a value of `TRUE` and restarting sendmail.

Reference information

None.

SNA Services: Update TIBUF pool size and T1BUF pool size Description

z/OS V2R2 reduces the number of buffers per page of storage for the following buffer pools:

TIBUF pool bufsize change

The TIBUF pool contains control information to support HPDT services for HPR or IP. It is used to contain the HPR headers and the media, IP, and UDP headers for an Enterprise Extender connection. It is also used to contain data for APPC conversations.

T1BUF pool bufsize change

The T1BUF pool contains control information to support HPDT services for HPR or IP. It is similar to the TIBUF pool, but larger. It is used as a packing buffer by HiperSockets accelerator and QDIO. It is also used to contain the HPR headers and the media, IP, and UDP headers for an Enterprise Extender connection.

Table 95 on page 151 provides more details about this migration action. Use this information to plan your changes to the system.

Table 262. Information about this migration action

Element or feature:	z/OS Communications Server.
---------------------	-----------------------------

Migration actions from z/OS V1R13: Communications Server

Table 262. Information about this migration action (continued)

When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have modified the buffer pool values for the TIBUF pool or the T1BUF pool, and you might want to revisit your settings.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Enterprise Extender performance degradation can result from poorly tuned buffers.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you have tuned your systems to require a specific number of pages of TIBUF or T1BUF buffer storage, you might need to recalculate the number of pages required. For information, see Tuning Enterprise Extender specific buffer pools in *z/OS Communications Server: SNA Network Implementation Guide*.

Reference information

For information about how to adjust the value, see Tuning Enterprise Extender specific buffer pools in *z/OS Communications Server: SNA Network Implementation Guide*.

For more information, see the following references:

- *z/OS Communications Server: SNA Resource Definition Reference*
- *z/OS Communications Server: SNA Operation*

Communications Server actions to perform after the first IPL of z/OS V2R2

This topic describes Communications Server migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

Migrate environment variable settings

Description

With PM62905 and OA39422 applied on z/OS V1R13, support for the TLSv1.2 protocol or support for the RFC 5746 renegotiation could be configured by coding environment variables such as GSK_PROTOCOL_TLSV1_2=ON or GSK_RENEGOTIATION=NONE in a file pointed to by the Envfile parameter on the TTLSTGroupAdvancedParms statement. In z/OS V2R1, support for the TLSv1.2 protocol and the RFC 5746 renegotiation is configured in the AT-TLS policy configuration. The TLSv1.2 protocol is configured on the TTLSEnvironmentAdvancedParms or TLSSTConnectionAdvancedParms statement. The RFC 5746 renegotiation is configured on the TTLSEnvironmentAdvancedParms statement.

Table 263 on page 341 provides more details about this migration action. Use this information to plan your changes to the system.

Migration actions from z/OS V1R13: Communications Server

Table 263. Information about this migration action

Element or feature:	z/OS Communications Server.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the TLSv1.2 support or the RFC 5746 renegotiation is enabled in a file pointed to by the Envfile parameter on the TTLSEnvironmentAdvancedParms statement.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. If support for the TLSv1.2 protocol is configured by specifying `GSK_PROTOCOL_TLSV1_2=ON` from the file pointed to by the Envfile parameter on the `TTLSEnvironmentAdvancedParms` statement, remove `GSK_PROTOCOL_TLSV1_2=ON` from the file and configure TLSv1.2 On on the `TTLSEnvironmentAdvancedParms` statement.
2. If support for the RFC 5746 renegotiation is configured from the file pointed to by the Envfile parameter on the `TTLSEnvironmentAdvancedParms` statement, remove the environment variable from the file and configure the equivalent support on the `TTLSEnvironmentAdvancedParms` statement.
 - If `GSK_RENEGOTIATION=NONE` is configured, configure Renegotiation Default.
 - If `GSK_RENEGOTIATION=DISABLE` is configured, configure Renegotiation Disable.
 - If `GSK_RENEGOTIATION=ALL` is configured, configure Renegotiation All.
 - If `GSK_RENEGOTIATION=ABBREVIATED` is configured, configure Renegotiation Abbreviated.
 - If `GSK_EXTENDED_RENEGOTIATION_INDICATOR=OPTIONAL` is configured, configure RenegotiationIndicator Optional.
 - If `GSK_EXTENDED_RENEGOTIATION_INDICATOR=CLIENT` is configured, configure RenegotiationIndicator Client.
 - If `GSK_EXTENDED_RENEGOTIATION_INDICATOR=SERVER` is configured, configure RenegotiationIndicator Server.
 - If `GSK_EXTENDED_RENEGOTIATION_INDICATOR=BOTH` is configured, configure RenegotiationIndicator Both.
 - If `GSK_RENEGOTIATION_PEER_CERT_CHECK=OFF` is configured, configure RenegotiationCertCheck Off.
 - If `GSK_RENEGOTIATION_PEER_CERT_CHECK=ON` is configured, configure RenegotiationCertCheck On.

Reference information

See *z/OS Communications Server: IP Configuration Reference* for information about:

- Using the `TTLSEnvironmentAdvancedParms` or `TTLSEnvironmentAdvancedParms` statement for the syntax for coding TLSv1.2.
- Configuring support for the RFC 5746 renegotiation.

Cryptographic Services migration actions

This topic describes migration actions for base element Cryptographic Services. Included are the components Integrated Cryptographic Service Facility (ICSF), Open Cryptographic Services Facility (OCSF), PKI Services, and System Secure Sockets Layer (SSL).

Cryptographic Services actions to perform before installing z/OS V2R2

This topic describes Cryptographic Services migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

ICSF: Detect any coprocessor that will not become active when HCR77A1 or later is started

Description

For ICSF FMIDS HCR7780, HCR7790, and HCR77A0, the activation procedure was designed to maximize the number of active coprocessors by selecting the set of master keys that are available on the majority of coprocessors. A DES master key is no longer required in order for a coprocessor to become active. Instead, any one of four master keys – the DES master key, the AES master key, the RSA master key (which in earlier releases was called the asymmetric master key), or the ECC master key – is enough for a coprocessor to become active. However, because the goal is to select the combination of master keys that will maximize the number of active coprocessors, if a certain master key is not set on all the same coprocessors, that master key support will not be available.

Starting with FMID HCR77A1, the activation procedure now uses the master key verification patterns (MKVP) in the header record of the CKDS and PKDS to determine which coprocessors become active. If the MKVP of a master key is in the CKDS or PKDS, that master key must be loaded and the verification pattern of the current master key register must match the MKVP in the CKDS or PKDS. If all of the MKVPs in the CKDS and PKDS match the current master key registers, the coprocessor will become active. Otherwise, the status is master keys incorrect. This applies to all master keys that the coprocessor supports. When there is a MKVP in the CKDS or PKDS and the coprocessor does not support that master key, it is ignored. When a MKVP is not in the CKDS or PKDS, the master key is ignored.

If there are no MKVPs in the CKDS and PKDS, the coprocessor will be active. If the CKDS is initialized without any MKVPs, the CKDS cannot be used on a system that has cryptographic features installed.

Table 96 on page 152 provides more details about this migration action. Use this information to plan your changes to the system.

Table 264. Information about this migration action

Element or feature:	Cryptographic Services
When change was introduced:	Cryptographic Support for z/OS V1R13 - z/OS V2R1 web deliverable (FMID HCR77A1), which installs on z/OS V1R13 or z/OS V2R1.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without the Cryptographic Support for z/OS V1R13 - z/OS V2R1 web deliverable (FMID HCR77A1) or a later ICSF web deliverable installed.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you are affected by the change in the way master keys are processed to determine which coprocessors become active.
Target system hardware requirements:	None.
Target system software requirements:	None.

Migration actions from z/OS V1R13: Cryptographic Services

Table 264. Information about this migration action (continued)

Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	Use check ICSFMIG77A1_COPROCESSOR_ACTIVE to determine which coprocessors will not become active when Cryptographic Support for z/OS V1R13 - z/OS V2R1 Web Deliverable (FMID HCR77A1) is started. This check is delivered in APAR OA42011 available for ICSF FMIDs HCR7770, HCR7780, HCR7790 and HCR77A0.

Steps to take

Run the migration check ICSFMIG77A1_COPROCESSOR_ACTIVE to find any coprocessors that will not become active when you start HCR77A1 or a later ICSF web deliverable.

Reference information

For more information, see the following references:

- See the chapter on migration in *z/OS Cryptographic Services ICSF System Programmer's Guide*
- For information about IBM Health Checker, see *IBM Health Checker for z/OS User's Guide*.

ICSF: Detect TKDS objects that are too large for the new record format in HCR77A1

Description

In ICSF FMID HCR77A1, ICSF is introducing a common key data set record format for CCA key tokens and PKCS #11 tokens and objects. This new record format adds new fields for key utilization and metadata. Because of the size of the new fields, some existing PKCS #11 objects in the TKDS might cause ICSF to fail. If you do not have a Token Data Set (TKDS) with PKDS #11 objects in it, there is no need to run this check.

The problem exists for TKDS object records with large objects. The User data field in the existing record will cause the TKDS not be to loaded if the object size is greater than 32,520 bytes. The TKDSREC_LEN field in the record has the size of the object. If the User data field is not empty and the size of the object is greater than 32,520 bytes, the TKDS cannot be loaded.

Note that ICSF does not provide any interface to modify the User data field in the TKDS object record. A field can be created using IDCAMS. Check the contents of the User data field and determine if the information in the field is valuable. If you want to preserve the data, consider how the information can be stored other than in the object record. The field can only be modified by editing the record. For information about the TKDS object record, see *z/OS Cryptographic Services ICSF System Programmer's Guide*. The IBM Health Checker migration check, ICSFMIG77A1_TKDS_OBJECT detects any TKDS object that is too large to allow the TKDS is read into storage during ICSF initialization starting with ICSF FMID HCR77A1. This migration check is available for HCR7770, HR7780, HCR7790, and HCR77A0 through APAR OA42011

Table 97 on page 153 provides more details about this migration action. Use this information to plan your changes to the system.

Table 265. Information about this migration action

Element or feature:	Cryptographic Services
---------------------	------------------------

Migration actions from z/OS V1R13: Cryptographic Services

Table 265. Information about this migration action (continued)

When change was introduced:	Cryptographic Support for z/OS V1R13 – z/OS V2R1 web deliverable (FMID HCR77A1), which installs on z/OS V1R12, z/OS V1R13 or z/OS V2R1.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without the Cryptographic Support for z/OS V1R13 - z/OS V2R1 web deliverable (FMID HCR77A1) installed.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you affected by the record format changes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	Use the IBM Health Checker migration check ICSFMIG77A1_TKDS_OBJECT to detect any TKDS object with a value in the User data field that is too large to preserve in the User data field of the new format record. This migration check is available for HCR7770, HR7780, HCR7790, and HCR77A0 through APAR OA42011.

Steps to take

Run the migration check ICSFMIG77A1_TKDS_OBJECT to detect if TKDS objects are too large for the new record format in HCR77A1.

Note: ICSF does not provide any interface to modify the User data field in the TKDS object record. A flat file can be created using IDCAMS. Check the contents of the User data field and determine if the information in the field is valuable. If you want to preserve the data, consider how the information can be stored other than in the object record. The field can only be modified by editing the record. For information about the TKDS object record, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.

Reference information

For more information, see the following references:

- For information about TKDS, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.
- For information about IBM Health Checker, see *IBM Health Checker for z/OS User's Guide*.

ICSF: Determine if applications using hash services have archived hashes of long data

Description

Due to service introduced by APAR OA43937, new Hash Method Rule keywords for the ICSF One-Way Hash Generate (CSNBOWH or CSNBOWH1 and CSNEOWH or CSNEOWH1) and PKCS11 One-Way Hash Services (CSFPOWH and CSFPOWH6) will support generation of legacy hash values for verification of archived hash values generated from pre-OA43937 releases of HCR7770 and higher.

Note: This correction of hashing function does not apply to the case where the sum of the length of hashed text over a series of chained calls exceeds 256 megabytes (or 512, as described further in this topic), but no single invocation supplies an input *text_length* that exceeds 256 (or 512) megabytes. Correct hashes are created when no single invocation of the callable services exceeds the described limit prior to (and after) application of the PTFs for OA43937.

Migration actions from z/OS V1R13: Cryptographic Services

Applications that wish to verify archived hash values created by pre-OA43937 HCR7770 and higher releases of ICSF callable services One-Way Hash Generate and PKCS11 One-Way Hash may need to invoke these callable services with new rule array keywords that support the creation of legacy hash values. The hash generated using the new rule array keywords must be used to verify the archived hash values.

The ICSF Callable Services One-Way Hash Generate and PKCS11 One-Way Hash, sign, or verify have corrected the way they create hash values when the length of the text on a single invocation of one of these services supplies an input *text_length* that equals or exceeds 256 megabytes (512 megabytes on z990/z890 or later hardware on HCR7770). The hashing services are corrected with the application of the PTFs for OA43937.

Table 98 on page 155 provides more details about this migration action. Use this information to plan your changes to the system.

Table 266. Information about this migration action

Element or feature:	Cryptographic Services.
When change was introduced:	PTFs for OA43937, which are applicable to: ICSF FMIDs HCR7770 - HCR77A1 (z/OS V1R12 - z/OS V2R1).
Applies to migration from:	ICSF FMIDs HCR7770 - HCR77A1, without the PTF for OA43937.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have archived hash values created before the installation of the PTFs for OA43937 which meet the length restrictions described here.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	If you do not use the legacy rule array keywords for affected applications, then the application may fail to verify the legacy hashes/signatures.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Identify if your application needs to verify archived hash values created by either of the ICSF callable service One-Way Hash Generate (CSNBOWH or CSNBOWH1 and CSNEOWH or CSNEOWH1) or PKCS11 One-Way Hash (CSFPOWH and CSFPOWH6) on releases pre-OA43937 at HCR7770 and higher. (See the ICSF Application Programmer's Guide documentation changes in this APAR for new ICSF callable service keywords that support the creation of hashes for the verification of archived hash values and the input text length requirements.)
2. If your application has these archived hash values and intends to verify them, then invocations of ICSF callable services One-Way Hash Generate, PKCS11 One-Way Hash, sign, or verify that create hashes for verification of the archived hash values may need to be updated to use the new legacy rule array keywords (ONLY if those archived hash values were created with input text length exceeding the limits described).

Reference information

For more information, see *z/OS Cryptographic Services ICSF Application Programmer's Guide* .

Cryptographic Services actions to perform before the first IPL of z/OS V2R2

This topic describes Cryptographic Services migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

ICSF: Determine if applications using hash services have archived hashes of long data

Description

Due to service introduced by APAR OA43937, new Hash Method Rule keywords for the ICSF One-Way Hash Generate (CSNBOWH or CSNBOWH1 and CSNEOWH or CSNEOWH1) and PKCS11 One-Way Hash Services (CSFPOWH and CSFPOWH6) will support generation of legacy hash values for verification of archived hash values generated from pre-OA43937 releases of HCR7770 and higher.

Note: This correction of hashing function does not apply to the case where the sum of the length of hashed text over a series of chained calls exceeds 256 megabytes (or 512, as described further in this topic), but no single invocation supplies an input *text_length* that exceeds 256 (or 512) megabytes. Correct hashes are created when no single invocation of the callable services exceeds the described limit prior to (and after) application of the PTFs for OA43937.

Applications that wish to verify archived hash values created by pre-OA43937 HCR7770 and higher releases of ICSF callable services One-Way Hash Generate and PKCS11 One-Way Hash may need to invoke these callable services with new rule array keywords that support the creation of legacy hash values. The hash generated using the new rule array keywords must be used to verify the archived hash values.

The ICSF Callable Services One-Way Hash Generate and PKCS11 One-Way Hash, sign, or verify have corrected the way they create hash values when the length of the text on a single invocation of one of these services supplies an input *text_length* that equals or exceeds 256 megabytes (512 megabytes on z990/z890 or later hardware on HCR7770). The hashing services are corrected with the application of the PTFs for OA43937.

Table 98 on page 155 provides more details about this migration action. Use this information to plan your changes to the system.

Table 267. Information about this migration action

Element or feature:	Cryptographic Services.
When change was introduced:	PTFs for OA43937, which are applicable to: ICSF FMIDs HCR7770 - HCR77A1 (z/OS V1R12 - z/OS V2R1).
Applies to migration from:	ICSF FMIDs HCR7770 - HCR77A1, without the PTF for OA43937.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have archived hash values created before the installation of the PTFs for OA43937 which meet the length restrictions described here.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.

Migration actions from z/OS V1R13: Cryptographic Services

Table 267. Information about this migration action (continued)

System impacts:	If you do not use the legacy rule array keywords for affected applications, then the application may fail to verify the legacy hashes/signatures.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Identify if your application needs to verify archived hash values created by either of the ICSF callable service One-Way Hash Generate (CSNBOWH or CSNBOWH1 and CSNEOWH or CSNEOWH1) or PKCS11 One-Way Hash (CSFPOWH and CSFPOWH6) on releases pre-OA43937 at HCR7770 and higher. (See the ICSF Application Programmer's Guide documentation changes in this APAR for new ICSF callable service keywords that support the creation of hashes for the verification of archived hash values and the input text length requirements.)
2. If your application has these archived hash values and intends to verify them, then invocations of ICSF callable services One-Way Hash Generate, PKCS11 One-Way Hash, sign, or verify that create hashes for verification of the archived hash values may need to be updated to use the new legacy rule array keywords (ONLY if those archived hash values were created with input text length exceeding the limits described).

Reference information

For more information, see *z/OS Cryptographic Services ICSF Application Programmer's Guide* .

ICSF: Deprecated parameters in installation options data set Description

The ICSF installation options data set parameters COMPENC and PKDSCACHE were deprecated in FMID HCR7751 and parameters CKTAUTH, KEYAUTH, and TRACEENTRY were deprecated in FMID HCR77A1.

Table 99 on page 156 provides more details about this migration action. Use this information to plan your changes to the system.

Table 268. Information about this migration action

Element or feature:	Cryptographic Services.
When change was introduced:	ICSF FMIDs HCR7751 and HCR77A1.
Applies to migration from:	All ICSF FMIDs before FMID HCR77B0.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Migration actions from z/OS V1R13: Cryptographic Services

Steps to take

Edit the ICSF installation options data set and remove all of the deprecated parameters.

Note: ICSF starts with the deprecated parameters in the ICSF installation options data set, but the parameters are ignored and message CSFO0212 is issued for each deprecated parameter.

Reference information

For more information, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.

OCSF: Migrate the directory structure

Description

If you previously configured Open Cryptographic Services Facility (OCSF), you need to verify that the OCSF directories have been migrated to the target system. When your system is up and running, customize OCSF by running the customization script and then the IVP.

Note: If you want to take advantage of the Software Cryptographic Service Provider 2 (SWCSP2), you should bypass this migration action. When your system is up and running, install OCSF by running the install script and then the IVP.

Table 100 on page 157 provides more details about this migration action. Use this information to plan your changes to the system.

Table 269. Information about this migration action

Element or feature:	Cryptographic Services.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you currently use OCSF or if new products or functions on your new z/OS system require OCSF to be active. However, if you installed your new z/OS system with ServerPac or SystemPac, the OCSF installation script has been run and you do not have to perform this migration action for that system.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Migrate the OCSF /var directory structure to the target system. If you installed z/OS with CBPDO or by cloning an already-installed z/OS system, you can either copy the /var/ocsf directory from your old system or rerun the installation script. If you installed z/OS with ServerPac, the OCSF installation script has been run and you have no migration actions for that target system (although you still have to migrate the directory structure to any cloned systems, as already described).

Migration actions from z/OS V1R13: Cryptographic Services

If you installed z/OS V1R13 with CBPDO or by cloning an already-installed V1R13 system, you can either copy the /var/ocsf directory from your old system or rerun the installation script. If you installed z/OS V1R13 with ServerPac or SystemPac, the OCSF installation script has been run and you have no migration actions for that target system (although you still have to migrate the directory structure to any cloned systems, as already described).

If you copy /var/ocsf, verify that the OCSF /var directory structure has been migrated to the target system as described in “Migrate /etc and /var system control files” on page 16. The OCSF registry (the /var/ocsf files) contains the directory path names to the code libraries. If the registry files are copied, the CSSM DLL and the add-ins must be in the same location on the target system as on the prior release. The normal locations are /usr/lpp/ocsf/lib for the CSSM and supporting DLLs and /usr/lpp/ocsf/addins for the add-in libraries.

If you copied /var/ocsf, do the following:

1. Verify that the following four files exist in that directory:
 - CDSA_Registry.dir with permissions (-rw-r--r--)
 - CDSA_Registry.pag with permissions (-rw-r--r--)
 - CDSA_Sections.dir with permissions (-rw-r--r--)
 - CDSA_Sections.pag with permissions (-rw-r--r--)
2. Verify that the required RACF FACILITY class profiles are defined and set up:
 - CDS.CSSM — authorizes the daemon to call OCSF services
 - CDS.CSSM.CRYPTO — authorizes the daemon to call a cryptographic service provider (CSP)
 - CDS.CSSM.DATALIB — authorizes the daemon to call a data storage library (DL) service provider
3. Ensure that the necessary libraries are program controlled:
 - XL C/C++ runtime libraries
 - Language Environment libraries
 - SYS1.LINKLIB
 - SYS1.SIEALNKE

If you did not copy /var/ocsf, rerun the installation script:

1. Set up the RACF FACILITY class profiles required by OCSF and authorize the appropriate user IDs to those profiles:
 - CDS.CSSM — authorizes the daemon to call OCSF services
 - CDS.CSSM.CRYPTO — authorizes the daemon to call a cryptographic service provider (CSP)
 - CDS.CSSM.DATALIB — authorizes the daemon to call a data storage library (DL) service provider
2. Ensure that the following libraries are defined as program controlled:
 - XL C/C++ runtime libraries
 - Language Environment libraries
 - SYS1.LINKLIB
 - SYS1.SIEALNKE
3. Run the **ocsf_install_crypto** script from the OMVS shell. This must be run from the target system.
 - a. Verify and update \$LIBPATH.
 - b. Change directory to the location of the script (/usr/lpp/ocsf/bin).
 - c. Run the script.

Whether you reinstalled or migrated, it is strongly recommended that you rerun IVP **ocsf_baseivp** from the OMVS shell. This IVP verifies that OCSF is installed and configured correctly. To run the IVP:

1. Mount /usr/lpp/ocsf/ivp.
2. Read the README file and follow the instructions.
3. Run the IVP.

If you were using other IBM or non-IBM services to supplement the functions in OCSF, such as the Open Cryptographic Enhanced Plug-ins (OCEP) component of base element Integrated Security Services, or the

Migration actions from z/OS V1R13: Cryptographic Services

PKI Services component of base element Cryptographic Services, you must ensure that these are migrated or reinstalled.

Reference information

For more information, see *Integrated Security Services Open Cryptographic Enhanced Plug-ins Application Programming*.

System SSL: Ensure ICSF is available when running System SSL in FIPS 140-2 mode

Description

In z/OS V2R1, System SSL, when running in FIPS 140-2 mode, uses ICSF's random number generation and Diffie-Hellman support. Before running System SSL in FIPS 140-2 mode you must ensure that ICSF is running and that all user IDs that start SSL applications in FIPS 140-2 mode, invoke the gskkyman utility to manage FIPS 140-2 key database files, or invoke the GSKSRVR started task in FIPS mode have access to certain CSFSERV classes.

When it is running in non-FIPS mode, System SSL uses its own implementation of Diffie-Hellman and does not require ICSF. In non-FIPS 140-2 mode, however, System SSL attempts to use ICSF's random number generation as it would when running in FIPS 140-2 mode. If ICSF or the required resource is unavailable, System SSL uses its own random number generation capabilities as in earlier releases.

Table 270 provides more details about this migration action. Use this information to plan your changes to the system.

Table 270. Information about this migration action

Element or feature:	Cryptographic Services.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if your installation runs System SSL in FIPS mode.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None

Steps to take

To run System SSL in FIPS 140-2 mode, you must now make sure that ICSF is running and that all user IDs that start SSL applications in FIPS 140-2 mode, invoke the GSKSRVR started task in FIPS 140-2 mode, or invoke the gskkyman utility to manage FIPS 140-2 key database files can access the necessary ICSF callable services.

1. Make sure that ICSF is running. Assuming CSF is the name of the ICSF started task, you would enter:

```
DISPLAY A,CSF*
```

To display status about all started tasks, you would enter:

```
DISPLAY A,ALL
```

In z/OS V1R13, System SSL is providing capability to identify System SSL applications that are running in FIPS 140-2 mode, which are started before ICSF is available. Identification of these

Migration actions from z/OS V1R13: Cryptographic Services

applications is done by using the System SSL started task (GSKSRVR) and the z/OS tracking facility. This migration assistance support is delivered in APAR OA40816. See *Brief overview of APAR OA40816* for more information.

2. System SSL applications that are running in FIPS 140-2 mode, the GSKSRVR started task that is running in FIPS 140-2 mode, and the gskkyman utility (if managing FIPS 140-2 key database files) must be able to access ICSF's PKCS #11 pseudo-random function callable service for random number generation. In addition, applications and the gskkyman utility must access the following callable services to use ICSF's Diffie-Hellman capabilities:
 - PKCS #11 Token record create
 - PKCS #11 Derive key
 - PKCS #11 Generate key pair
 - PKCS #11 Generate secret key
 - PKCS #11 Get attribute value
 - PKCS #11 Token record delete

To ensure that RACF user IDs have access to the necessary services:

- a. Determine if the CSFSERV class is active. If active, this class restricts access to the ICSF programming interface. If it is not active, access to the ICSF programming interface (and the necessary callable services) is unrestricted. No configuration is necessary.
To determine which RACF classes are currently active, enter the SETROPTS command with the LIST parameter specified.`SETROPTS LIST`
- b. If the SETROPTS LIST command shows that the CSFSERV class is active, identify the profile or profiles that cover the following resources:
 - CSFRNG (which represents the PKCS #11 Pseudo-random function callable service)
 - CSF1TRC (which represents the PKCS #11 Token record create callable service)
 - CSF1DVK (which represents the PKCS #11 Derive key callable service)
 - CSF1GKP (which represents the PKCS #11 Generate key pair callable service)
 - CSF1GSK (which represents the PKCS #11 Generate secret key callable service)
 - CSF1GAV (which represents the PKCS #11 Get attribute value callable service)
 - CSF1TRD (which represents the PKCS #11 Token record delete callable service)

Each of these resources can be covered by a discrete profile or, if generic profile checking is activated, a generic profile. You can use the RLIST command to determine if a profile is defined to protect each resource. For example, to determine if a profile is defined to protect the CSFRNG resource, enter the following RLIST command: `RLIST CSFSERV CSFRNG`. When you enter this command, RACF lists information for the discrete profile CSFRNG. If there is no matching discrete profile, RACF lists the generic profile that most closely matches the resource name.

- c. If the RLIST command output reveals that there is a discrete or generic profile that covers the resource, examine the command output to ensure that all RACF user IDs that might start System SSL applications in FIPS 140-2 mode have at least READ access to the resource. If necessary, use the PERMIT command to give the appropriate users or groups access. For example, if a discrete profile CSFRNG exists, the following command would give the user JASMINE access:
`PERMIT CSFRNG CLASS(CSFSERV) ID(JASMINE) ACCESS(READ)`

If you do make changes, refresh the in-storage RACF profiles for the CSFSERV class: `SETROPTS RACLIST(CSFSERV) REFRESH`

Overview of APAR OA40816: In z/OS V1R13, System SSL is providing capability to identify System SSL applications that are running in FIPS 140-2 mode that have been started before ICSF was available. Identification of these applications is done by using the System SSL started task (GSKSRVR) and the z/OS tracking facility. See *z/OS MVS Planning: Operations* for more information about the z/OS tracking facility.

Migration actions from z/OS V1R13: Cryptographic Services

When the System SSL started task is enabled to write to the tracking facility, the started task will get notified of any SSL applications that are running in FIPS 140-2 mode before ICSF was available. The messages in the z/OS tracking facility can be monitored by issuing a **DISPLAY OPDATA,TRACKING** command to see which System SSL applications are running in FIPS 140-2 mode before ICSF being available. The following example shows output from the **DISPLAY OPDATA,TRACKING** command:

```
12.43.50          d o,tr
12.43.50          CNZ1001I 12.43.50 TRACKING DISPLAY 788
STATUS=ON        NUM=4      MAX=1000 MEM=n/a EXCL=0      REJECT=0
---- TRACKING INFORMATION----- -VALUE-- JOBNAME      PROGNAME+OFF-- ASID NUM
GSK01058I No ICSF for FIPS.          00 GSKSRVR      GSKSRVR      D9D6  48  1
GSK01059I SSLAPP1 no ICSF.           00 GSKSRVR      GSKSRVR      DAB0  48  5
GSK01059I SSLAPP2 no ICSF.           00 GSKSRVR      GSKSRVR      DAB0  48  2
GSK01059I SUIMGVD9 no ICSF.          00 GSKSRVR      GSKSRVR      DAB0  48  1
-----
```

From the tracking information in this example:

1. The GSK01058I message is the generic message that is written to the z/OS tracking facility once for the life of the System SSL started task. This message is issued the first time when either the System SSL started task or a System SSL application is running in FIPS 140-2 mode before ICSF being available.
2. The SSLAPP1 job was started or submitted 5 times
3. The SSLAPP2 job was started or submitted 2 times.
4. The SUIMGVD9 job was started or submitted just 1 time.

For more information about the support in APAR OA40816, see the documentation updates in OA40816.

Reference information

For more information, see the following references:

- For information about System SSL use of ICSF callable services, see *z/OS Cryptographic Services System SSL Programming*
- For information about the ICSF installation options file, see *z/OS Cryptographic Services ICSF System Programmer's Guide*
- For information about the ICSF CSFSERV resource class and the Installation Option Display panel, see *z/OS Cryptographic Services ICSF Administrator's Guide*.

System SSL: Modify automated scripts running the gskkyman utility to interact with new menus

Description

When you run the **gskkyman** program in interactive mode, a series of menus guide you through various tasks, prompting you for each piece of information required to complete the task. In z/OS V2R1 and later, some of the existing **gskkyman** menus have been refined to make the tasks simpler and more intuitive for the user to perform.

Although users should find the new **gskkyman** menus clearer and more straightforward, installations that have created automated scripts to interact with the **gskkyman** menus will need to modify these scripts to work with the new menus. Similarly, if you have created documentation that describes the **gskkyman** menus, the documentation will need to be updated to describe the new menus.

Table 271 provides more details about this migration action. Use this information to plan your changes to the system.

Table 271. Information about this migration action

Element or feature:	Cryptographic Services.
---------------------	-------------------------

Table 271. Information about this migration action (continued)

When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if your installation has automated scripts or documentation for the gskkyman menus.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None

Steps to take

If your installation has automated scripts or documentation based on the earlier **gskkyman** menus, be aware that the certificate creation, certificate request creation, and key parameters creation menus have been altered. You will need to modify any scripts that interact with these menus. Similarly, you will need to modify any documentation that describes these menus. The following topics in *z/OS Cryptographic Services System SSL Programming* describe the tasks that have changed because of the menu restructuring. If necessary, compare these topics against the same topics in the earlier version of the documentation.

- Creating a Self-Signed Server or Client Certificate
- Creating a Certificate Request
- Creating a Signed Certificate and Key
- Creating a Signed ECC Certificate and Key
- Creating a certificate to be used with a fixed Diffie-Hellman key exchange

Reference information

For information on the **gskkyman** program and the menus provided when this program is run in interactive mode, see *z/OS Cryptographic Services System SSL Programming*.

System SSL: Ensure all RACF user IDs that start SSL applications in non-FIPS mode can access the CSFRNG resource of the CSFSERV class

Description

Before z/OS V2.1, System SSL always used its own random number generation support available in software. As of z/OS V2R1, System SSL now exploits ICSF random number generation support if ICSF is available. In order to utilize ICSF when the random number generation service is protected by a RACF resource profile (CSFRNG), the userid under which the application is executing must have at least READ access to the resource profile. If the application is not FIPS enabled the processing is able to fall back to a software implementation and allow the application to continue (as a result, you might receive RACF unauthorized messages). If the application is FIPS enabled, it will fail.

If the user ID that starts the SSL application cannot access the CSFRNG resource of the CSFSERV class, System SSL will not be able to use the PKCS #11 Pseudo-random function callable service, and the informational message ICH408I (which indicates insufficient authorization) may be issued to the console. Although System SSL processing will continue, your application will be using System SSL's random number generation and will not be exploiting the random number generation capability provided by ICSF software or the Crypto Express3 Coprocessor card or the Crypto Express4 Coprocessor card.

Migration actions from z/OS V1R13: Cryptographic Services

Table 272 provides more details about this migration action. Use this information to plan your changes to the system.

Table 272. Information about this migration action

Element or feature:	Cryptographic Services.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the following conditions are true: <ul style="list-style-type: none">• Your installation uses ICSF.• The CSFSERV general resource class is active.• A profile covering the CSFRNG resource of the CSFSERV class is defined and does not grant READ access to all users.
Target system hardware requirements:	ICSF might use one of multiple techniques to derive the random content. For both FIPS certified random content and for non-FIPS certified random content, the availability of CCA and/or PKCS #11 coprocessors enables ICSF to derive the random content without imposing significant CPU overhead on the system. Either type of coprocessor can be exploited for non-FIPS certified content, but only a PKCS #11 coprocessor can be used to avoid CPU cycles for FIPS certified random content. Installations might want to plan for CCA and/or PKCS #11 coprocessor availability to avoid potentially excessive CPU cycles being exhausted on random number content generation.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	The system issues informational message ICH408I that indicates insufficient authorization might be issued to the console.
Related IBM Health Checker for z/OS check:	None

Steps to take

If your installation uses ICSF, you should ensure that any RACF user ID that will start SSL applications can access the CSFRNG callable service. This includes the SSL started task (GSKSRVR), and the **gskkyman** and **gsktrace** utilities.

1. Determine if the CSFSERV class is active. If active, this class restricts access to the ICSF programming interface. If it is not active, access to the ICSF programming interface (and specifically the CSFRNG callable service) is unrestricted. No configuration is necessary.

To determine which RACF classes are currently active, enter the SETROPTS command with the LIST parameter specified:

```
SETROPTS LIST
```

2. If the SETROPTS LIST command shows that the CSFSERV class is active, identify the profile that covers the CSFRNG resource. This could be a discrete profile named CSFRNG or, if generic profile checking is activated, a generic profile.

To determine if a profile has been defined to protect the CSFRNG resource, enter the following RLIST command:

Migration actions from z/OS V1R13: Cryptographic Services

```
RLIST CSFSERV CSFRNG
```

When you enter this command, RACF lists information for the discrete resource profile CSFRNG. If there is no matching discrete profile, RACF will list the generic profile that most closely matches the resource name.

3. If the RLIST command output revealed that there is a discrete or generic profile defined that covers the CSFRNG resource, examine the command output to ensure that all RACF user IDs that may start System SSL applications have at least READ access to the CSFRNG resource. If necessary, use the PERMIT command to give the appropriate users or groups access. For example, if a discrete profile CSFRNG exists, the following command would give user BAILEY access.

```
PERMIT CSFRNG CLASS(CSFSERV) ID(BAILEY) ACCESS(READ)
```

If you do make any changes, refresh the in-storage RACF profiles for the CSFSERV class:

```
SETROPTS RACLIST(CSFSERV) REFRESH
```

Reference information

For more information, see the following references:

- For more information about System SSL use of ICSF callable services, see *z/OS Cryptographic Services System SSL Programming*
- For more information on the ICSF installation options file, see *z/OS Cryptographic Services ICSF System Programmer's Guide*
- For more information about the ICSF CSFSERV resource class and the Installation Option Display panel, see *z/OS Cryptographic Services ICSF Administrator's Guide*.

System SSL: Modify code or System SSL application configurations to enable SSLV2 or SSLV3

Description

Starting in z/OS V2R2, z/OS System SSL has changed its default protocol support. When a System SSL application calls the `gsk_environment_open()` routine to establish a secure environment, SSL V2 and SSL V3 will now be disabled by default. TLS V1.0 will continue to be enabled by default. For applications that must continue to use these protocols, the protocol must be explicitly enabled.

If SSL V2, SSL V3, or both are the only supported protocols in the application, the following are example SSL errors that may occur when the SSL V2 or SSL V3 protocols are disabled:

- Return code 402: No SSL cipher specifications.
- Return code 412: SSL protocol or certificate type is not supported.
- Return code 429: SSL V2 header is not valid.

For applications that use the SSL V2 or SSL V3 protocol, evaluate the application's usage and change the application to use the TLS protocols if possible. TLS has addressed many security deficiencies in the prior SSL V2 and SSL V3 protocols.

Table 101 on page 159 provides more details about this migration action. Use this information to plan your changes to the system.

Table 273. Information about this migration action

Element or feature:	Cryptographic Services
When change was introduced:	z/OS V2R2. z/OS V2R1 and z/OS V1R13, both with APAR OA46489.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA46489.
Timing:	Before the first IPL of z/OS V2R2.

Migration actions from z/OS V1R13: Cryptographic Services

Table 273. Information about this migration action (continued)

Is the migration action required?	Yes, if System SSL applications for secure SSL/TLS connections are used.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If your installation utilizes System SSL applications for secure SSL/TLS connections, examine those applications to determine if they require either the SSL V2 or SSL V3 protocols to be enabled.

z/OS System SSL provides two methods for controlling the SSL/TLS protocols supported when negotiating a secure connection:

- The first method is the Application Programming Interface (API) **gsk_attribute_set_enum()** routine. This routine allows the enablement of the SSL/TLS protocols at either the SSL/TLS environment or connection level. To enable the usage of SSL V2, enumeration parameter GSK_PROTOCOL_SSLV2 must be set to GSK_PROTOCOL_SSLV2_ON. To enable the usage of SSL V3, enumeration parameter GSK_PROTOCOL_SSLV3 must be set to GSK_PROTOCOL_SSLV3_ON.
- The second method uses environment variables GSK_PROTOCOL_SSLV3 and GSK_PROTOCOL_SSLV2. To enable the usage of SSL V2, environment variable GSK_PROTOCOL_SSLV2 must be set to ON, 1, or ENABLED. To enable the usage of SSL V3, environment variable GSK_PROTOCOL_SSLV3 must be set to ON, 1, or ENABLED. Note that an environment variable setting is overridden if the application calls the **gsk_attribute_set_enum()** routine to set the GSK_PROTOCOL_SSLV2 and GSK_PROTOCOL_SSLV3 values.

If the protocols are required, consult each application configuration documentation to determine the appropriate enablement capability.

Reference information

For more information about System SSL, see *z/OS Cryptographic Services System SSL Programming*.

System SSL: Modify code or System SSL application configurations to enable null encryption, RSA-Export, or RC4 ciphers Description

Starting in z/OS V2R2, z/OS System SSL has changed its default SSL and TLS cipher support. The cipher defines the authentication, encryption, message authentication code (MAC), and key exchange algorithm used when negotiating a secure connection using SSL or TLS. When a System SSL application calls the **gsk_environment_open()** routine to establish a secure environment or the deprecated SSL or TLS **gsk_secure_soc_init()** routine specifying *cipher_specs* or *v3cipher_spec set* as NULL, the default enabled ciphers no longer includes the NULL encryption, RSA-EXPORT, or RC4 ciphers.

Migration actions from z/OS V1R13: Cryptographic Services

Table 274. SSL V3 and TLS ciphers

2 character cipher number	4 character cipher number	Short name	Description
00	0000	TLS_NULL_WITH_NULL_NULL	No encryption or message authentication and RSA key exchange.
01	0001	TLS_RSA_WITH_NULL_MD5	No encryption with MD5 message authentication and RSA key exchange.
02	0002	TLS_RSA_WITH_NULL_SHA	No encryption with SHA-1 message authentication and RSA key exchange.
03	0003	TLS_RSA_EXPORT_WITH_RC4_40_MD5 ¹	40-bit RC4 encryption with MD5 message authentication and RSA (export) key exchange.
04	0004	TLS_RSA_WITH_RC4_128_MD5	128-bit RC4 encryption with MD5 message authentication and RSA key exchange.
05	0005	TLS_RSA_WITH_RC4_128_SHA	128-bit RC4 encryption with SHA-1 message authentication and RSA key exchange.
06	0006	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 ¹	40-bit RC2 encryption with MD5 message authentication and RSA (export) key exchange.

¹ Ciphers are not supported for TLS V1.1 and TLS V1.2.

Table 275. SSL V2 ciphers

Cipher number	Description
1	128-bit RC4 encryption with MD5 message authentication.
2	128-bit RC4 export encryption with MD5 message authentication.

Notes:

1. The null encryption, RSA-EXPORT, and RC4 based ciphers are not supported when running in FIPS mode.
2. The SSL V2 and SSL V3 protocols are no longer being enabled by default. Therefore, the ciphers for those protocols do not have any meaning unless the protocol is explicitly enabled. See “System SSL: Modify code or System SSL application configurations to enable SSLV2 or SSLV3” on page 158 for more information about protocol defaults and enabling the protocols.

For the cipher values that are in the default cipher specification list along with their order, see the description of the **gsk_environment_open()** routine in *z/OS Cryptographic Services System SSL Programming*.

For applications that must continue to use these ciphers, the ciphers must be explicitly enabled.

If the ciphers in Table 102 on page 160 and Table 103 on page 160 are the only ciphers in common between the two secure connection endpoints, the following are example SSL errors that may occur when the ciphers are not explicitly enabled:

- Return code 402: No SSL cipher specifications.
- Return code -1: No SSL cipher specifications.

The full list of supported ciphers is available in *z/OS Cryptographic Services System SSL Programming*.

Table 104 on page 161 provides more details about this migration action. Use this information to plan your changes to the system.

Migration actions from z/OS V1R13: Cryptographic Services

Table 276. Information about this migration action

Element or feature:	Cryptographic Services
When change was introduced:	z/OS V2R2. z/OS V2R1 and z/OS V1R13, both with APAR OA47405.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA47405.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if System SSL applications for secure SSL/TLS connections are used.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	SSL and TLS secure connections may fail if a System SSL application is relying on one of the System SSL defined default ciphers and it is no longer enabled.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If your installation utilizes System SSL applications for secure SSL/TLS connections, examine those applications to determine if they require the usage of null encryption, RSA-EXPORT, or RC4 based ciphers.

If the System SSL application runs in FIPS mode, these ciphers are not supported and no migration action is needed.

For each System SSL application that requires the usage of one or more of these ciphers, consult each application's configuration documentation to determine the appropriate enablement capability. If the application supports the use of environment variables, see Method 2 in this section for environment variable information.

If your System SSL written application needs to support one or more of the removed ciphers, z/OS System SSL provides two methods to override the default SSL/TLS ciphers enabled when negotiating a secure connection using the SSL/TLS routines. Your application will need to utilize one of the following methods:

Method 1

Use the `gsk_attribute_set_buffer()` or `gsk_secure_soc_init()` routine:

`gsk_attribute_set_buffer()`

The `gsk_attribute_set_buffer()` routine supports the specification of SSL V2 and SSL V3/TLS ciphers in preference order through the `GSK_V2_CIPHER_SPECS`, `GSK_V3_CIPHER_SPECS`, and `GSK_V3_CIPHER_SPECS_EXPANDED` attributes. Each attribute buffer consists of a single character string consisting of the cipher values enabled to be used for the secure connection.

To re-enable one or more of the SSL V2 ciphers, specify the `GSK_V2_CIPHER_SPECS` attribute along with the complete list of ciphers to be available during the negotiation of the secure connection. For example, if you want to restore the V2 default cipher list, you need to set the buffer value to "713642" when the System SSL Security Level 3 FMID

Migration actions from z/OS V1R13: Cryptographic Services

(JCPT421) is installed. Otherwise, set the buffer to "642". Setting the value to "713642" when the System SSL Security Level 3 FMID (JCPT421) is not installed results in ciphers "713" being ignored.

To re-enable one or more of the SSL V3 ciphers, specify GSK_V3_CIPHER_SPECS if 2-character cipher specifications is enabled (this is the default), or GSK_V3_CIPHER_SPECS_EXPANDED if 4-character cipher specifications is enabled along with the complete list of ciphers to be available during the negotiation of the secure connection. For example, if you want to restore the SSL V3 2-character default cipher list, set the buffer value to "050435363738392F303132330A1613100D0915120F0C0306020100" when the System SSL Security Level 3 FMID (JCPT421) is installed. Otherwise, set the buffer to "0915120F0C0306020100". Setting the value to "050435363738392F303132330A1613100D0915120F0C0306020100" when the System SSL Security Level 3 FMID (JCPT421) is not installed results in ciphers "050435363738392F303132330A1613100D" being ignored. When using the 4-character cipher values, the buffer value is "0005000400350036003700380039002F0030003100320033000A001600130010000D000900150012000F000C00030006000200010000" when the System SSL Security Level 3 FMID (JCPT421) is installed. Otherwise, set the buffer to "000900150012000F000C00030006000200010000". Setting the value to "0005000400350036003700380039002F0030003100320033000A001600130010000D000900150012000F000C00030006000200010000" when the System SSL Security Level 3 FMID (JCPT421) is not installed results in ciphers "0005000400350036003700380039002F0030003100320033000A001600130010000D" being ignored.

gsk_secure_soc_init()

The **gsk_secure_soc_init()** routine (deprecated API) supports the specification of SSL V2 and SSL V3/TLS ciphers through the *cipher_specs* and *v3cipher_specs* fields in the *gsk_soc_init_data* structure.

To re-enable one or more of the SSL V2 ciphers, specify the complete list of ciphers to be available during the negotiation of the secure connection in the *cipher_specs* field. For example, if you want to restore the SSL V2 default cipher list, set the buffer value to "713642" when the System SSL Security Level 3 FMID (JCPT421) is installed. Otherwise, set the buffer to "642". Setting the value to "713642" when the System SSL Security Level 3 FMID (JCPT421) is not installed results in ciphers "713" being ignored.

To re-enable one or more of the SSL V3/TLS ciphers, specify the complete list of ciphers to be available during the negotiation of the secure connection in the *v3cipher_specs* field. For example, if you want to restore the SSL V3 2-character default cipher list, set the buffer value to "050435363738392F303132330A1613100D0915120F0C0306020100" when the System SSL Security Level 3 FMID (JCPT421) is installed. Otherwise, set the buffer to "0915120F0C0306020100". Setting the value to "050435363738392F303132330A1613100D0915120F0C0306020100" when the System SSL Security Level 3 FMID (JCPT421) is not installed results in ciphers "050435363738392F303132330A1613100D" being ignored.

Method 2

Use the environment variables GSK_V2_CIPHER_SPECS, GSK_V3_CIPHER_SPECS, and GSK_V3_CIPHER_SPECS_EXPANDED:

GSK_V2_CIPHER_SPECS

To re-enable one or more of the SSL V2 ciphers, specify the GSK_V2_CIPHER_SPECS attribute along with the complete list of ciphers to be available during the negotiation of the secure connection. See Method 1 in this section for cipher specification list examples.

GSK_V3_CIPHER_SPECS

To re-enable one or more of the SSL V3 ciphers, specify GSK_V3_CIPHER_SPECS if

Migration actions from z/OS V1R13: Cryptographic Services

2-character cipher specifications is enabled (this is the default) along with the complete list of ciphers to be available during the negotiation of the secure connection. See Method 1 in this section for cipher specification list examples.

GSK_V3_CIPHER_SPECS_EXPANDED

To re-enable one or more of the SSL V3 ciphers, specify GSK_V3_CIPHER_SPECS_EXPANDED if 4-character cipher specifications is enabled along with the complete list of ciphers to be available during the negotiation of the secure connection. See Method 1 in this section for cipher specification list examples.

Note: Applications that have specified the SSL V3 cipher specifications using the `gsk_attribute_set_buffer()` or `gsk_secure_soc_init()` routine override the respective environment variable settings.

Reference information

For more information about System SSL, see *z/OS Cryptographic Services System SSL Programming*.

Cryptographic Services actions to perform after the first IPL of z/OS V2R2

This topic describes Cryptographic Services migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

ICSF: Accommodate the TRACEENTRY option deprecation Description

Starting with ICSF HCR77A1, option TRACEENTRY has been deprecated and ICSF CTRACE support has been enhanced to support configurable ICSF CTRACE options from PARMLIB. A default CTICSF00 PARMLIB member is installed in SYS1.PARMLIB. The CTICSF00 PARMLIB member provides default component trace values for ICSF. By default, ICSF CTRACE support will trace with the KdsIO, CardIO, and SysCall filters using a 2M buffer. Configurable options are commented out within this PARMLIB member to provide examples of how to turn them on.

Table 105 on page 163 provides more details about this migration action. Use this information to plan your changes to the system.

Table 277. Information about this migration action

Element or feature:	Cryptographic Services
When change was introduced:	Cryptographic Support for z/OS V1R13 - z/OS V2R1 web deliverable (FMID HCR77A1), which installs only on z/OS V1R13 or z/OS V2R1.
Applies to migration from:	z/OS V2R1 and z/OS V1R13 without the Cryptographic Support for z/OS V1R13 - z/OS V2R1 web deliverable (FMID HCR77A1). Note that when the Cryptographic Support for z/OS V1R13 - z/OS V2R1 Web deliverable (FMID HCR77A1) is not installed, this migration item is not applicable.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have installed the Cryptographic Support for z/OS V1R13 - z/OS V2R1 web deliverable (FMID HCR77A1) to handle TKDS with PKDS #11 objects for the new format in HCR77A1.
Target system hardware requirements:	None.
Target system software requirements:	None.

Migration actions from z/OS V1R13: Cryptographic Services

Table 277. Information about this migration action (continued)

Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	If the TRACEENTRY option is specified it will be ignored and will produce message CSFO0212 at startup; processing continues.
Related IBM Health Checker for z/OS check:	None.

Steps to take

You can code the new CTRACE option within a BEGIN(HCR77A1) END option pair in a options data set shared between multiple releases of ICSF.

- If you share the installation options data set between HCR77A1 and pre-HCR77A1 systems, you can continue to supply the TRACEENTRY option at the lower-level systems as it is ignored, and processing will continue on the HCR77A1 systems.
- If your installation cannot tolerate the CSFO0212 message that is issued at startup, you need to use different installation option data sets. Note that new CTRACE options will be in effect:
 - Review the default CTRACE options to ensure that they are satisfactory for your system.
 - Make any necessary changes. Use the CTICSF00 PARMLIB to create customized ICSF CTRACE Configuration Data Sets in PARMLIB. You can use the new CTRACE option to specify the customized ICSF CTRACE Configuration Data Set in the ICSF Options Data Set.

For example, you can specify CTRACE(CTICSFxx), where xx is any two characters that were used when copying the default CTICSF00 parmlib member.

Component tracing is active when ICSF starts using the trace options defined in the CTICSFxx PARMLIB member, where 00 is the default. If the CTICSF00 PARMLIB member is incorrect or missing, ICSF CTRACE performs tracing using an internal default set of trace options. The operator can specify trace options individually on the TRACE CT command or specify the name of a CTICSFxx PARMLIB member containing the desired trace options. Using a PARMLIB member on the TRACE CT command can help minimize operator intervention and avoid syntax or keystroke errors

Reference information

For more information, see the following references:

- *z/OS Cryptographic Services ICSF Administrator's Guide*
- For information about TKDS, see *z/OS Cryptographic Services ICSF System Programmer's Guide*.
- For IBM Health Checker, see *IBM Health Checker for z/OS User's Guide*.

PKI Services: Migrate to IBM HTTP Server - Powered by Apache Description

Before z/OS V2R2, PKI Services used IBM HTTP Server powered by Domino. In z/OS V2R2, IBM HTTP Server - Powered by Apache replaces it as a base element of z/OS V2R2. You must now use the IBM HTTP Server - Powered by Apache.

Table 106 on page 165 provides more details about this migration action. Use this information to plan your changes to the system.

Table 278. Information about this migration action

Element or feature:	Cryptographic Services
When change was introduced:	z/OS V2R2.

Migration actions from z/OS V1R13: Cryptographic Services

Table 278. Information about this migration action (continued)

Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

This information assumes that you used the installer program (*bin/install_ihs*) to install IBM HTTP Server - Powered by Apache. You must know the installation directory for the server instance, which is referred to as *ihs-install-dir* in the sample commands. (This directory must be different from the product directory, usually */usr/lpp/ihsa_zos*).

Replace the references to *pki-install-dir* with the z/OS UNIX file system directory where z/OS PKI Services was installed. Usually, the directory is */usr/lpp/pkiserv/*.

The IBM HTTP Server installer program creates the *ihs-install-dir/conf/httpd.conf* configuration file that must be updated with directives provided in samples that are shipped by PKI Services and with information specific to your installation. The samples that are provided by PKI Services assume that the *conf/httpd.conf* contains directives that apply to each HTTP Server process, and that configuration directives for unsecure port, SSL server authentication port, and SSL client authentication port configuration are in separate configuration files that contain the `<VirtualHost>` directives that are then included in the *conf/httpd.conf* file. The port-specific configuration files are then included in the base *conf/httpd.conf* file. Follow the steps that follow to incorporate information from the PKI Services sample *httpd.conf* file into your *conf/httpd.conf* file, and to create and update the `VirtualHost` files specific to the PKI Services configuration.

Follow these steps:

1. Incorporate the directives from the PKI Services sample *httpd.conf* file (*pki-install-dir/samples/httpd.conf*) into the *ihs-install-dir/conf/httpd.conf* configuration file.
 - a. Locate the section of the *conf/httpd.conf* file that contains the `LoadModule` directives. Ensure that the following directives are specified and not commented out (a `#` in the first position of a line indicates that the line is a comment).
 - `LoadModule rewrite_module modules/mod_rewrite.so`
 - `LoadModule alias_module modules/mod_alias.so`
 - `LoadModule authnz_saf_module modules/mod_authnz_saf.so` (This `LoadModule` directive is located after the `# z/OS specific modules` comment.)
 - b. Locate the existing `AddType` directives in the *conf/httpd.conf* and add the `AddType` directives from the PKI Services sample *httpd.conf* file:
 - `AddType application/x-x509-user-cert.cer`
 - `AddType application/x-x509-ca-cert.der`
 - `AddType application/octet-stream.msi`
 - `AddType application/pkix-crl.crl`
 - c. Add the `Include` directives for the `VirtualHost` configuration files from the PKI Services sample *httpd.conf* file near the end of the *conf/httpd.conf* file:
 - `Include conf/vhost80.conf`

Migration actions from z/OS V1R13: Cryptographic Services

- Include conf/vhost443.conf
- Include conf/vhost1443.conf

Note: If you use different port numbers than 80, 443, and 1443, change the name of the files to match the port numbers that are used. For example, if you use port 1080 instead of 80 for the unsecure port, change the vhost80.conf file to vhost1080.conf. Also, make sure that the port number change is made within the vhost*.conf files. For example, change the <VirtualHost *:80> directive to <VirtualHost *:1080>.

2. Copy the sample VirtualHost configuration files from the PKI Services samples directory to the *ihs-install-dir/conf* directory. For example, if the *pki-install-dir* is /usr/lpp/pkiserv, and the *his-install-dir* is /etc/websrvissue the following command to copy the VirtualHost *:80 files:

```
cp /usr/lpp/pkiserv/samples/vhost*.conf /etc/websrv/conf
```

Note: To fully support the capabilities of PKI Services, the IBM HTTP Server powered by Domino required these instances to be running:

- An instance for non-secure and server authentication SSL connections, and
- an instance for client authentication SSL connections.

The IBM HTTP Server - Powered by Apache fully supports PKI Services capabilities in a single instance using VirtualHost configuration files for non-secure, server authentication SSL, and client authentication SSL connections.

3. Make the following updates to each of the VirtualHost configuration files using information from the httpd.conf files from the IBM HTTP Server powered by Domino (These are referred to as the old httpd.conf files). The sample VirtualHost configuration files that are shipped with PKI Services have directives that assume the use of the PKIServ and Customers domain names. If you use different or additional domain names, you must update or add additional directives to the vhost*.conf files.
 - a. Change all instances of <server-domain-name> to the fully qualified domain name of your web server. (This is in the Hostname directive value that is from the old httpd.conf files).
 - b. Change all instances of <application-root> to the *pki-install-dir* value. (/usr/lpp/pkiserv/ by default).
 - c. If you are not using the default location of /etc/pkiserv for the PKI Service configuration directory, update the SetEnv directive for _PKISERV_CONFIG_PATH with the value specified in the old httpd.conf files (as InheritEnv directives) or in the old httpd.envvars file. If additional _PKISERV_CONFIG_PATH_* environment variables are defined in your old httpd.conf or httpd.envvars files, add another SetEnv directive for each in the VirtualHost configuration files.
 - d. The ScriptAliasMatch directives replace the Exec directives from the old httpd.conf files. The sample vhost*.conf files provide ScriptAliasMatch directives for the PKIServ and Customers domain names. Change or add additional ScriptAliasMatch directives based on the Exec directives from the old httpd.conf file. (ScriptAliasMatch directives for public-cgi URLs are placed in the vhost80.conf file, ssl-cgi-bin URLs are placed in the vhost443.conf file, and clientauth-cgi-bin URLs are placed in the vhost1443.conf file).

Old httpd.conf file Exec directives:

```
Exec /PKIServ/public-cgi/* /usr/lpp/pkiserv/PKIServ/public-cgi/*
Exec /Customers/public-cgi/* /usr/lpp/pkiserv/PKIServ/public-cgi/*
```

Equivalent vhost80.conf file ScriptAliasMatch directive:

```
ScriptAliasMatch /(PKIServ|Customers)/public-cgi/(.*) /usr/lpp/pkiserv/PKIServ/public-cgi/$2
```

- e. The AliasMatch directives replace the Pass directives from the old httpd.conf files. The sample vhost*.conf files provide AliasMatch directives for the PKIServ and Customers domain names. Change or add additional AliasMatch directives based on the Pass directives from the old httpd.conf file. (AliasMatch directives for public-cgi URLs are placed in the vhost80.conf file, ssl-cgi-bin URLs are placed in the vhost443.conf file, and clientauth-cgi-bin URLs are placed in the vhost1443.conf file).

Old httpd.conf Pass directives:

Migration actions from z/OS V1R13: Cryptographic Services

```
Pass /PKIServ/cacerts/* /var/pkiserv/*
Pass /PKIServ/PKIXEnroll/* /usr/lpp/pkiserv/ActiveX/PKIXEnroll/*
Pass /PKIServ/PKICEnroll/* /usr/lpp/pkiserv/ActiveX/PKICEnroll/*
```

Equivalent vhost80.conf file AliasMatch directives:

```
AliasMatch /PKIServ/cacerts/(.*) /var/pkiserv/$1
AliasMatch /PKIServ/(PKIXEnroll|PKICEnroll)/(.*) /usr/lpp/pkiserv/ActiveX/$1/$2
```

- f. The Redirect directives from the old httpd.conf files are replaced with RewriteRule directives in the vhost*.conf files. If you are not using the PKIServ and Customers domain names or have additional domain names, you will need to change or create new RewriteRule directives. Also, if you are not using ports 80 and 443, the ports you are using for the non-secure and server authentication SSL must be added to the URL in the RewriteRule directives.

Old httpd.conf Redirect directive:

```
Redirect /PKIServ/ssl-cgi/* https://pokey.example.com/PKIServ/ssl-cgi-bin/*
Redirect /PKIServ/ssl-cgi/auth/* https://pokey.example.com/PKIServ/ssl-cgi-bin/auth/*
```

Equivalent RewriteRule directive:

```
RewriteRule ^/(PKIServ|Customers)/ssl-cgi/(.*)https://pokey.example.com/$1/ssl-cgi-bin/$2 [R,NE]
```

Note: This example is for redirecting from a non-secure URL to a server authentication SSL URL using the standard SSL port of 443. If a non-standard port is being used, the port number must be specified after the host name. For example, if port 4443 is used instead of 443, the URL starts with: `https://pokey.example.com:4443/PKIServ/...`

- g. The Directory and DirectoryMatch directives replace the Protect and Protection directives from the old httpd.conf files. The sample vhost*.conf files provide Directory and DirectoryMatch directives for the PKIServ and Customers domain names. Change or add additional Directory and DirectoryMatch directives based on the Protect and Protection directives from the old httpd.conf file. The surrogate user ID specified in the Directory/DirectoryMatch directives is PKISERV. If you use a different surrogate user ID, you must change PKISERV to the user ID specified in the old httpd.conf files.
 - h. The LocationMatch directives in the vhost*.conf files apply specific behavior to a specific URL for the PKIServ and Customers domain names. Change or add LocationMatch directives based on the domain names in the old httpd.conf files.
4. Update the vhost443.conf file to specify the keyfile value from the old httpd.conf file. (This assumes the IBM HTTP Server - Powered by Apache runs as the same USERID as the IBM HTTP Server powered by Domino.)

Old httpd.conf keyfile directive:

```
keyfile SSLring SAF
```

Equivalent keyfile directive:

```
Keyfile /saf SSLring
```

5. Take the following steps to update the vhost1443.conf file:
 - a. Update the keyfile value from the value that is specified in the old httpd.conf file. (This assumes the IBM HTTP Server - Powered by Apache runs as the same USERID as the IBM HTTP Server powered by Domino.)

Old httpd.conf keyfile directive:

```
keyfile SSLring SAF
```

Equivalent keyfile directive:

```
Keyfile /saf SSLring
```

- b. If you configured the IBM HTTP Server powered by Domino to perform revocation checking and want to continue to perform revocation checking in the IBM HTTP Server - Powered by Apache, add the following directive to the vhost1443.conf file after the SSLClientAuth directive:
 - SSLCRLHostName - Set the value from the old httpd.conf file SSLX500Host directive.
 - SSLCRLPort - Set the value from the old httpd.conf file SSLX500Port directive.
 - SSLCRLUserID - Set the value from the old httpd.conf file SSLX500UserID directive.
 - SSLStashfile - Set the value from the old httpd.conf file SSLX500Password directive.

Note: SSLStashfile is the fully qualified path to the file that contains the password for the user name on the LDAP server. This directive is not required for an anonymous bind. Use it when you specify a user ID. Use the `sslstash` command, which is in the `bin` directory of IBM HTTP Server, to create your CRL password stash file. Specify the password that you use to log in to your LDAP server as the password on the `sslstash` command. The format of the `sslstash` command is:

```
sslstash [-c] file function password
```

where:

-c Creates a new stash file. If not specified, an existing file is updated.

file

Is the fully qualified name of the file to create or update.

function

Indicates the function for which the password is to be used. Valid values include `crl` and `crypto`.

password

Is the password to stash.

Reference information

For more information, see the following references:

- *z/OS Cryptographic Services PKI Services Guide and Reference*
- WebSphere Application Server Knowledge Center (www.ibm.com/support/knowledgecenter/SSEQTP)

DFSMS migration actions

This topic describes migration actions for base element DFSMSdfp and optional features DFSMSdss, DFSMSHsm, DFSMSrmm, and DFSMSStvs.

DFSMS actions to perform before installing z/OS V2R2

This topic describes DFSMS migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

DFSMSdfp: Back up SMS control data sets

Description

In a multisystem Storage Management Subsystem (SMS) complex, operating systems share a common set of SMS classes, groups, ACS routines, and a configuration base, which make up the storage management policy for the complex. This storage management policy is maintained in a source control data set (SCDS). When this policy is activated for SMS, the bound policy is maintained in processor storage and on DASD in an active control data set (ACDS). Systems in the complex communicate SMS information through a common communications data set (COMMDS).

It is recommended that to successfully share SMS control data sets in a multisystem environment where there are mixed levels of DFSMS, you update, translate, validate, and activate SMS policies on the system with the latest level of DFSMS. When an earlier control data set is to be updated or activated, the control data set is formatted by the later-level system. The shared SMS control blocks reflect the new, rather than the previous, lengths and control information.

For fallback, IBM recommends restoring SMS control data sets from backups taken on the fallback release.

Migration actions from z/OS V1R13: DFSMS

Editing a policy on an earlier system could invalidate unused control information and prevent the control data set from being accessed by a later system. A warning message is provided before a policy can be changed on an earlier system. ACS routines may need to be updated and translated so to not reference policy items not known to the earlier system.

Remember, you risk policy activation failures if SCDS changes are not validated using the latest-level system in a sysplex.

Table 107 on page 169 provides more details about this migration action. Use this information to plan your changes to the system.

Table 279. Information about this migration action

Element or feature:	DFSMSdfp.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended to ensure data integrity.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	Install the PTFs in “Install coexistence and fallback PTFs” on page 6 if they are not already installed.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Do the following on your pre-z/OS V2R2 systems:

1. Back up SMS control data sets according to established procedures in the event that fallback is required. The control data set format is VSAM linear.
2. Install all coexistence PTFs in “Install coexistence and fallback PTFs” on page 6.

In addition, if you modified and activated a higher-level policy on a pre-z/OS V2R2 system, do the following to ensure that the ACDS can be accessed on z/OS V2R2 and that the SMS control block reflect the new lengths and control information:

1. On the pre-z/OS V2R2 system, save the active ACDS as an SCDS with the SETSMS SAVESCDS command.
2. On z/OS V2R2, update, translate, validate, and activate the saved SMS policy.

Reference information

For more information, see the following references:

- *z/OS DFSMS Implementing System-Managed Storage*
- *z/OS DFSMSdfp Storage Administration*

DFSMSdfp: Obtain descriptive text in messages for Open/Close/End of Volume ABENDs

Description

z/OS V1R13 DFSMSdfp introduced a new function that displays descriptive text for certain IECxxxx messages for OPEN, CLOSE, and end of volume determinant ABENDs. You can enable this function by specifying it in the MPFLSTxx PARMLIB member: .MSGOPTION VERBOSE(x), where x is either Y or N, with N as the default. If you were using OCE_ABEND_DESCRIP in DEVSUPxx to obtain this descriptive text before OA37505 was installed, you need to convert to using MPFLSTxx after OA37505 is installed.

Note: Beginning in z/OS V2R1, or after applying the PTF for APAR OA37505 in z/OS V1R13, the VERBOSE message is displayed only in the JOBLOG.

In addition, all OPEN, CLOSE and end-of-volume ABEND messages are issued using a Message Buffer Manager service, whether or not the new VERBOSE message function is enabled. One change this introduces is that the IECxxxx portion of the message always appears as a multi-line WTO message. Automated operation services that parse these messages may be affected.

Table 280 provides more details about this migration action. Use this information to plan your changes to the system.

Table 280. Information about this migration action

Element or feature:	DFSMSdfp
When change was introduced:	z/OS V2R1. z/OS V1R13 with PTF for APAR OA37505 applied.
Applies to migration from:	z/OS V1R13 without PTF for APAR OA37505 applied.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if any of these conditions are true: <ul style="list-style-type: none"> You have z/OS V1R13 without APAR OA37505 installed, and are using the OCE_ABEND_DESCRIP function in DEVSUPxx for verbose messages. If you have automation or programs that depend upon the type (single-line WTO as opposed to multi-line WTO) of the IECxxxx message for OPEN, CLOSE, end-of-Volume determinant ABENDs.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Remove OCE_ABEND_DESCRIP from DEVSUPxx parmlib member; otherwise you receive the following informational message at IPL time: IEA253I DEVSUP OCE_ABEND_DESCRIP NO LONGER HAS AFFECT. USE MPFLSTXX MEMBER
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you were using DEVSUPxx to obtain the ABEND descriptive text before OA37505 was installed, then you need to convert to using MPFLSTxx to obtain this information after OA37505 is installed. In the MPFLSTxx PARMLIB member, specify .MSGOPTION VERBOSE(Y) to enable display of the descriptive text.

Migration actions from z/OS V1R13: DFSMS

Because OPEN, CLOSE and end-of-volume ABEND messages now include the IECxxxx portion of the message as a multi-line WTO message, any automated operation services that parse these messages might need to be adjusted. Examine such automated operation services and adjust them to handle the new format as needed.

Here is an example of the output message you receive after you install APAR OA37505:

```
JOB00608 00000090 IEC141I 013-18,IGG0191B,IBMUSER9,S01,SYST1,5901,ZR1DT1, 651
651      00000090 SYS1.SAMPLIB(ZZZZZZZZ)
```

Reference information

For more information about using the VERBOSE option in MPFLSTxx, see *z/OS MVS Initialization and Tuning Reference*.

DFSMSdfp: Remove SMA fields from the SMS storage group construct IGDSGD and from ISMF panels

Description

Before z/OS V1R13, new SMS storage group constructs were created in DFSMS in support of the z/OSMF DASD Management task. Starting with z/OS V1R13, the DASD Management task has been removed from z/OSMF, and these fields (known as SMA attributes) will be removed from the storage group construct (IGDSGD). The fields have been removed from ISMF panels, Naviquest APIs, and DCOLLECT records.

Table 281 provides more details about this migration action. Use this information to plan your changes to the system.

Table 281. Information about this migration action

Element or feature:	DFSMSdfp
When change was introduced:	z/OS V1R13 with APAR PM40869 applied. See Software Announcement 211-252 (RFA56143).
Applies to migration from:	z/OS V1R13 without APAR PM40869 applied.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you parse the new attributes in DCOLLECT output or view/update them through NAVIQUEST. IBM might redefine these storage group and DCOLLECT fields in a future release.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Look for the following storage group attributes (known as SMA attributes) as defined by the IGDSGD macro.
 - SGDMANTH
 - SGDMASUG

- SGDMAMAX
 - SGDMAVSZ
 - SGDMAVTC
 - SGDMARSP
 - SGDMAVNM
2. Identify the following Navquest functions associated with the SMA attributes identified in step 1:
 - ACBQBAJ2: clist for Define/Alter/Display pool storage group
 - ACBQBAJG: clist for Pool Storage Group Display
 - ACBJBAJ2: Sample JCL for Pool Storage Group to define, alter, and display.
 3. Use the IDCDOU mapping macro to map the following DCOLLECT fields and remove the references to those fields:
 - DSGFSMA
 - DSGMANTH
 - DSGMASUG
 - DSGMAMAX
 - DSGMAVSZ
 - DSGMAVTC
 - DSGMARSP
 - DSGMAVNM

Reference information

For more information about the SMA attributes, see the following references:

- *z/OS DFSMS Using the New Functions*
- *z/OS DFSMSdfp Storage Administration*
- *z/OS DFSMS Access Method Services Commands*

DFSMSdss: Determine whether you need DISABLE(REFUCB) in parmlib member DEVSUPxx

Description

With z/OS V2R2, the automatic refresh UCB (REFUCB) function of the Device Manager is enabled by default. Previously, it was disabled by default. If you want the function to be disabled, you must explicitly disable it by using the statement `DISABLE(REFUCB)` in parmlib member `DEVSUPxx`.

ICKDSF `FLASHCPY`, `INIT`, and `REFORMAT` commands, and DFSMSdss full volume `COPY` and `RESTORE` functions, might update the volume serial and location of the volume table of contents (VTOC). This behavior can present a problem when the device is online to other systems. To address this problem, the automatic refresh UCB function (REFUCB) was introduced in z/OS V1R13, and is controlled by `DISABLE` | `ENABLE(REFUCB)` in parmlib member `DEVSUPxx`. `DISABLE(REFUCB)` was the default.

Table 108 on page 170 provides more details about this migration action. Use this information to plan your changes to the system.

Table 282. Information about this migration action

Element or feature:	DFSMSdss
When change was introduced:	z/OS V2R2
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.

Migration actions from z/OS V1R13: DFSMS

Table 282. Information about this migration action (continued)

Is the migration action required?	Yes, if you require the automatic refresh UCB function to be disabled. Note that the automatic refresh UCB function is only applicable to volumes that are shared with other systems in the same sysplex.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	For each system that has enabled the REFUCB function, an unconditional VARY ONLINE to the device is performed when the system is notified that the volume serial, the VTOC location, or both, has changed since the device was last varied online. This action updates fields in the UCB, including the volume serial (UCBVOLI) and the start location of the VTOC (UCBVTOC). If the VARY ONLINE,UNCOND fails for the device, or if the VARY ONLINE,UNCOND is not performed because the REFUCB function is not enabled on a system in the sysplex, the following write-to-operator (WTO) message is written to the system console: DM00063E dddd,volser,UCB NOT UPDATED REFUCB=[Y/N],USERS=xxxx.
Related IBM Health Checker for z/OS check:	Use check IBMDMO, DMO_REFUCB to determine whether the REFUCB function is disabled by the system. This check is provided as of z/OS V2R2. For more information, see <i>IBM Health Checker for z/OS User's Guide</i> .

Steps to take

If you determine that you need the automatic refresh UCB function to be disabled, review your current parmlib member DEVSUPxx. If DISABLE(REFUCB) is not present, add DISABLE(REFUCB). If ENABLE(REFUCB) is present, delete it.

Reference information

For information about enabling or disabling the automatic refresh UCB function, see the description of parmlib member DEVSUPxx in *z/OS MVS Initialization and Tuning Reference*.

DFSMSdfp: Prepare for the removal of TSO copy services commands Description

z/OS V2R2 is planned to be the last release to include a number of TSO/E-based System Data Mover (SDM) related commands. Except for the query commands (CQUERY, FCQUERY, RQUERY, XQUERY, XSTATUS), the ANTRQST API, and the XSET command, which will remain, IBM recommends that users migrate to the REXX versions of these commands.

Specifically, the following commands will no longer be supported in TSO:

- FCESTABL
- FCWITHDR
- CDELPAIR
- CDELPATH
- CESTPAIR
- CESTPATH
- CGROUP

- CRECOVER
- CSUSPEND
- RSESSION
- RVOLUME
- XADDPAIR
- XADVANCE
- XCOUPLE
- XDELPAIR
- XEND
- XRECOVER
- XSTART
- XSUSPEND

Table 109 on page 171 provides more details about this migration action. Use this information to plan your changes to the system.

Table 283. Information about this migration action

Element or feature:	DFSMSdfp
When change was introduced:	See IBM United States Software Announcement 215-267 "IBM z/OS Version 2 Release 2—Fueling the new digital enterprise," dated July 28, 2015.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use the TSO commands.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS checks:	None.

Steps to take

Convert existing non-query TSO commands to the REXX version using the programs provided in SYS1.DGTCLIB (ANTFREXX for FlashCopy, ANTPREXX for PPRC, ANTXREXX for XRC). Some of the command keywords are slightly different than the TSO version, and might need to be modified. For example, for full volume FlashCopy establish, you might enter the TSO command, as follows:

```
FCESTABL SDEVN(0F60) TDEVN(0F61)
```

To use the REXX interface, you can enter:

```
ANTFREXX FCESTABLISH SDEVN(0F60) TDEVN(0F61) SRCEXTNA() andTGTEXTNA()
```

Reference information

For more information about using the REXX commands, see *z/OS DFSMS Advanced Copy Services* .

DFSMSrmm: Prepare for the removal of the DFSMSrmm CIM provider

Description

z/OS V2R2 is planned to be the last release to support the DFSMSrmm Common Information Model (CIM) provider. The DFSMSrmm CIM provider uses the DFSMSrmm application programming interface (API) to retrieve information about DFSMSrmm resources in real time.

Migration actions from z/OS V1R13: DFSMS

IBM recommends that you remove the provider registration and its associated files from your system. If you need to retrieve information about DFSMSrmm resources, see “Steps to take” on page 173 for alternative methods.

Table 110 on page 172 provides more details about this migration action. Use this information to plan your changes to the system.

Table 284. Information about this migration action

Element or feature:	DFSMSrmm
When change was introduced:	See IBM United States Software Announcement 215-267 “IBM z/OS Version 2 Release 2—Fueling the new digital enterprise,” dated July 28, 2015.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you configured the DFSMSrmm CIM provider.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS checks:	None.

Steps to take

Follow these steps:

1. Determine whether the DFSMSrmm CIM provider is configured on your system. Check for the following conditions, which must be true if the DFSMSrmm CIM provider is active:
 - Determine whether Java Version 1.5.x is active on your system. This level is the maximum supported Java version for the DFSMSrmm CIM provider. You can use the following shell command: **java -version**
 - Determine whether the following files exist in z/OS UNIX System Services:
`/etc/rmm/rmmcust.properties`
`/var/rmm/rmm.properties`
or equivalent files exist in Linux, for example, in the `$RMM_DIR-` directory.
 - Determine whether the cimserver process is running under z/OS UNIX, or the CFZCIM started task procedure is running under z/OS.
 - Determine whether any DFSMSrmm providers are registered and running. You can use the following shell command: **cimprovider -l -s**
2. For any DFSMSrmm CIM providers that you find, unregister the providers. You can use the following shell command: **cimprovider -r -m module_name**
3. Remove the following files from z/OS UNIX or the equivalent files in Linux:
`/var/rmm/rmm.properties`
`/etc/rmm/rmmcust.properties`
`/etc/rmm/rmmlog.properties`

If you need to display information about DFSMSrmm resources in real time, you can use DFSMSrmm subcommands or panels. To obtain this information programmatically, for example, to create reports or implement automation, you can retrieve the output through:

- REXX variables

- Structured field introducers (SFIs) or XML, by using high-level language APIs or web services.

Reference information

For more information, see the following references:

- For information about the DFSMSrmm CIM provider, see *z/OS DFSMSrmm Implementation and Customization Guide*
- For information about the DFSMSrmm API, see *z/OS DFSMSrmm Application Programming Interface*

DFSMSdfp: Review the DCB block size specified in IDCAMS REPRO JCL Description

As of z/OS V2R1, the IDCAMS utility is enhanced to support the large block interface (LBI) for working with data sets having a block size larger than 32 K. As a result of this change, the system is now sensitive to any incorrect DCB parameters that might be coded in the IDCAMS REPRO command. Specifically, the IDCAMS utility now uses an extended DCB (DCBE), which allows a large block size to be passed to OPEN macro processing. The block size is verified during OPEN processing.

Before z/OS V2R1, the IDCAMS utility could not pass a large block size (more than 32 K) to OPEN processing through the DCB; the block size specification was ignored. Instead, OPEN processing obtained the block size from the data set VTOC entry.

Note: IBM 3390 storage devices do not support large block sizes (more than 32 K).

Table 285 provides more details about this migration action. Use this information to plan your changes to the system.

Table 285. Information about this migration action

Element or feature:	DFSMSdfp
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you have JCL or programs that issue the IDCAMS REPRO command for data sets having large block sizes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	If an incorrect block size is specified when the IDCAMS REPRO command runs, the system ends REPRO processing with condition code 12 (CC12) and error message IEC141I 013-68.
Related IBM Health Checker for z/OS checks:	None.

Steps to take

To detect potential errors, review the DCB block size value that is specified in the IDCAMS REPRO JCL to ensure that a valid block size is specified for the intended storage device. Or, that the block size value is set to zero, which causes OPEN processing to use the system determined block size by default.

Migration actions from z/OS V1R13: DFSMS

Reference information

For more information about the IDCAMS utility, see *z/OS DFSMS Access Method Services Commands* .

DFSMS actions to perform before the first IPL of z/OS V2R2

This topic describes DFSMS migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

DFSMSdfp: Ensure that the Language Environment runtime library is available for DLLs

Description

Language Environment provides common services and language-specific routines in a single runtime environment. You can use Language Environment to build and use dynamic link libraries (DLLs) for applications.

Table 111 on page 174 provides more details about this migration action. Use this information to plan your changes to the system.

Table 286. Information about this migration action

Element or feature:	DFSMSdfp.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if your installation builds or references DLLs.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If your installation builds or references DLLs, either you must set up the system link list to refer to the Language Environment runtime libraries (SCEERUN and SCEERUN2), or each job that creates or uses a DLL must include a STEPLIB DD statement referencing these libraries.

Reference information

For more information, see the following references:

- *z/OS V2R1.0 Language Environment Runtime Application Migration Guide*
- *z/OS Language Environment Customization*
- *z/OS Language Environment Programming Guide*

DFSMSdfp: Update SYS1.IMAGELIB

Description

If you use page mode printers such as the IBM 3800 or the IBM 3900 running in line mode (not page mode), you must install library character sets, graphic character modification modules, and character arrangement tables in SYS1.IMAGELIB. This migration action does not apply if you are using IBM 3900 printers that are driven by PSF.

Table 112 on page 174 provides more details about this migration action. Use this information to plan your changes to the system.

Table 287. Information about this migration action

Element or feature:	DFSMSdfp.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you are not using your old SYS1.IMAGELIB, you are installing with ServerPac or SystemPac, and you are using line mode printers such as the 3800 or 3900.
Target system hardware requirements:	IBM 3800 or 3900 printers.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Run the LCSBLD1 job from the samplib data set to create character sets, graphic character modification modules, and character arrangement tables in SYS1.IMAGELIB.
2. Copy customized or locally-written FCBs and UCS images from your old system's SYS1.IMAGELIB data set to the new system's SYS1.IMAGELIB data set.

Reference information

For information about maintaining SYS1.IMAGELIB, see *z/OS DFSMSdfp Advanced Services*.

DFSMSdfp: Accommodate changes in LISTCAT LEVEL output

Description

To be similar to ISPF, DFSMSdfp has enhanced the LISTCAT LEVEL output for the qualifier level specification as of z/OS V2R1. Prior to z/OS V2R1, the LISTCAT LEVEL command output would only include entries that had additional qualifiers after those specified. Additional qualifiers would include GDG data sets that were defined. Empty GDG base entries would not be included.

As of z/OS V2R1 (and matching ISPF), the command output provides the matches for:

- The specified qualifiers
- Any entries that had additional matching qualifier entries
- An alias entry of the specified value

Migration actions from z/OS V1R13: DFSMS

- Empty GDG base entries. (GDG data sets are included, as before.)

Table 288 provides more details about this migration action. Use this information to plan your changes to the system.

Table 288. Information about this migration action

Element or feature:	DFSMSdfp.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you are using LISTCAT LEVEL by specifying the GDG base name to detect that a GDG is empty (contains no GDSs).
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Although LISTCAT output is not a programming interface, review if this change will affect your system. An example of the output differences is shown. On pre-z/OS V2R1 systems:

```
LISTCAT LEVEL(A.B.C)
IDC3012I ENTRY A.B.C NOT FOUND
IDC3007I ** VSAM CATALOG RETURN-CODE IS 8
IDC1566I ** A.B.C NOT LISTED
...
IDC0001I FUNCTION COMPLETED, HIGHEST CONDITION CODE WAS 4
```

As of z/OS V2R1, the same command may produce:

```
LISTCAT LEVEL(A.B.C)
NONVSAM ----- A.B.C
          IN-CAT --- CATALOG.UCATA
...
IDC0001I FUNCTION COMPLETED, HIGHEST CONDITION CODE WAS 0
```

Notice that not only the information returned is different, but the return code and condition codes may be different as of z/OS V2R1. Take steps to convert any programs that rely upon LISTCAT output to use the Catalog Search Interface (CSI) instead. CSI is a supported general-use programming interface for the catalog, and will remove any dependency you have on future possible changes that may occur to LISTCAT output. Until such time as you can use the CSI interface, the following suggestions may be of help:

- Change invocations of LISTCAT LEVEL(A.B.C) to LISTCAT ENT(A.B.C.*) to return to the behavior prior to z/OS V2R1.
- Change invocations from PGM=IDCAMS to PGM=IDCNOGFL.

Reference information

For more information, see the following references:

- For the LISTCAT command, see *z/OS DFSMS Access Method Services Commands* .

- For information on the Catalog Search Interface, see *z/OS DFSMS Managing Catalogs*. Information APAR II14670 also provides a description of this change.
- For information on previous LISTCAT changes, see informational APAR II14250.

DFSMSdfp: Do not use IEBCOPYO

Description

In z/OS V1R13, the IEBCOPY utility was enhanced, and one of the enhancements was that the utility was no longer APF-authorized. For users who needed to fallback from the new IEBCOPY to the previous APF-authorized form, IEBCOPY was retained in z/OS V1R13 under the name IEBCOPYO. The IEBDSCPYPY alias name for IEBCOPY was also revised to apply to IEBCOPYO for z/OS V1R13.

In z/OS V2R1, the IEBCOPYO form of the utility was eliminated and the IEBDSCPYPY alias now applies to the standard non-APF-authorized form of IEBCOPY.

Table 289 provides more details about this migration action. Use this information to plan your changes to the system.

Table 289. Information about this migration action

Element or feature:	DFSMSdfp.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you used IEBCOPYO directly or through the alias IEBDSCPYPY.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Any programs or jobs that called IEBCOPYO in z/OS V1R13 must be changed to call IEBCOPY in V2R2. It is not expected that you used IEBCOPYO on z/OS V1R13, unless you had a problem with the z/OS V1R13 level of IEBCOPY and had to fall back to the z/OS V1R12 level of IEBCOPY.
- Any programs or jobs that call the IEBDSCPYPY alias name in z/OS V2R2 will invoke the non-APF-authorized IEBCOPY. Make any appropriate changes if this affects your programs or jobs.

Reference information

For more information about the IEBCOPY utility, see *z/OS DFSMSdfp Utilities*.

DFSMSdfp: Examine and update program calls to IEBCOPY

Description

Before z/OS V2R1, the IEBCOPY utility assumed that calls from programs (not from JCL) that passed three parameters, had the high order bit set on in the third word of the parameter list. Starting in z/OS

Migration actions from z/OS V1R13: DFSMS

V2R1, IEBCOPY requires the high order bit to be on in the third word of a parameter list; if that bit is not on, IEBCOPY causes a failure. This change can affect your programs that call IEBCOPY, requiring you to update them if needed.

Table 290 provides more details about this migration action. Use this information to plan your changes to the system.

Table 290. Information about this migration action

Element or feature:	DFSMSdfp.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have programs that pass a parameter list of exactly three words to IEBCOPY and do not set on the high order bit in the last word.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Examine calls from programs (not from JCL) to IEBCOPY, to see whether any pass three parameters without turning on the high order bit in the last word. If you have such programs, revise them to turn on the high order bit of the last word of the parameter list. If you are using the CALL, LINK or ATTACH macro, the simplest way to do this is to add the VL parameter to CALL or VL=1 parameter to LINK or ATTACH.

Reference information

For more information about program calls to IEBCOPY, see *z/OS DFSMSdfp Utilities*.

DFSMSdfp: Specify new option to suppress the message IGD17054I

Description

In z/OS V1R13, issuance of the IGD17054I message was controlled by the value specified for the SUPPRESS_DRMSGS parameter, which was new in z/OS V1R13, in the IGDSMSxx parmlib member. Beginning in z/OS V2R1, issuance of the IGD17054I message is controlled by the new SUPPRESS_SMSMSG parameter, also in the IGDSMSxx parmlib member. Issuance of all other DELETE/RENAME messages are controlled as before by the SUPPRESS_DRMSGS parameter.

Table 291 provides more details about this migration action. Use this information to plan your changes to the system.

Table 291. Information about this migration action

Element or feature:	DFSMSdfp
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.

Table 291. Information about this migration action (continued)

Is the migration action required?	Yes, if you specify the SUPPRESS_DRMSGS(YES) parameter in IGDSMSxx parmlib member to suppress the IGD17054I message and continue to suppress the message IGD17054I.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you specify the SUPPRESS_DRMSGS(YES) parameter in an IGDSMSxx parmlib member to suppress the IGD17054I message, you need additionally to specify the SUPPRESS_SMSMSG(YES,IGD17054I) parameter in your IGDSMSxx parmlib member. This enables the message suppression from consoles and all logs, including the job log and the hardcopy log. Without this action, you are unable to suppress the message IGD17054I by default regardless of what is specified for SUPPRESS_DRMSG.

Tip: If you currently suppress the message IGD17054I by coding any message processing exit routines or specifying the MPFLSTxx parmlib option in prior versions of z/OS, you are now able to make use of the new parameter SUPPRESS_SMSMSG(YES,IGD17054I) alternatively.

Reference information

For more information, see *z/OS MVS Initialization and Tuning Reference*.

DFSMSdfp: Adjust parameters to control whether offline device discovery is performed

Description

Beginning in APAR OA43706 (PTFs: UA74649 for z/OS V2R1 and UA74648 for z/OS V1R13), the System Data Mover (ANTAS000 address space) is changed to conditionally invoke offline device discovery during IPL. Prior to this APAR, offline device discovery was always performed.

APAR OA43706 introduced a new keyword called OfflineDiscovery to the ANTXIN00 parmlib member to allow you to control whether offline device discovery is performed during IPL when ANTAS000 first starts up, and thereafter when ANTAS000 restarts following a CANCEL. A value of YES causes offline discovery to take place. A value of NO bypasses offline device discovery. If OfflineDiscovery is not specified, the default is OfflineDiscovery(NO).

Tip: The Offline Device Discovery was introduced by APAR OA36570 (PTFs for z/OS V1R12 and V1R13) and incorporated into z/OS V2R1 to reduce the XSTART time following an IPL.

SYSLOG messages example:

```
ANTB8000I XRC INITIALIZATION STARTED
ANTB8002I OFFLINE DEVICE DISCOVERY COMPLETE; RC=0 REAS=606
ANTB8001I XRC INITIALIZATION COMPLETED
```

Table 113 on page 175 provides more details about this migration action. Use this information to plan your changes to the system.

Migration actions from z/OS V1R13: DFSMS

Table 292. Information about this migration action

Element or feature:	DFSMSdftp.
When change was introduced:	z/OS V2R1 and z/OS V1R13, both with APAR OA43706 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA43706 applied.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you need offline device discovery to be performed during IPL.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	See “Steps to take” on page 176 for specific configuration considerations.
Related IBM Health Checker for z/OS check:	None.

Steps to take

You should only need to perform offline device discovery during IPL (that is, specify OfflineDiscovery(YES) in ANTXIN00) if you are using one of the following:

- GDPS MzGM (aka XRC) in HYPER-PPRC mode (Incremental Resynch)
- GDPS MzGM under z/OS with XRC Offline Primary devices

Other XRC configurations or non-XRC environments will not directly benefit from having offline discovery performed at IPL. Therefore, if it is not required, do not specify the keyword and avoid discovery, which may reduce overall IPL elapsed time.

Tip: The value of OfflineDiscovery takes effect when the ANTAS000 address space is started during IPL, or with the automatic restart of ANTAS000 after it has been cancelled. To activate a new value for OfflineDiscovery without an IPL, do the following:

1. Update the value in PARMLIB member ANTXIN00
2. Issue the system command CANCEL ANTAS000

The OfflineDiscovery keyword is ignored and will not be processed if it is specified in the ALL or session member of hlq.XCOPY.PARMLIB.

Reference information

For more information, see *z/OS DFSMS Advanced Copy Services* .

DFSMSdftp: Define a security profile for VSAM exception exits

Description

VSAM users can specify an exit to receive control for physical I/O errors that might occur against a VSAM data set, through either of the following methods:

- EXCEPTIONEXIT keyword of the IDCAMS define function
- SYNAD= sub-parameter of the AMP= keyword of the DDNAME JCL statement.

Migration actions from z/OS V1R13: DFSMS

As of APAR OA46090, the exit name that can be specified on these keywords is controlled through a FACILITY class profile. The FACILITY class profile is named IDA.VSAMEXIT.*exitname* where *exitname* identifies the exit to be invoked.

You must ensure that the exit name is protected through a FACILITY class profile, and that callers of the exit have at least READ authority.

Table 114 on page 176 provides more details about this migration action. Use this information to plan your changes to the system.

Table 293. Information about this migration action

Element or feature:	DFSMSdftp.
When change was introduced:	z/OS V2R1 and z/OS V1R13, both with APAR OA46090 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA46090 applied.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if your installation has VSAM exception exits that are specified through the AMP or EXCEPTIONEXIT parameters.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	If you have programs that specify VSAM exception exits in this manner and you do not take the necessary migration action, the programs will encounter the following open errors: <ul style="list-style-type: none">• Non-authorized exits specified in the EXCEPTIONEXIT parm: IEC161I 40(1)-53• Non-authorized exits specified in the SYNAD parm: IEC161I 40(2)-81
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Define a FACILITY class profile with the resource name IDA.VSAMEXIT.*exitname*, where *exitname* is the EXCEPTIONEXIT or SYNAD parameter value.
- Ensure that callers of the exit have at least READ authority to the FACILITY class resource name.

Use caution if you choose to use a generic RACF profile to ensure that you do not allow unintended modules to be used as VSAM exception exits.

Note: This action must be taken even if the exits do not actually exist, unless you choose to remove the EXCEPTIONEXIT or SYNAD parameter.

Reference information

For more information, see *z/OS DFSMS Using Data Sets* .

Migration actions from z/OS V1R13: DFSMS

DFSMSdfp: Accommodate change for data set name prefix in IDCAMS ALLOCATE Description

With IDCAMS APAR OA42679 and TSO/E APAR OA43330 applied, the **IDCAMS ALLOCATE** command is changed in the way that it starts TSO/E to allocate a data set. IDCAMS processing now uses the TSO/E Service Facility (TSF) to allocate a data set, rather than running the **ALLOCATE** command under the TSO/E terminal monitor program (IKJEFT01). With this change, the user ID assigned to the IDCAMS batch job is treated as the default data set prefix. That is, the user ID for the IDCAMS batch job is appended to the data set name as a high-level qualifier, if you specify the data set name on the DATASET keyword without quotation marks and the user ID does not have a RACF TSO segment.

Previously, the **IDCAMS ALLOCATE** command used a null prefix for the allocated data set, if you specified the data set name on the DATASET keyword without quotation marks and the user ID did not have a RACF TSO segment.

Assume, for example, that the user ID *ZZZZZZZ* is defined in both UADS and in RACF without a TSO segment; note the following differences in behavior:

- Before this change, TSO runs under the UADS user. If the data set name is specified without quotation marks on the DATASET keyword, and the user has a UADS PROFILE PREFIX(*prefix*), the prefix is used as the data set prefix. Otherwise, the user ID is used as the data set prefix.
- After this change, the user ID is always used as the data set prefix. Therefore, if the user ID and UADS PROFILE PREFIX(*prefix*) are different, the high-level qualifier for the data set is changed.

Table 115 on page 178 provides more details about this migration action. Use this information to plan your changes to the system.

Table 294. Information about this migration action

Element or feature:	DFSMSdfp
When change was introduced:	z/OS V2R1 and z/OS V1R13, both with APARs OA42679 (DFSMS) and OA43330 (TSO/E) applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APARs OA42679 (DFSMS) and OA43330 (TSO/E).
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use IDCAMS ALLOCATE , do not specify the data set name in quotation marks on the DATASET keyword, and the user ID assigned to the IDCAMS batch job does not have a RACF TSO segment.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Failure to include the data set name in quotation marks can result in allocation errors.
Related IBM Health Checker for z/OS checks:	None.

Steps to take

Check for JCL and programs that use the **IDCAMS ALLOCATE** command. Ensure that the data set name is specified in quotation marks on the DATASET keyword. Doing so ensures that the user ID is not appended to the data set name as a high-level qualifier.

When the **IDCAMS ALLOCATE** command is run by a user with a RACF TSO segment defined, no change is required.

Reference information

Documentation APAR OA47508 describes these changes. For more information about the IDCAMS utility, see *z/OS DFSMS Access Method Services Commands* .

DFSMSdfp: Accommodate new authorization requirements for users of the IDCAMS DEFINE command

Description

IDCAMS APAR OA47269 introduces changes to the RACF authorization checking of data set aliases, VSAM cluster paths, and alternate indexes (AIXs). As a result of this change, users of the **IDCAMS DEFINE** command might require additional security authorizations for defining these objects.

In previous releases:

- For a **DEFINE ALIAS** request, if the alias was for a generation data set or a non-VSAM data set, the generation data set name or the non-VSAM data set name was used for RACF authorization checking
- For a **DEFINE ALTERNATEINDEX** or **DEFINE PATH** request, the associated cluster name was used for RACF authorization checking.

With IDCAMS APAR OA47269 applied, the user of the **IDCAMS DEFINE** command requires SAF ALTER authority:

- To the target data set when defining an alias for the data set. This requirement is added to the existing requirement that users have SAF UPDATE authority to the catalog that is to contain the alias, if the associated data set is non-SMS-managed. If the associated data set is SMS-managed, no SAF authority is required.
- To the VSAM cluster, when defining a VSAM path or alternate index name (AIX) for the cluster. This requirement is added to the existing requirement that users have SAF UPDATE authority to the catalog, if the related cluster is not SMS-managed.

Table 116 on page 179 summarizes the changes to authorization requirements for defining data set aliases, VSAM cluster paths, and alternate indexes.

Table 295. Required security authorization for data set aliases, VSAM cluster paths, and alternate indexes

IDCAMS command	Function performed	Authorization that is required for the related data set or cluster (without APAR OA47269 applied)	Authorization that is required for the related data set or cluster (with APAR OA47269 applied)
DEFINE ALIAS	Defines an alternate name for a non-VSAM data set or a user catalog.	NONE	ALTER See Note 1.
DEFINE PATH	Defines a path directly over a base cluster or over an alternate index and its related base cluster.	NONE	ALTER See Note 2.
DEFINE ALTERNATEINDEX	Defines an alternate index.	NONE	ALTER See Note 2.

Notes:

Migration actions from z/OS V1R13: DFSMS

1. The user requires ALTER authority to the alias name, unless the user has READ authority to resource name STGADMIN.IGG.CATALOG.SECURITY.CHANGE. If so, the user does not require authorization to the data set name.
2. The user requires ALTER authority to the entry name, unless the user has READ authority to resource name STGADMIN.IGG.CATALOG.SECURITY.CHANGE. If so, the user requires ALTER authority to the cluster name.

Table 117 on page 180 provides more details about this migration action. Use this information to plan your changes to the system.

Table 296. Information about this migration action

Element or feature:	DFSMSdfp.
When change was introduced:	z/OS V2R1 and z/OS V1R13, both with APAR OA47269 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA47269 applied.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if your installation has data sets with aliases, paths, or alternate indexes (AIXs) that are not covered by existing security profiles.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	If you do define the required security profiles, authorization errors might occur, due to insufficient authority.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Review the security profiles for data sets that use aliases, paths, and alternate indexes. For any alias, path, or alternate index (AIX) that is not covered by an existing security profile, add or change security profiles for alias, path, or AIX to grant the appropriate authority.
Depending on your installation's naming conventions, you might find that your existing security profiles do not require any changes. For example, if the user ID of the user is the data set high-level qualifier.
- If your installation cannot immediately tolerate the change in authorization checking, you can reinstate the previous method of authorization checking by doing the following:
 - Defining a FACILITY class profile with the resource name of STGADMIN.IGG.CATALOG.SECURITY.CHANGE
 - Ensuring that users have at least READ authority to the FACILITY class resource name.

Reference information

For more information about creating authorizations for IDCAMS commands, see *z/OS DFSMS Access Method Services Commands*.

DFSMSdss: Review changes to the messages that result from a COPY or RESTORE operation with COPYVOLID

Description

With APAR OA36296 on z/OS V1R13, DFSMSdss uses the IEEVARYD service, rather than the VARY command, to vary the target volume offline during a COPY or RESTORE operation with either FULL or TRACKS and the COPYVOLID parameter, when the target volume becomes a duplicate of the source volume. As a result, the hardcopy log no longer contains:

- VARY device-number,OFFLINE DFSMSDSS INTERNAL VARY
- IEF281I device-number NOW OFFLINE.

Instead, the hardcopy log contains message IEF880I, as follows:

```
IEF880I device-number NOW OFFLINE BY ADRSBRTN
```

Programs or procedures that rely on the presence of either the VARY command or the IEF281I message in the hardcopy log or job logs should be updated.

Table 297 provides more details about this migration action. Use this information to plan your changes to the system.

Table 297. Information about this migration action

Element or feature:	DFSMSdss
When change was introduced:	z/OS V1R13 with APAR OA36296 applied.
Applies to migration from:	z/OS V1R13 without APAR OA36296 applied.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have programs or procedures that rely on the presence of either the VARY command or the IEF281I message.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Modify your programs or procedures to check for the following message, which in z/OS V2R2 is no longer a command response:

```
IEF880I device-number NOW OFFLINE BY ADRSBRTN
```

This message indicates that the device has been varied offline as the result of a DFSMSdss operation with the COPYVOLID parameter.

Reference information

For more information about COPY and RESTORE, see *z/OS DFSMSdfp Storage Administration*.

Migration actions from z/OS V1R13: DFSMS

DFSMSdss: Build the IPLable stand-alone DFSMSdss image

Description

Starting with z/OS V1R12, DFSMSdss uses BSAM instead of EXCP to read from and write to DFSMSdss dump data sets during DUMP, COPYDUMP, and RESTORE operations. As a result, if you plan to use DFSMSdss Stand-Alone Services, you must rebuild the IPL-capable core image for the Stand-Alone Services program.

Table 118 on page 181 provides more details about this migration action. Use this information to plan your changes to the system.

Table 298. Information about this migration action

Element or feature:	DFSMSdss.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you want to use DFSMSdss Stand-Alone Services.
Target system hardware requirements:	Stand-Alone Services supports the IBM 3494 TotalStorage Enterprise Automated Tape Library, the IBM 3495 TotalStorage Enterprise Automated Tape Library, and the IBM 3590 TotalStorage Enterprise Tape Subsystem.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	Stand-Alone Services does not support the creation of the core image on an SMS-managed volume.
System impacts:	If this migration action is not performed, users of DFSMSdss standalone restore cannot restore to tape any backups that were created with greater than 65520-byte blocks. The operation fails with the message ADRY3530I SEQUENCE ERROR ON RESTORE TAPE. Backups created with 65520 byte blocks can be restored as before.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Use the DFSMSdss command BUILD_SA to create a Stand-Alone Services IP-capable core image. On the command, you can specify:
 - Device from which Stand-Alone Services are to be IPLed (such as a card reader, tape drive, or DASD volume)
 - Operator console to be used for Stand-Alone ServicesThe BUILD_SA command builds the IPLable core image on the current operating system and determines a record size, based on whether the IPL is performed from a card, tape, or DASD.
2. Use your security management product, such as RACF, to protect the SYS1.ADR.SAIPLD.Vvolser data set and the Stand-Alone Services modules.
3. If you have not already done so, create a backup copy of your system that can be restored by this function. For information about backing up volumes, see *z/OS DFSMSdss Storage Administration*.

Notes:

1. To ensure that Stand-Alone Services is available when you run from DASD, do not delete the SYS1.ADR.SAIPLD.Vvolser data set or move it to another volume.
2. If you IPL from DASD and later change the volume serial number, you must rerun the BUILDSDA function to create a new core image data set with the new volume serial number in the name.
3. If you attempt to use the DFSMSdss stand-alone restore program from z/OS V1R11 to restore a backup that was created with a block size greater than 65520 bytes, the operation fails with the message ADRY3530I SEQUENCE ERROR ON RESTORE TAPE.

Reference information

For more information, see *z/OS DFSMSdss Storage Administration*.

DFSMSdss: Accommodate ADREID0 EIREC14 expansion

Description

With APAR OA42238, the length of the EIREC14 structure in the ADREID0 macro is increased by 16 bytes. This expansion, which is related to DFSMSdss support for dump data sets compressed with zEDC services, may require changes for applications that invoke DFSMSdss using its application programming interface.

Table 119 on page 182 provides more details about this migration action. Use this information to plan your changes to the system.

Table 299. Information about this migration action

Element or feature:	DFSMSdss
When change was introduced:	z/OS V2R1 and z/OS V1R13, both with APAR OA42238 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA42238 applied.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use the DFSMSdss application programming interface.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Check for use of the Function Ending user interaction module exit option (EIOPTION14) in applications that exploit the DFSMSdss application programming interface. If EIOPTION14 is used, determine if the UIM copies the structure pointed to by EIRECPTR. In this exit the structure pointed to by EIRECPTR is named EIREC14. If the application copies the area of storage pointed to by EIRECPTR, then action may be required.

If the application copies the area of storage using EIRECLEN for the amount of data to copy, then the application must ensure the area that is the destination of the copy is large enough to accommodate the larger EIREC14 structure.

Migration actions from z/OS V1R13: DFSMS

The length of the EIREC14 structure is not provided in the ADREID0 data area. Prior to the application of the PTFs for OA42238, determine the length of the EIREC14 structure with an equate of this form:

```
EQU EI14CPUT+L'EI14CPUT-EIREC14
```

After the application of the PTFs for OA42238, determine the length of the EIREC14 structure with an equate of this form:

```
EQU EI14ZCSV+L'EI14ZCSV+15-EIREC14
```

Reference information

For more information about the application programming interface and Eioption 14, see *z/OS DFSMSdss Storage Administration*.

DFSMSHsm: Update applications that depend on LIST command output Description

Beginning in z/OS V2R2, the output of the **LIST DUMPCLASS** command includes a new MINSTACK value, and the position of the existing STACK value in the output has changed. This new and changed output is displayed when OUTDATASET, SYSOUT (the default), or TERMINAL is specified as the destination for the output.

Beginning in z/OS V2R1, the output of the **LIST DUMPCLASS** command includes the value of the RECOVERRESET parameter. RECOVERRESET specifies whether the data-set-changed indicator in the VTOC entry is reset for all data sets that are restored during full volume recover processing.

Table 300 provides more details about this migration action. Use this information to plan your changes to the system.

Table 300. Information about this migration action

Element or feature:	DFSMSHsm
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if your application depends on the output of the LIST DUMPCLASS command.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Update applications that depend on the output of the **LIST DUMPCLASS** command to accommodate the following:

- RECOVERRESET value
- MINSTACK field with a output target of TERM, OUTDATASET, or SYSOUT.

Also, remove any dependency on the STACK field location in the **LIST DUMPCLASS** command with a output target of TERM, OUTDATASET, or SYSOUT.

Reference information

For information about the **LIST DUMPCLASS** command, see *z/OS DFSMSShsm Storage Administration*

DFSMSHsm: Accommodate default value change for dump VTOC copies

Description

Before z/OS V2R1, the system used a default value of 2 for the VTOCCOPIES parameter of the DFSMSHsm DEFINE DUMPCLASS command. Starting with z/OS V2R1, if the VTOCCOPIES parameter is not specified, the system uses a default value of 0 when DFSMSHsm dumps copy pool volumes. The default value of 2 will continue to be used when DFSMSHsm dumps non-copy pool volumes. If the VTOCCOPIES parameter is never specified, the LIST DUMPCLASS output displays a VTOCCOPIES value of *** to indicate that no value is specified. VTOC copies are not needed in a FRBACKUP/FRRECOV environment.

Table 301 provides more details about this migration action. Use this information to plan your changes to the system.

Table 301. Information about this migration action

Element or feature:	DFSMSHsm
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you want the old default value of VTOCCOPIES(2) in a FRBACKUP/FRRECOV environment.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you want to keep the default value of VTOCCOPIES(2) used before z/OS V2R2 in a FRBACKUP/FRRECOV environment, specify VTOCCOPIES(2) on the DEFINE DUMPCLASS command for each dump class used to dump copy pool volumes.

Reference information

For more information about the VTOCCOPIES parameter of the DEFINE DUMPCLASS command, see *z/OS DFSMSShsm Storage Administration*.

DFSMSrmm: Check how you control your RACF tape profile processing

Description

The currently supported releases of DFSMSrmm support the TAPEAUTHDSN parameter in the DEVSUPxx (device support) parmlib member; however, this support has required enhancements in z/OS V2R2 to be properly implemented.

Migration actions from z/OS V1R13: DFSMS

Before z/OS V2R1, for TAPEAUTHDSN=YES, DFSMSrmm performed tape authorization checks in the DATASET class with DSTYPE=T to indicate to RACF that the check was for data sets on tape volumes and that RACF had to perform a check for discrete profiles.

With z/OS V2R2, DFSMSrmm correctly supports option TAPEAUTHDSN according to the documentation in *z/OS MVS Initialization and Tuning Guide* and in *z/OS DFSMSrmm Implementation and Customization Guide*. If TAPEAUTHDSN=YES is set, DFSMSrmm now performs authorization checking without DSTYPE=T. The RACROUTE is issued in the DATASET class as if for a DASD data set.

If you want to continue using your existing data set profiles (generic or discrete), you need to change your existing TAPEAUTHDSN settings. See “Steps to take.”

Table 302 provides more details about this migration action. Use this information to plan your changes to the system.

Table 302. Information about this migration action

Element or feature:	DFSMSrmm
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have set up the RACF implementation.
Target system hardware requirements:	None
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Check to determine if you use the TAPEAUTHDSN=YES option in your DEVSUPxx parmlib member. If the option is specified, based on the RACF and DFSMSrmm configuration that you use with discrete data set profiles, you must prepare for a change in processing after you IPL V2R2.

If you want to continue using your existing data set profiles (generic or discrete), you need to exchange the current TAPEAUTHDSN settings:

1. Change TAPEAUTHDSN=NO to TAPEAUTHDSN=YES to now make use of generic profiles.
2. Change TAPEAUTHDSN=YES to TAPEAUTHDSN=NO to now make use of discrete profiles.

Reference information

For more information, see the following references:

- See “Enhanced security for tape data sets” in *z/OS MVS Initialization and Tuning Guide*
- See “Recommendations for using RACF tape profile processing” in *z/OS DFSMSrmm Implementation and Customization Guide*.

DFSMS actions to perform after the first IPL of z/OS V2R2

This topic describes DFSMS migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

DFSMSdfp: Configure clusters and storage groups for SMS volume selection

Description

Before z/OS V2R1, when allocating or extending a multi-volume data set, SMS preferred the candidate volumes in the same storage facility image (SFI) if the storage class accessibility attribute was set to CONTINUOUS or CONTINUOUS PREFERRED. With z/OS V2R1, SMS prefers volumes that are in the same cluster. Similarly, when allocating the target data set for the data set fast replication function, SMS now prefers volumes that are in the same cluster as the source data set. In both cases, if it is not possible to honor the preference of volumes in the cluster, SMS reverts to preferring volumes in the same SFI. If you wish SMS to select volumes in the same cluster, you should configure your clusters accordingly.

Before z/OS V2R1, when allocating a striped data set, SMS allocated the stripes across separate logical control units (LCUs). With z/OS V2R1, SMS attempts to allocate the stripes across separate extent pools. If this is not possible, SMS continues to allocate the stripes across LCUs. If you wish SMS to separate the stripes across extent pools, you should configure your storage groups accordingly.

Table 303 provides more details about this migration action. Use this information to plan your changes to the system.

Table 303. Information about this migration action

Element or feature:	DFSMSdfp.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	No, but recommended for optimum efficiency of data set fast replication and for the most uniform performance with striped data sets.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you wish SMS to select volumes in the same cluster, configure your clusters accordingly.

For striped data sets, if you wish SMS to separate the stripes across extent pools, configure your storage groups accordingly.

Reference information

For more information about SMS volume selection and about striped data sets, see *z/OS DFSMSdfp Storage Administration*.

DFSMSdfp: Run OAM DB2 BIND jobs

Description

When migrating to any new release of z/OS, you must run OAM DB2 BIND jobs if you are using OAM for object support. The BIND jobs update DB2 with new OAM DB2 code.

Migration actions from z/OS V1R13: DFSMS

Table 121 on page 184 provides more details about this migration action. Use this information to plan your changes to the system.

Table 304. Information about this migration action

Element or feature:	DFSMSdftp.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use OAM object support.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Run the BIND jobs appropriate to your installation:

1. Update and execute the samplib job CBRPBIND (OAM DB2 Bind Package Job).
2. Do one of the following:
 - If your installation starts OAM, uses the file system sublevel or optical or tape devices, or uses the OAM storage management component (OSMC), do the following:
 - Update and execute samplib job CBRABIND (OAM DB2 Application Plan Bind for LCS and OSR).
 - Update and execute samplib job CBRHBIND (OAM DB2 Application Plan Bind for OSMC).
 - If your installation does not start OAM, use the file system sublevel or optical or tape devices, or use OSMC, update and execute samplib job CBRIBIND (OAM DB2 Application Plan Bind for OSR only).
3. For more information, see the topic on migrating, installing, and customizing OAM in *z/OS DFSMS OAM Planning, Installation, and Storage Administration Guide for Object Support*.

Note: If you choose to edit a previous version of an OAM BIND job, you must incorporate any new changes as described in the header of each samplib OAM BIND job.

Reference information

For more information about OAM, see *z/OS DFSMS OAM Planning, Installation, and Storage Administration Guide for Object Support*.

DFSMSdftp: Define a security product profile for IDCAMS DCOLLECT exit Description

The EXITNAME parameter of the IDCAMS DCOLLECT command allows you to specify an exit to receive control during DCOLLECT processing. After applying the PTF for APAR OA46062 (which was shipped for z/OS V2R1 and V1R13), you must ensure that the exit name is protected through a FACILITY class profile, and that callers of the exit have the appropriate authorization.

Table 122 on page 185 provides more details about this migration action. Use this information to plan your changes to the system.

Table 305. Information about this migration action

Element or feature:	DFSMSdftp.
When change was introduced:	z/OS V2R1 and z/OS V1R13, both with APAR OA46062 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA46062 applied.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if your installation uses the EXITNAME parameter on the IDCAMS DCOLLECT command.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	If a caller attempts to invoke the exit without the proper authorization, the DCOLLECT command fails with the error message: IDC31811I INSUFFICIENT FACILITY CLASS AUTHORIZATION TO INVOKE <i>exitname</i>
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Define a FACILITY class profile with resource name STGADMIN.IDC.DCOLLECT.*exitname*, where *exitname* is the DCOLLECT EXITNAME parameter value.
If the EXITNAME parameter is not specified, the default name is IDCDCX1. You do not require a FACILITY class profile for the default name IDCDCX1.
- Ensure that callers of the exit have at least READ authority to the FACILITY class resource name. If callers have READ authority to one of the FACILITY class profiles STGADMIN.**, STGADMIN.IDC.**, and STGADMIN.IDC.DCOLLECT.*, no action is needed.

Reference information

For more information, see *z/OS DFSMS Access Method Services Commands* .

DFSMSdss: Accommodate new default behavior for full-volume and track restore operations

Description

The data-set-changed indicator (DS1DSCHA) in the VTOC indicates whether or not the data set has changed since its last backup. Before z/OS V2R1, during a full-volume restore operation, DFSMSdss unconditionally reset (turned off) the data-set-changed indicator for each data set restored to the target volume. During a tracks restore operation, if any VTOC track was restored, DFSMSdss might reset the data-set-changed indicator for all data sets on the volume. This applies to all VSAM and non-VSAM data sets and all SMS and non-SMS data sets.

With z/OS V2R1, the default behavior for full-volume and tracks restore operations has changed. By default, DFSMSdss now resets the data-set-changed indicator only if the RESET keyword was specified on the DUMP command. Along with this change, a RESET keyword has been added to the RESTORE FULL and RESTORE TRACKS commands, which allows you to specify whether the data-set-changed indicator is to be reset. In addition, you can use the options installation exit routine, ADRUIXIT, to control the resetting of the data-set-changed indicator.

Migration actions from z/OS V1R13: DFSMS

You can use RESET on the RESTORE command for any FULL or TRACKS dump taken with V2R1, or any previous releases. RESET(YES) and RESET(NO) will work as expected. However, RESET(DUMP) will act as RESET(NO) because there is no way to determine if the RESET keyword was specified at DUMP time on a down-level dump. The new RESET(DUMP) functionality is only available in V2R1.

Note that the default behavior for DFSMSdss DUMP is unchanged when DFSMSHsm invokes DFSMSdss to perform a full volume restore. By default, DFSMSHsm will pass RESET(YES) to DFSMSdss. The other parameters might be specified through the DEFINE DUMPCLASS command.

Table 306 provides more details about this migration action. Use this information to plan your changes to the system.

Table 306. Information about this migration action

Element or feature:	DFSMSdss.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you want DFSMSdss to unconditionally reset the data-set-changed indicator during full-volume and tracks restore operations.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	RESET(DUMP) will act as RESET(NO) because there is no way to determine if the RESET keyword has been specified at DUMP time on a down-level dump. The new RESET(DUMP) function is only available when restoring the dump data set which was taken in V2R2.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

To obtain the behavior in previous releases to allow DFSMSdss to unconditionally reset the data-set-changed indicator during full-volume and tracks restore operations, use RESET(YES) with the RESTORE FULL and RESTORE TRACKS commands. The other options for the RESET keyword are:

NO DFSMSdss does not alter the DS1DSCHA values. Each DS1DSCHA represents the value the data sets had at the time the dump was taken.

DUMP

DFSMSdss resets the data-set-changed indicator (DS1DSCHA=OFF) only if the RESET keyword was specified on the DUMP command. This is the default.

You can also use the options installation exit routine ADRUIXIT or API programs to override the behavior. The ADRUFO parameter list contains these bits in the UFO8FLGS structure:

UF08RESY

Corresponds to RESET(YES)

UF08RESN

Corresponds to RESET(NO)

UF08RESD

Corresponds to RESET(DUMP).

Note: The default behavior is unchanged when DFSMSShsm invokes DFSMSDss to perform a full volume restore. By default, DFSMSShsm will pass RESET(YES) to DFSMSDss. You can specify the other parameters through the DEFINE DUMPCLASS command.

Reference information

For more information, see the following references:

- For details about the RESTORE command, see *z/OS DFSMSdss Storage Administration*
- For details about the installation exit, see *z/OS DFSMS Installation Exits*.
- .

DFSMSDss: Lock or suspend user catalog data sets before performing a logical restore operation

Description

Beginning with V2R1, you must lock or suspend an existing user catalog data set that will be overwritten by a logical restore operation.

If the data set is not locked or suspended, DFSMSDss fails the logical restore operation with the following message:

```
ADR439E (001)-TDVSM(04), A PREALLOCATED DATA SET WAS FOUND
FOR DATA SET UCAT.~ BUT WAS UNUSABLE, 144
```

Note: To use the BCSRECOVER parameter, you require READ access to the RACF FACILITY class profile IGG.CATLOCK. Otherwise, you will receive the following error message:

```
ADR497E (001)-CATLG(05), A CATALOG ERROR OCCURRED WHILE ALTERING ACCESS
TO USER CATALOG UCAT.~. RETURN CODE IS 186, REASON CODE IS FT-002
```

Table 307 provides more details about this migration action. Use this information to plan your changes to the system.

Table 307. Information about this migration action

Element or feature:	DFSMSDss.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, when an existing user catalog data set will be overwritten by a logical restore operation.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Look for batch jobs that are designed to recover a catalog data set using the ADRDSSU utility.
2. If it does not perform an IDCAMS ALTER LOCK of the catalog data set prior to issuing the RESTORE command, modify the batch job to do one of the following:

Migration actions from z/OS V1R13: DFSMS

- Enter a RESTORE command with the BCSRECOVER(LOCK | SUSPEND) parameter, which instructs DFSMSdss to lock or suspend the catalog
- Enter an IDCAMS ALTER command with the SUSPEND or LOCK parameter prior to entering the DFSMSdss RESTORE command
- Enter a MODIFY CATALOG with the RECOVER(LOCK | SUSPEND) parameter prior to entering the RESTORE command.

For example:

```
F CATALOG,RECOVER,LOCK(ucat)
F CATALOG,RECOVER,SUSPEND(ucat)
```

Reference information

For more information about command syntax, see the following references:

- For information about the RESTORE command, see *z/OS DFSMSdss Storage Administration*.
- For more information about the ALTER command, see *z/OS DFSMS Access Method Services Commands*.
- For information about the MODIFY CATALOG command, see *z/OS DFSMS Managing Catalogs*.

DFSORT migration actions

This topic describes migration actions for optional feature DFSORT.

DFSORT actions to perform before installing z/OS V2R2

This topic describes DFSORT migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

DFSORT actions to perform before the first IPL of z/OS V2R2

This topic describes DFSORT migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Update automation for changed DFSORT messages

Description

In z/OS V2R1, the text for some DFSORT messages (ICExxxx) is changed. Text and insert fields have been added, changed, or removed in the messages listed in “Steps to take” on page 397. These changes can affect automation programs that examine the text of the messages.

Table 308 provides more details about this migration action. Use this information to plan your changes to the system.

Table 308. Information about this migration action

Element or feature:	DFSORT.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have automation routines that examine the message text of the messages listed in “Steps to take” on page 397.
Target system hardware requirements:	None.

Table 308. Information about this migration action (continued)

Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Update your automation to handle the following DFSORT message changes:

- The product number has changed from “5694-A01” to “5650-ZOS”, and the release level has changed from “V1R12” to “V2R1”, in message ICE000I.
- The following new messages have been added:
 - ICE290A
 - ICE291I
- Text and insert fields have been changed in the following messages to provide new information:
 - ICE083A
 - ICE099A
 - ICE118I
 - ICE121A
 - ICE141A
 - ICE236I
 - ICE285A
 - ICE288I
 - ICE997I

Reference information

For more information about the ICE messages, see *z/OS DFSORT Messages, Codes and Diagnosis Guide*.

Use TUNE=OLD option to prevent balancing resources for concurrent sort applications

Description

Beginning with z/OS V2R1, a new TUNE installation default allows you to specify whether DFSORT should allocate storage in increments with additional disk work space to minimize the risk of failure, or to allocate all storage at initialization so disk work space allocation can be reduced. The IBM-supplied default for the new TUNE installation option is TUNE=STOR which specifies allocation of available central storage as needed in increments sized to balance resource usage for concurrent sorts. If you want DFSORT to allocate available central storage using fixed sized increments, as in previous releases, you can set TUNE=OLD.

TUNE has the following values:

- STOR
- DISK
- DDYN
- OLD

Migration actions from z/OS V1R13: DFSORT

Table 309 provides more details about this migration action. Use this information to plan your changes to the system.

Table 309. Information about this migration action

Element or feature:	DFSORT.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the default value TUNE=STOR is not acceptable.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	ICEPRMxx member(s) of PARMLIB can be shared between systems running different releases of DFSORT. Any installation options specified in the ICEPRMxx member that are only supported in the newer release of DFSORT will be ignored on the system using the earlier release of DFSORT.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Use ICEPRMxx members activated by a START ICEOPT started task command to set the TUNE=OLD option, as appropriate.
- Alternatively, you can set TUNE=OLD with the previous (less preferred) method of using the ICEMAC macro and usermods.

Reference information

For more information about the TUNE installation option, see *z/OS DFSORT Installation and Customization*.

Use EXPOLD=MAX and EXPRES=0 to prevent changed defaults

Description

Beginning with z/OS V2R1, IBM-supplied defaults have been changed to EXPOLD=50% (from EXPOLD=MAX) and to EXPRES=10% (from EXPRES=0). If you want DFSORT to use the old defaults, as in previous releases, you can set EXPOLD=MAX and EXPRES=0.

Table 310 provides more details about this migration action. Use this information to plan your changes to the system.

Table 310. Information about this migration action

Element or feature:	DFSORT.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the new defaults are not acceptable.
Target system hardware requirements:	None.

Table 310. Information about this migration action (continued)

Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Use ICEPRMxx members activated by a START ICEOPT started task command to set the EXPOLD=MAX or EXPRES=0 options, as appropriate.
- Alternatively, you can set EXPOLD=MAX or EXPRES=0 with the previous (less preferred) method of using the ICEMAC macro and usermods.

Reference information

For more information about the EXPOLD and EXPRES installation options, see *z/OS DFSORT Installation and Customization*.

DFSORT actions to perform after the first IPL of z/OS V2R2

This topic describes DFSORT migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

Distributed File Service migration actions

This topic describes migration actions for base element Distributed File Service.

Distributed File Service actions to perform before installing z/OS V2R2

This topic describes Distributed File Service migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Determine whether to accept the new defaults for variables in the zFS IOEFSPRM file

Description

Before z/OS V2R1, certain default values were used for the IOEFSPRM files or IOEPRMxx parmlib member variables `meta_cache_size`, `metaback_cache_size`, `user_cache_size`, or `convert_auditfid`. Starting in z/OS V2R1, new default values are created for them.

In z/OS V2R1, the zFS IOEFSPRM configuration file variable `convert_auditfid` default value was changed to ON so that all files and directories in zFS file systems can be uniquely identified in SMF audit records. The zFS IOEFSPRM configuration file variable `user_cache_size` default value will be changed to a value that is calculated based on the amount of real storage in the system. The zFS IOEFSPRM configuration file variables `meta_cache_size` and `metaback_cache_size` default values will be changed when both values are not specified to also be calculated based on the amount of real storage in the system. These are so that a system that has the capacity for more storage use and has sufficient space in the ZFS address space can have better performing caches.

Migration actions from z/OS V1R13: Distributed File Service

Table 311 provides more details about this migration action. Use this information to plan your changes to the system.

Table 311. Information about this migration action

Element or feature:	z/OS Distributed File Service
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you do not want the new default values to take effect or if you want to change existing values to the new default values.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	If enough real storage exists, zFS can use more storage by default than it would have used in prior releases.
Related IBM Health Checker for z/OS check:	Use check ZOSMIGV2R1_ZFS_VERIFY_CACHESIZE, which was introduced in APAR OA42672 for z/OS V1R13 (and z/OS V1R12). This check determines whether you are using the default meta_cache_size, metaback_cache_size and user_cache_size and indicates whether the new defaults would affect you. The check name for z/OS V2R1 and higher is ZFS_VERIFY_CACHESIZE. See <i>IBM Health Checker for z/OS User's Guide</i> .

Steps to take

Follow these steps:

- Look for these:
 - IOEFSPRM files or IOEPRMxx parmlib members that do not specify both meta_cache_size and metaback_cache_size options.
 - IOEFSPRM files or IOEPRMxx parmlib members that do not specify the user_cache_size option.
 - IOEFSPRM files or IOEPRMxx parmlib members that do not specify convert_auditfid settings.
 - Programs that use **zfsadm format** commands where unique auditfids are not desired.
 - JCL that contains calls to **ioeagfmt** that create aggregates for which unique auditfids are not desired.
 - Programs that use zFS format API where unique auditfids are not desired.
- Take these actions:
 - For meta_cache_size, metaback_cache_size, or user_cache_size, if the old default values are desired, specify these values in your IOEFSPRM files or IOEPRMxx parmlib members.
 - For auditfid, if you want the previous defaults, specify -nonewauditfid on calls to **ioeagfmt** or **zfsadm format** and convert_auditfid=0FF in your IOEFSPRM files or IOEPRMxx parmlib members.

Reference information

None.

Remove usage of zFS clone function

Description

z/OS V1R13 was the last release that zFS supported the cloning file systems function. The zFS clone functions included the **zfsadm clone** and **zfsadm clonesys** commands. Also removed was the ability to mount any zFS file system aggregates that contain a cloned (.bak) file system. Additional changes as a result of the removal of the cloning file systems function are listed in “Steps to take.”

Table 312 provides more details about this migration action. Use this information to plan your changes to the system.

Table 312. Information about this migration action

Element or feature:	z/OS Distributed File Service
When change was introduced:	z/OS V1R13 was the last release for the function. The function was removed in z/OS V2R1. See <i>IBM United States Software Announcemen 211-007t</i> , dated February 15, 2011.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you are using or have used the zFS clone function.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	If any system earlier than z/OS V2R2 mounts a zFS aggregate that contains a .bak (clone) file system in a shared file system environment, any catch-up mounts on a V2R2 system fail and z/OS UNIX function ships from the V2R2 system to the z/OS UNIX owning system.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Determine whether you have any .bak file systems. You should delete all .bak file systems before you bring zFS into the shared file system environment or before you IPL the V2R2 system. Minimally, you must ensure that no zFS aggregates that contain .bak file systems are mounted. You can do this by issuing a command like the following:

```
zfsadm lsfs | grep .bak
```

You might see results as in this example:

```
PLEX.JMS.AGG1.bak (Not Mounted) 458 K alloc 458 K quota On-line
PLEX.JMS.AGG2.bak (Not Mounted) 26 K alloc 26 K quota On-line
```

This example shows that there are two zFS aggregates that contain a .bak file system: PLEX.JMS.AGG1 and PLEX.JMS.AGG2. In this case, unmount the .bak file systems (if they are mounted) and delete each .bak file system from the aggregate with a command similar to the following example:

```
zfsadm delete PLEX.JMS.AGG1.bak
```

Migration actions from z/OS V1R13: Distributed File Service

(The file system name is case-sensitive.) If the delete fails because the file system was not found, it probably means that the zFS aggregate is not attached. Attach it, delete the .bak file, and detach the aggregate.

- Determine whether any of your tools or application programs use any of the keywords that were removed from the **zfsadm config** or **zfsadm configquery** commands and remove them.
 - In **zfsadm configquery**, `-auto_attach`, `-fsgrow`, and `-user_cache_readahead` were removed.
 - In **zfsadm config**, `-fsgrow` and `-user_cache_readahead` were removed.
- Determine whether any of your tools or application programs use any of the **zfsadm** commands and remove them.
 - zfsadm create**
 - zfsadm lsquota**
 - zfsadm rename**
 - zfsadm setquota**
- Determine whether any of your tools or application programs use the following subcommand numbers for PFSCCTL APIs, which are no longer valid, and remove them.
 - Clone File System (143)
 - Query `auto_attach` setting (183)
 - Query `fsgrow` setting (188)
 - Query `user_cache_readahead` (209)
 - Rename File System (140)
 - Set File System Quota (141)
 - Set `fsgrow` (172)
 - Set `user_cache_readahead` (162)
- (Optional step) The IOEFSPRM variables (`auto_attach`, `fsgrow`, `user_cache_readahead`) are ignored, but you can remove them from your configuration files if you want.

Reference information

For more information, see *z/OS Distributed File Service zFS Administration*.

zFS: Copy data from zFS multi-file system aggregates to zFS compatibility mode aggregates

Description

z/OS V1R13 was the last release of zFS support for multi-file system aggregates. If you have data stored in zFS multi-file system aggregates, you should copy the data from the zFS multi-file system aggregates into zFS compatibility mode aggregates.

As of z/OS V2R1, only zFS compatibility mode aggregates are supported, only zFS compatibility mode aggregates will be supported.

Table 313 provides more details about this migration action. Use this information to plan your changes to the system.

Table 313. Information about this migration action

Element or feature:	z/OS Distributed File Service
When change was introduced:	z/OS V1R13 was the last release for the function. The function was removed in z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you have any multi-file system aggregates.
Target system hardware requirements:	None.

Table 313. Information about this migration action (continued)

Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	Use check ZOSMIGV1R11_ZFS_RM_MULTIFS or check ZOSMIGREC_ZFS_RM_MULTIFS to help determine if any multi-file system aggregates are attached on your system.

Steps to take

Use one of the following methods to determine if you are using zFS multi-file system aggregates:

- Use the IBM Health Checker for z/OS check referenced in Table 313 on page 402.
- Scan your zFS IOEFSPRM configuration options file for `define_aggr` statements.
- Scan your `/etc/rc` file for any **zfsadm attach** commands.
- Enter the **zfsadm agrinfo** command to determine whether an aggregate is a multi-file system aggregate; in the command response, COMP indicates compatibility mode and MULT indicates multi-file system.

If you are using zFS multi-file system aggregates, copy the data from each of those file systems into its own zFS compatibility mode aggregate.

Reference information

For more information, see the following references:

- For more information about zFS commands and administration tasks, see *z/OS Distributed File Service zFS Administration*.
- For more information about IBM health checks, see *IBM Health Checker for z/OS User's Guide*.

Distributed File Service actions to perform before the first IPL of z/OS V2R2

This topic describes Distributed File Service migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

z/FS: Ensure that the zFS kernel is active when using the batch utility ioeagfmt Description

Before z/OS V2R1, the batch utility **ioeagfmt** did not require that the zFS kernel be active. Starting in V2R1, **ioeagfmt** requires that the zFS kernel be active.

Table 314 provides more details about this migration action. Use this information to plan your changes to the system.

Table 314. Information about this migration action

Element or feature:	z/OS Distributed File Services.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.

Migration actions from z/OS V1R13: Distributed File Service

Table 314. Information about this migration action (continued)

Is the migration action required?	Yes, if you did not run ioeagfmt after the kernel was initialized. However, it would be unusual not to have zFS active when running ioeagfmt .
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Look for JCL or vendor applications that might be creating or submitting JCL that contain **ioeagfmt** calls that are run when the zFS kernel is not active. Run them when the zFS kernel is active. If you are formatting file systems to be used by another system, you should be setting the **-version** parameter on **ioeagfmt** because the local zFS kernel would not have the information for a remote zFS system. You can also use the IOEFSUTL program to format aggregates. IOEFSUTL does not require the zFS kernel to be active to format a file system if you specify the **-version** parameter. But it will require the zFS kernel to be active if the **-version** parameter is omitted.

Reference information

For more information, see *z/OS Distributed File Service zFS Administration*.

Distributed File Service actions to perform after the first IPL of z/OS V2R2

This topic describes Distributed File Service migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

SMB: Add **_BPXK_UNUSEDTASKS=KEEP** to the DFSCNTL environment file Description

Before z/OS V2R2 and without the z/OS UNIX PTF for APAR OA39909, which changed threading behavior, SMB users did not have to specify that medium weight threads were to be kept. As of APAR OA39909 and z/OS V2R2, SMB users must keep the original threading behavior by setting the **_BPXK_UNUSEDTASKS=KEEP** environment variable, as described in DFS SMB APAR OA45175.

Table 124 on page 187 provides more details about this migration action. Use this information to plan your changes to the system.

Table 315. Information about this migration action

Element or feature:	Server Message Block (SMB) support of the IBM z/OS Distributed File Service base element.
When change was introduced:	z/OS V2R2, and z/OS V1R13 and V2R1 with PTFs for APARs OA39909 and APAR OA43472 installed.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APARs OA39909 and APAR OA43472 installed.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use SMB.

Migration actions from z/OS V1R13: Distributed File Service

Table 315. Information about this migration action (continued)

Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Failure to implement this migration action prevents the DFS/SMB server from starting or restarting because z/OS UNIX System Services issues a SIGKILL to the DFS/SMB server. The following symptoms might be encountered if this migration action is not implemented: DFSKERN S069 422 SA03 BPXP023I IOEP01100I IOEP01123A RESTART SIGKILL or SYSTEM ABEND S069 - REASON CODE 04
Related IBM Health Checker for z/OS check:	None.

Steps to take

Because SMB is dependent on the threading model that was in effect before the PTFs for APAR OA39909 and APAR OA43472 were installed, you need to take the following steps:

1. To allow SMB to use the original threading behavior, add the environment variable `_BPXK_UNUSEDTASKS=KEEP` to the SMB DFSCNTL environment file, which is typically found in the `/opt/dfslocal/home/dfsctl/envar` directory.
2. If SMB is started, it must be stopped and restarted using the C DFS and S DFS commands.

After you complete the steps, SMB will use the original threading behavior that was in place prior to the PTF for APAR OA39909.

Reference information

For more information, see the following references:

- *z/OS Distributed File Service SMB Administration*
- *z/OS UNIX System Services Planning*

HCD migration actions

This topic describes migration actions for the base element Hardware Configuration Definition (HCD).

HCD actions to perform before installing z/OS V2R2

This topic describes HCD migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Migrate security definitions for HCM users

Description

With z/OS V2R1, Hardware Configuration Definition (HCD) uses the application ID `CBDSERVE` to verify any user that logs on to the HCD agent, that is, any user that uses Hardware Configuration Manager (HCM) to perform hardware configuration definitions. If you have the `APPL` class active in your external security manager, for example in RACF, and you have a generic profile in that class that covers the new

Migration actions from z/OS V1R13: HCD

HCD application ID CBDSERVE, you need to permit all HCM users READ access to that profile. Otherwise, the users of HCM are no longer able to log on to HCD.

Table 316 provides more details about this migration action. Use this information to plan your changes to the system.

Table 316. Information about this migration action

Element or feature:	HCD
When change was introduced:	z/OS V2R1
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use HCM to perform hardware configuration definitions, have the APPL security class active in your security product, and have a APPL profile that covers the application ID CBDSERVE.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

You can either give all HCM users READ access to your existing APPL profile that covers the HCD application ID CBDSERVE, or you can define a specific profile for the new HCD application ID and permit all HCM users to that profile. Sample definitions for a new profile and a user HCDUSER for RACF are similar to the following:

```
RDEFINE APPL CBDSERVE UACC(NONE)
PERMIT CBDSERVE CLASS(APPL) ID(HCDUSER) ACCESS(READ)
```

Reference information

For more information, see the following references:

- For information about protecting applications and the security definitions in RACF, see *z/OS Security Server RACF Security Administrator's Guide*.
- For information about setting up the HCD agent for use by HCD and HCM users, see *z/OS HCD User's Guide*.

HCD actions to perform before the first IPL of z/OS V2R2

This topic describes HCD migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

None.

HCD actions to perform after the first IPL of z/OS V2R2

This topic describes HCD migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

HLASM migration actions

This topic describes migration actions for the base element High Level Assembler (HLASM).

HLASM actions to perform before installing z/OS V2R2

This topic describes HLASM migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Accommodate new assembler mnemonics for new machine instructions

Description

IBM z Systems introduced new instructions with mnemonics that might collide with existing macro instruction names. Collisions can be managed by using a different OPTABLE option or mnemonic tag.

Note: HLASM APAR PM79901 provides new hardware support for IBM z13. New instructions have been added to the UNI and ZS7 optables. The ESA vector facility instructions have been removed from the UNI optable. For a complete list of the instructions that are affected, see the technote *New hardware support - APAR PM79901* at the following web site: IBM Support Portal.

Table 125 on page 189 provides more details about this migration action. Use this information to plan your changes to the system.

Table 317. Information about this migration action

Element or feature:	HLASM
When change was introduced:	z/OS V2R1, z/OS V1R13, and z/OS V1R12, all with hardware support HLASM APARs. Some of the most recent APARs include PM79901, PM49761, and PM86821.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, without hardware support HLASM APARs installed.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you have a collision with a new instruction mnemonic.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Look for possible conflicts between new mnemonics and existing macro instructions with the same name:

1. Assemble an END statement with the OPTABLE(UNI,LIST) option to cause HLASM to display all mnemonics in the UNI opcode table.
2. If a conflicting name appears, do one of the following:
 - Use either a different OPTABLE option to avoid the new mnemonics or mnemonic tags to distinguish machine instruction use from macro instruction use.
 - Change the macro names.

Migration actions from z/OS V1R13: IBM HLASM

Tip: For a tool to help in identifying mnemonic conflicts, see *Techdoc PRS5289* at the IBM Techdocs website.

Reference information

For more information, see the following references:

- For information about the OPTABLE option, see *HLASM Programmer's Guide*.
- For information about mnemonic tags, see *HLASM Language Reference*.

HLASM actions to perform before the first IPL of z/OS V2R2

This topic describes HLASM migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Adjust the block size on assembler SYSLIN when using the HEWLKED linkage editor program

Description

Historically, when a SYSPUNCH or SYSLIN data set is created by HLASM on z/OS and the BLKSIZE parameter is either not specified or specified with a value of 0, HLASM will create a data set which has a BLKSIZE equal to the LRECL value. This is typically not an optimal BLKSIZE value and may result in a poorly performing data set.

By the enhancement of APAR PI10515 (PTF UI15579 for z/OS V2R1, V1R13, and V1R12), HLASM has been modified not to set the default BLKSIZE to LRECL if a block size of zero is supplied for SYSLIN and SYSPUNCH data sets. HLASM will now leave the BLKSIZE as zero to allow DFSMS to determine the block size based upon the its criteria.

Note: When system-determined block sizes (SDBs) are used for SYSLIN data sets, the data set may be created with a larger block size than supported by the HEWLKED linkage editor.

Table 126 on page 190 provides more details about this migration action. Use this information to plan your changes to the system.

Table 318. Information about this migration action

Element or feature:	HLASM.
When change was introduced:	z/OS V2R1 and z/OS V1R13, both with APAR PI10515 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR PI10515 applied.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you invoke the linkage editor (HEWLKED) rather than the Binder (IEWBLINK) and will be affected by the block size selection as described.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

When you invoke the linkage editor (HEWLKED) rather than the Binder (IEWBLINK), the maximum block size of data sets defined in the SYSLIN definition is 3200 bytes. After the HLASM APAR PI10515 (PTF UI15579), when the BLKSIZE is not supplied to the SYSLIN data set in the ASM step, it is created with large block size (for example, 27920) by the SDB. The old linkage editor does not accept the block size larger than 3200, which results in the following error message:

```
CC16.IEW0594 ERROR - INPUT DATA SET BLOCKSIZE IS INVALID
```

To avoid using SDB when invoking the HEWLKED linkage editor, you need to supply a BLKSIZE of 3200 or less (which is a multiple of the LRECL) in the SYSLIN data set in ASM step.

Reference information

For more information, see the following references:

- PTF UI15579 and DOC APAR PI19003.
- PSP Bucket (Upgrade HLASM160, Subset HMQ4160).
- For more information on HEWLKED, see *z/OS MVS Program Management: User's Guide and Reference* .
- For more information on system-determined block sizes, see *z/OS DFSMS Using Data Sets* .
- For more information on assembler data set characteristics, see *HLASM Programmer's Guide* .

HLASM actions to perform after the first IPL of z/OS V2R2

This topic describes HLASM migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

IBM HTTP Server migration actions

This topic describes migration actions for base element IBM HTTP Server.

IBM HTTP Server actions to perform before installing z/OS V2R2

This topic describes IBM HTTP Server migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Plan for the removal of IBM HTTP Server powered by Domino Description

z/OS V2R1 was the last release to include the IBM HTTP Server powered by Domino. New base element, IBM HTTP Server - Powered by Apache (IHSA), is introduced in z/OS V2R2. This element replaces IBM HTTP Server powered by Domino. z/OS V2R2 contains IHSA at level 9.0.

If your installation is using IBM HTTP Server powered by Domino, you must migrate to IBM HTTP Server - Powered by Apache. It is strongly recommended that you perform this migration in two phases, as described in "Steps to take" on page 192. Both IBM HTTP Server - Powered by Apache 8.5.5 and IBM HTTP Server - Powered by Apache 9.0 are supported on z/OS V2R2. Note, however, that IBM HTTP Server - Powered by Apache 8.5.5 support on z/OS V2R2 is planned to continue only until the end of service date for z/OS V2R1 (planned for September 2018).

IBM HTTP Server powered by Domino is not supported on z/OS V2R2.

Table 127 on page 191 provides more details about this migration action. Use this information to plan your changes to the system.

Migration actions from z/OS V1R13: IBM HTTP Server

Table 319. Information about this migration action

Element or feature:	IBM HTTP Server powered by Domino.
When change was introduced:	z/OS V2R2. This change was also announced in the statement of direction <i>IBM United States Software Announcement 213-292 "IBM z/OS Version 2 Release 1 delivers the foundation for Smarter Computing,"</i> dated July 23, 2013.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you currently use IBM HTTP Server powered by Domino.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	The HTTP servers that are included in other IBM licensed programs, such as WebSphere Application Server, are not affected. This migration action applies only to users of the IBM HTTP Server that is included in the base z/OS operating system.
Related IBM Health Checker for z/OS check:	<p>The check IBMZMIG,ZOSMIG_HTTP_SERVER_DOMINO is used to determine whether IBM HTTP Server powered by Domino is in use on your system. The check is written in REXX and is provided on an as-is basis at http://www.ibm.com/systems/z/os/zos/installation/HTTP_Health_Checker.html.</p> <p>The check is not provided in an APAR; for instructions on adding it to your system, see the web page.</p>

Steps to take

In z/OS V2R2, you must migrate to IBM HTTP Server - Powered by Apache, which is included as a base element of z/OS. It is recommended that you perform this migration in two phases, as follows:

1. Before you install z/OS V2R2, use the separate licensed program z/OS Ported Tools HTTP Server feature (5655-M23) on z/OS V2R1 or z/OS V1R13. You can run the IBM Ported Tools HTTP Server and the IBM HTTP Server powered by Domino concurrently, if necessary, for certain functions that do not support the IBM Ported Tools HTTP Server on z/OS V2R1 or z/OS V1R13, such as Infoprint Server at those release levels (see "Infoprint migration action for HTTP Server").

In this phase of the migration, you can perform much of the migration work for z/OS V2R2 IBM HTTP Server in advance and stabilize on IBM HTTP Server - Powered by Apache. The z/OS Ported Tools HTTP Server feature is at level 8.5.5 (Apache V2.2.8 level).

2. After you install z/OS V2R2, migrate from z/OS Ported Tools HTTP Server feature to z/OS V2R2 IBM HTTP Server - Powered by Apache. In z/OS V2R2, IBM HTTP Server - Powered by Apache is at the 9.0 level (based on Apache V2.4). Here, you need only to perform the migration actions between IBM HTTP Server 8.5.5 and 9.0, which are fewer than the number of migration actions that are needed to move from IBM HTTP Server powered by Domino directly to IBM HTTP Server - Powered by Apache at the 9.0 level.

Note: To avoid an error (condition code 0137 and ABENDU4093 RC00000281) ensure that REGION=0M is specified on the EXEC statement of the IBM HTTP Server started procedure. APAR PI47828 (Apache 8.5.5) and APAR PI50373 (Apache 9.0) updates the sample procedure to specify REGION=0M and TIME=NOLIMIT.

Reference information

For more information, see the following references:

- For information about supported versions of IBM HTTP Server, see Washington Systems Center flash 10857 at <http://www.ibm.com/support/techdocs>. Search for “flash10857”.
- For instructions on migrating from IBM HTTP Server powered by Domino to IBM HTTP Server - Powered by Apache, see IBM Redbook *IBM HTTP Server on z/OS: Migrating from Domino-powered to Apache-powered*, REDP-4987.
- For instructions on migrating from IBM HTTP Server - Powered by Apache 8.5.5 to 9.0, see <http://httpd.apache.org/docs/2.4/upgrading.html>.

IBM HTTP Server actions to perform before the first IPL of z/OS V2R2

This topic describes IBM HTTP Server migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

None.

IBM HTTP Server actions to perform after the first IPL of z/OS V2R2

This topic describes IBM HTTP Server migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

IBM Tivoli Directory Server migration actions

This topic describes migration actions for the base element IBM Tivoli Directory Server.

IBM Tivoli Directory Server actions to perform before installing z/OS V2R2

This topic describes IBM Tivoli Directory Server migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Accommodate new sslCipherSpecs default Description

Starting in z/OS V2R2, z/OS IBM Tivoli Directory Server changed its default setting for the LDAP server **sslCipherSpecs** configuration file option. This configuration option specifies the accepted cipher suites that are used in SSL/TLS secure connections. The **sslCipherSpecs** configuration file option can be specified in various ways as an arithmetic expression that represents a mask, including decimal values, hexadecimal values, or keywords that are included or excluded in combination with the **ANY** keyword.

If the LDAP server uses SSL/TLS secure connections and the **sslCipherSpecs** configuration option is not specified in the LDAP server configuration file, the default enabled ciphers no longer include the RSA-EXPORT or RC4 ciphers "03", "04", "05", or "06".

Migration actions from z/OS V1R13: IBM Tivoli Directory Server

These ciphers are specified in the `sslCipherSpecs` configuration file option individually in numeric or keyword form as follows:

Table 320. SSL ciphers supported by the `sslCipherSpecs` configuration option

SSL Cipher	LDAP Server keyword	Decimal value	Hexadecimal value	Description
"03"	RC4_MD5_EXPORT	8192	x00002000	40-bit RC4 encryption with MD5 message authentication and RSA key exchange.
"04"	RC4_MD5_US	2048	x00000800	128-bit RC4 encryption with MD5 message authentication and RSA key exchange.
"05"	RC4_SHA_US	1024	x00000800	128-bit RC4 encryption with SHA-1 message authentication and RSA key exchange.
"06"	RC2_MD5_EXPORT	4096	x00001000	40-bit RC2 encryption with MD5 message authentication and RSA key exchange.

Table 129 on page 194 provides more details about this migration action. Use this information to plan your changes to the system.

Table 321. Information about this migration action

Element or feature:	z/OS IBM Tivoli Directory Server.
When change was introduced:	z/OS V2R2. z/OS V2R1 and z/OS V1R13, both with APAR OA47491.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both without APAR OA47491.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you are using SSL/TLS secure connections.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	LDAP SSL/TLS secure connections might fail if a client application is relying on one of the defined default ciphers and it is no longer enabled.
Related IBM Health Checker for z/OS check:	None.

Steps to take

These ciphers are also included when the `sslCipherSpecs` configuration file option is specified as **ANY**. The `sslCipherSpecs` configuration file option includes 24 different ciphers in the **ANY** keyword.

For a complete description of the `sslCipherSpecs` configuration file option, see *Setting up the security options, and SSL ciphers supported by the `sslCipherSpecs` configuration option in z/OS IBM Tivoli Directory Server Administration and Use for z/OS*.

In z/OS V2R2, z/OS IBM Tivoli Directory Server has changed its default setting for the LDAP server `sslCipherSpecs` configuration file option from **ANY** to **ANY-RC4_MD5_EXPORT-RC4_MD5_US-RC4_SHA_US-RC2_MD5_EXPORT**. If you currently omit the `sslCipherSpecs` configuration file option

and want to continue accepting all ciphers included in the ANY keyword, specify `sslCipherSpecs ANY` in the general section of the LDAP server configuration file. Consider determining the actual set of ciphers that are needed and specify the appropriate value for the `sslCipherSpecs` configuration file option.

Reference information

For more information, see *z/OS IBM Tivoli Directory Server Administration and Use for z/OS*.

IBM Tivoli Directory Server actions to perform before the first IPL of z/OS V2R2

This topic describes IBM Tivoli Directory Server migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

None.

IBM Tivoli Directory Server actions to perform after the first IPL of z/OS V2R2

This topic describes IBM Tivoli Directory Server migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

IBM z/OS Management Facility migration actions

This topic describes migration actions for the base element IBM z/OS Management Facility (z/OSMF).

z/OSMF actions to perform before installing z/OS V2R2

This topic describes z/OSMF migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Convert to SAF Authorization Mode Description

If your current (old) system is currently running z/OSMF V1R13 in Repository Authorization Mode, you must convert your existing security setup to SAF Authorization Mode before moving to z/OSMF V2R1. Doing so will require you to repeat the steps of the z/OSMF configuration process, supplying your current configuration file as input. The z/OSMF configuration process generates new REXX execs, which your security administrator can use to set up security for z/OSMF and authorize additional users to the product. If more than the default set of user authorizations is required, your security administrator is responsible for converting your existing z/OSMF user authorizations to SAF profiles and groups, for use under SAF authorization mode.

Table 322 provides more details about this migration action. Use this information to plan your changes to the system.

Table 322. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.

Migration actions from z/OS V1R13: z/OSMF

Table 322. Information about this migration action (continued)

Timing:	Before installing z/OS V2R2
Is the migration action required?	Yes, if your installation currently runs z/OSMF in repository authorization mode.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

The following procedure assumes that:

- You have a valid z/OSMF configuration
- The z/OSMF data file system is mounted
- IBM WebSphere® Application Server OEM Edition for z/OS has been started previously.

To switch your current configuration to SAF Authorization Mode, follow these steps:

1. Stop the WebSphere server. Ensure that IBM WebSphere Application Server OEM Edition for z/OS is not running. If IBM WebSphere Application Server OEM Edition for z/OS is active, you must enter the appropriate STOP command to shut it down.
2. Configure z/OSMF as you normally would, but specify SAF Authorization Mode for your configuration. For example, if you use an override file when configuring z/OSMF, you can specify the authorization mode as a property in your override file, as shown:

```
IZU_AUTHORIZATION_MODE=SAF
```

Figure 1. Override file updated for SAF Authorization Mode

Run the **izusetup.sh** script, as follows:

```
izusetup.sh -file izuconfig1.cfg -config  
-overridefile filename.ovr [-fastpath]
```

where *izuconfig1.cfg* is the configuration file that was used during the initial configuration of z/OSMF. This action will update the configuration file with the new values.

You can include the *-fastpath* option to have the **izusetup.sh** script run without any interactive prompting. Instead, the script uses the values from the configuration file and the override file. Omitted values will cause the script to end with errors.

For reference on the **izusetup.sh** script and the z/OSMF configuration process, see *IBM z/OS Management Facility Configuration Guide*.

3. Have your security administrator run the security commands for the new authorization mode. When you convert an existing z/OSMF configuration to SAF Authorization Mode, the configuration process creates two security commands REXX execs for your use:
 - *izuconfig1.cfg.rexx* contains the complete set of RACF commands for a new configuration.
 - *izuconfig1.cfg.convertFromREPtSAF.rexx* contains only the delta of security commands of RACF commands that are required for setting up security under SAF Authorization Mode.

You need run only one of the two execs. Most likely, you will run the conversion exec. If during the preceding step, however, you added more plug-ins to your configuration, use the `izuconfig1.cfg.rexx` exec. Have your security administrator review the contents of the REXX execs before running either.

With the `IZU_CONFIG_DIR` directory as your active directory, run the REXX exec. For example:

```
./izuconfig1.cfg.convertFromREPtoSAF.rexx
```

When running the RACF rexx exec, some commands might fail due to duplicate security settings. You can ignore these messages.

On completion, the REXX exec creates the security definitions needed for your configuration.

4. Have your security administrator verify the security for the configuration. Run the **izusetup.sh** script, as follows:

```
izusetup.sh -file izuconfig1.cfg -verify racf
```

5. Prime the z/OSMF data file system. Run the **izusetup.sh** script, as follows:

```
izusetup.sh -file izuconfig1.cfg -prime
```

For reference, see the topic "Step 4. Prime the z/OSMF data file system" in your copy of the *z/OSMF Configuration Guide* for z/OSMF V1R13. (The `-prime` option was removed in z/OSMF V2R1.)

6. Complete the setup. From the administrator user ID (ZOSMFAD, by default), run the **izusetup.sh** script, as follows:

```
izusetup.sh -file izuconfig1.cfg -finish
```

This script might take some time to complete. As it runs, the script writes messages to the script log file. For reference, see *IBM z/OS Management Facility Configuration Guide*.

7. Restart the WebSphere server.

Reference information

For information about z/OSMF configuration, see *IBM z/OS Management Facility Configuration Guide*.

Review the SAF profile prefix Description

Does your security product use the SAF profile prefix `BBNBASE` for z/OSMF resources? If so, be aware of the following changes, which occurred with z/OSMF V2R1.

- In previous releases, the configuration variable `IZU_WAS_PROFILE_PREFIX` was used to identify the WebSphere SAF profile prefix, which was `BBNBASE` by default. With the removal of IBM WebSphere Application Server OEM Edition for z/OS in z/OSMF V2R1, this variable is no longer specified.
- In z/OSMF V2R1, the configuration variable `IZU_SAF_PROFILE_PREFIX` is added. Use this value to specify the SAF profile prefix for a z/OSMF. By default, the prefix is `IZUDFLT`.

Table 323 provides more details about this migration action. Use this information to plan your changes to the system.

Table 323. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you want to use the current defaults.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.

Migration actions from z/OS V1R13: z/OSMF

Table 323. Information about this migration action (continued)

Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If your installation is migrating from an earlier release of z/OSMF, it is recommended that you review the use of the BBNBASE prefix and determine whether your security product definitions for z/OSMF should be revised to use the new prefix IZUDFLT.

Tip: To identify all of the affected profiles in a RACF database, you can use this RACF command: `SEARCH ALL CLASS(ZMFAPLA) FILTER(BBNBASE.**)`.

Reference information

For information about configuring z/OSMF, see *IBM z/OS Management Facility Configuration Guide*.

Check the security for ports 32207 and 32208

Description

With the removal of IBM WebSphere Application Server OEM Edition for z/OS in z/OSMF V2R1, the specification of HTTP port values is changed. You can use the z/OSMF supplied port settings, or specify new values during the z/OSMF configuration process.

The port values are specified through the following configuration variables:

- `IZU_HTTP_SSL_PORT`, which specifies the port number for SSL encrypted traffic from your z/OSMF configuration. As of z/OSMF V2R1, the default port number is changed from 32208 (the WebSphere default), to 443, which follows the Internet Engineering Task Force (IETF) standard.
- `IZU_HTTP_PORT`, which was added in z/OSMF V2R1. This variable specifies the port number for non-encrypted traffic, which is 80, by default. Note that if your installation is migrating from an earlier release of z/OSMF, however, you might have specified port number 32207 for this value, which is the WebSphere default.

Table 324 provides more details about this migration action. Use this information to plan your changes to the system.

Table 324. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you want to use the current defaults.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If your installation is migrating from an earlier release of z/OSMF, you might have used port numbers 32207 and 32208 for z/OSMF web traffic. These earlier values are not persisted when you migrate to z/OS V2R2. Determine whether ports 32207 and 32208 should remain active on your system, and update the settings or close the ports, as required by your installation security policies.

Reference information

For information about configuring z/OSMF, see *IBM z/OS Management Facility Configuration Guide*.

Evaluate your usage of the zOSMFAD user ID from previous releases

Description

In previous releases of z/OSMF, the configuration process created a special user ID known as the z/OSMF administrator user ID. By default, the user ID was ZOSMFAD. You used this user ID for running configuration scripts and performing administration tasks, such as adding users and working with z/OSMF log files.

As of z/OSMF V2R1, the configuration process no longer creates, or requires the use of, the administrator user ID. Though z/OSMF retains the concept of an administrator role, you can use any existing user ID for this purpose, as long as you define the user ID to the z/OSMF administrator security group (IZUADMIN).

If you do not use the z/OSMF administrator user ID for any other purposes, you can remove it and its associated authorizations as part of the migration to z/OS V2R2.

Table 325 provides more details about this migration action. Use this information to plan your changes to the system.

Table 325. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you want to continue using the ZOSMFAD user ID (or whichever value you specified for IZU_ADMIN_NAME) in z/OS V2R2, you must ensure that it has superuser authority, which is needed for running the z/OSMF configuration scripts. At a minimum, ensure that ZOSMFAD has the following UNIXPRIV class profile privileges:

- CONTROL access to SUPERUSER.FILESYS
- UPDATE access to SUPERUSER.FILESYS.MOUNT
- READ access to SUPERUSER.FILESYS.CHOWN

Migration actions from z/OS V1R13: z/OSMF

- READ access to SUPERUSER.FILESYS.CHANGEPERMS
- READ access to SUPERUSER.FILESYS.PFSCCTL

If you do not want to continue using the ZOSMFAD user ID, you can remove this user ID and its associated authorizations. For a RACF installation, your security administrator can use a utility to identify the user ID objects and authorizations in the RACF database, including the following examples:

- z/OSMF administrator user ID. By default, this is ZOSMFAD.
- Directories and files that were created for the ZOSMFAD user ID, such as /home/zosmfad
- Administrator user ID authorizations to z/OSMF resources, as follows:
 - WebSphere Application Server administrators group (WSCFG1)
 - CIM server administrators group (CFZADMGP)
 - Capacity Provisioning Query Group (CPOQUERY)
 - Capacity Provisioning Control Group (CPOCTRL)
 - Workload Management group (WLMGRP)

Reference information

For information about configuring z/OSMF, see *IBM z/OS Management Facility Configuration Guide*.

Remove WebSphere constructs from previous releases

Description

In previous releases of z/OSMF, your installation configured an instance of IBM WebSphere Application Server OEM Edition for z/OS for each instance of z/OSMF. This process produced a number of WebSphere constructs on your system, such as configuration files and log files, and the WebSphere servant region user ID. As of z/OSMF V2R1, these constructs are no longer needed; you can remove them.

Table 326 provides more details about this migration action. Use this information to plan your changes to the system.

Table 326. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended to clean up the system with unnecessary constructs.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

To find the residual constructs, check the directories and files under mount point /zWebSphereOEM/V7R0/config1. You can remove these constructs as part of your migration to z/OS V2R2.

Also, check for the WebSphere servant region user ID and any associated security authorizations in your security product. In previous releases, this user ID was defined on variable `IZU_SERVANT_USERID` in your configuration file or override file. By default, the user ID is `WSSRU1`.

Reference information

For information about configuring z/OSMF, see *IBM z/OS Management Facility Configuration Guide*.

Remove the APF authorization for SYS1.MIGLIB(AMATERSE)

Description

Beginning in z/OSMF V2R1, the Incident Log task no longer requires that your `SYS1.MIGLIB` data set be APF-authorized. If no other programs or functions on your system require `SYS1.MIGLIB` to be APF-authorized, you can remove this authorization when you are satisfied with z/OSMF V2R1, and have no plans to fall back to an earlier release. Otherwise, leave this authorization in place.

Table 327 provides more details about this migration action. Use this information to plan your changes to the system.

Table 327. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if the only reason you had APF authorized <code>SYS1.MIGLIB</code> was for the Incident Log task.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

APF authorizations are defined in the `PROGxx` member of `SYS1.PARMLIB`, if your site follows IBM recommendations. If you added `SYS1.MIGLIB` to the APF list for z/OSMF or the Incident Log task, it is recommended that you remove the explicit authorization. To do so, locate the appropriate `PROGxx` member and edit it to remove the APF ADD statement associated with `SYS1.MIGLIB`.

Reference information

For information about configuring z/OSMF, see *IBM z/OS Management Facility Configuration Guide*.

Remove the most-generic profile for z/OSMF authorizations

Description

In previous releases of z/OSMF, the generated program `izuconfig1.cfg.rexx` included RACF commands for defining the following generic profile in the `ZMFAPLA` class, and for creating permissions to it:

```
<SAF-prefix>.ZOSMF.**
```

Migration actions from z/OS V1R13: z/OSMF

where *<SAF-prefix>* is the SAF profile prefix that was defined for your configuration (by default, IZUDFLT). If you used **izuconfig1.cfg.rexx** in a previous release, this generic profile was created for your configuration.

As of z/OS V2R2, the z/OSMF configuration process no longer creates authorizations based on this most-generic profile. Instead, authorizations are now created based on the following discrete generic profile:

<SAF-prefix>.ZOSMF

In this release, a sample job is provided in SYS1.SAMPLIB(IZUSEC) to help you create the resource names and security authorizations for z/OSMF. Your security administrator can edit and run this job to secure various resources on the z/OS system.

For the profiles and permissions that are created, see the contents of the IZUSEC sample job.

Table 131 on page 197 provides more details about this migration action. Use this information to plan your changes to the system.

Table 328. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OSMF V2R1 with APAR PI20091 applied.
Applies to migration from:	z/OSMF V2R1 without APAR PI20091 applied, and z/OSMF V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have used a generic profile and want to use discrete profiles for more granular control.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	The older generic profiles still work, but you do not have the granularity of more discrete profiles, which provide better control over access to specific resources.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Create the discrete profiles that you need for z/OSMF. In a RACF installation, you can use the commands in job IZUSEC to define profiles and create authorizations.
2. Ensure that your existing user authorizations are converted to user authorizations based on the discrete profiles. To preserve your existing authorizations, you can copy the access list from an existing profile into another existing profile, using the FROM operand on the **PERMIT** command.
3. Remove the most-generic profile for z/OSMF authorizations. In a RACF installation, you can use the following commands to remove the generic profile:

```
RDELETE ZMFAPLA IZUDFLT.ZOSMF.**  
SETROPTS RACLIST(ZMFAPLA) REFRESH
```

Reference information

For a list of the authorizations required in z/OSMF, see *IBM z/OS Management Facility Configuration Guide*.

z/OSMF actions to perform before the first IPL of z/OS V2R2

This topic describes z/OSMF migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

None.

Check the security profile for the Software Management task Description

In z/OSMF V1R13 (prior to APAR PM73833), the deployment functions were provided in the Deployment task. In z/OSMF V2R1, the name of this task is changed to Software Management to reflect the software management functions that are provided in addition to the deployment functions.

Table 329 provides more details about this migration action. Use this information to plan your changes to the system.

Table 329. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if your installation created a discrete profile to control access to the Deployment task.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If your installation used SAF Authorization Mode in z/OSMF V1R13 and used the following default, generic profile to control access to the Deployment task, no migration actions are required:

```
<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.**
```

If your installation chose not to use the generic profile and instead created a discrete profile to control access to the Deployment task, a migration action is required. For example, suppose your installation created the following profile to control access to the Deployment task in z/OSMF V1R13:

```
<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DEPLOYMENT
```

Because the name changed in z/OSMF V2R1, your installation must create a generic profile like the default or a discrete profile like the following to control access to the Software Management task:

```
<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT
```

Migration actions from z/OS V1R13: z/OSMF

Reference information

For information about creating authorizations for z/OSMF plug-ins, see *IBM z/OS Management Facility Configuration Guide*.

Authorize the z/OSMF server to create PassTickets

Description

If your current (old) system includes the Capacity Provisioning plug-in or the Resource Monitoring plug-in, these functions might be using PassTickets for secure communication with a remote server, as an alternative to passwords. If so, you must ensure that the z/OSMF server user ID is authorized to create PassTickets in the same way that you did for the WebSphere servant user ID on previous systems. By default, this user ID is WSSRU1.

Table 330 provides more details about this migration action. Use this information to plan your changes to the system.

Table 330. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if your current (old) system includes the Capacity Provisioning plug-in or the Resource Monitoring plug-in, and these functions are using PassTickets for secure communication with a remote server.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- For the Capacity Provisioning plug-in, determine whether your installation is using PassTickets to authenticate requests against the CIM server on a remote system. If so, you defined the profile IRRPTAUTH.CFZAPPL.* in the PTKTDATA class. To authorize the z/OSMF server to create PassTickets, grant the z/OSMF started task user ID at least UPDATE access authority to this resource. For example:

```
PERMIT IRRPTAUTH.CFZAPPL.* CLASS(PTKTDATA) ID(passticket_creator_userid)  
ACCESS(UPDATE)  
SETROPTS RACLIST(PTKTDATA) REFRESH
```

where *passticket_creator_userid* is the z/OSMF started task user ID. By default, this is IZUSVR.

- For the Resource Monitoring plug-in, determine whether your installation is using PassTickets to authenticate requests against the RMF Distributed Data Server (DDS) on a remote system. If so, you defined the profile IRRPTAUTH.GPMSERVE.* in the PTKTDATA class. To enable PassTicket creation for the z/OSMF server, give the z/OSMF started task user ID at least UPDATE access authority. For example:

```
PERMIT IRRPTAUTH.GPMSERVE.* CLASS(PTKTDATA) ID(passticket_creator_userid)
ACCESS(UPDATE)
SETROPTS RACLIST(PTKTDATA) REFRESH
```

where *passticket_creator_userid* is the z/OSMF started task user ID. By default, this is IZUSVR.

Reference information

For more information, see the following references:

- For information about PassTickets, see *z/OS Security Server RACF Security Administrator's Guide*
- For information about clean-up actions for IBM WebSphere Application Server OEM Edition for z/OS, see "Remove WebSphere constructs from previous releases" on page 418.

Install the z/OSMF cataloged procedures

Description

z/OSMF requires that several cataloged procedures be installed on your system, as described in this topic.

Table 331 provides more details about this migration action. Use this information to plan your changes to the system.

Table 331. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

z/OSMF requires that the following cataloged procedures be installed on your system:

- **Started procedures for the z/OSMF server:** z/OSMF processing is managed through the z/OSMF server, which runs as a pair of started tasks on your system, IZUANG1 and IZUSVR1.
- **Logon procedure for the z/OS data set and file REST interface:** When you install the PTFs for APAR PM98630 and the corequisite APARs, z/OSMF requires that a TSO logon procedure be installed in your system proclib. The procedure is used internally by the z/OS data set and file REST interface services. IBM supplies a default procedure, IZUFPROC, which you must install prior to configuration. The default procedure should be sufficient for most z/OS installations. Review the procedure before installing it, however, to ensure that it is suitable for use in your environment.

If appropriate, you can use an alternative logon procedure, if it provides the same function as the shipped IZUFPROC procedure. Specifically, your logon procedure must contain, at a minimum, all of the DD statements from IZUFPROC; these must reference your system data sets that contain the z/OS UNIX REXX exec programs and ISPF libraries. Also, if your installation uses an actual (non-temporary) data set for ISPFPROF, the logon procedure must be configured to allow profile sharing.

Migration actions from z/OS V1R13: z/OSMF

IBM supplies the catalogued procedures for z/OSMF in your order, as follows:

- **ServerPac and CustomPac orders:** For a ServerPac order, IBM supplies the catalogued procedures in SYS1.IBM.PROCLIB. For a CustomPac order, you can rename this data set through the installation dialog.
- **CBPDO orders:** For a CBPDO order, the data set name is SYS1.PROCLIB; you can rename this data set. During installation, you can optionally catalog the data set, or you can defer this step.

Ensure that the z/OSMF catalogued procedures reside in the SMP/E defined PROCLIB, as follows:

- **ServerPac and CustomPac users:** Ensure that SYS1.IBM.PROCLIB (or whatever you renamed it to) resides in the JES PROCLIB concatenation. Or, copy its contents to a data set in the JES PROCLIB concatenation.
- **CBPDO users:** Ensure that SYS1.PROCLIB (or whatever you renamed it to) resides in the JES PROCLIB concatenation (and is catalogued). Or, copy its contents to a data set in the JES PROCLIB concatenation.

Note that these steps are the same as you would do for any SMP/E installed catalogued procedure that is provided with z/OS.

Reference information

For information about starting the started tasks, and optionally setting them up to start after every IPL, see *IBM z/OS Management Facility Configuration Guide*.

Verify that the z/OSMF server has sufficient authorization

Description

To ensure that the z/OSMF server can be started and stopped by your operations personnel, verify that the z/OSMF started task user ID has sufficient permissions for your environment. By default, this user ID is IZUSVR, but you might have specified another user ID during the configuration process. For example, many installations choose to restrict access to the MVS **START** and **STOP** operator commands. If so, ensure that the IZUSVR user ID is authorized to the appropriate resource profiles.

By default, both of the z/OSMF started tasks (IZUANG1 and IZUSVR1) run under the started task user ID, IZUSVR.

Table 332 provides more details about this migration action. Use this information to plan your changes to the system.

Table 332. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

To assign a user identity to the started tasks, you can specify a job name (JOBNAME=) on the START command. Here, the job name is used as part of the SAF resource name that is passed to the your security product. If you omit the JOBNAME= specification, the default member names will be used: IZUANG1 and IZUSVR1.

Ensure that the job name is defined in the security profiles for the started tasks. For considerations, see *IBM z/OS Management Facility Configuration Guide*.

Reference information

For information about starting the started tasks, see *IBM z/OS Management Facility Configuration Guide*.

Defining the z/OSMF started procedures to RACF

Description

When you create the new z/OSMF configuration, as described in *IBM z/OS Management Facility Configuration Guide*, you must define the z/OSMF started procedures to RACF.

Table 333 provides more details about this migration action. Use this information to plan your changes to the system.

Table 333. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

During the z/OSMF configuration process, the generated REXX exec **izuconfig1.cfg.rexx** contains RACF commands for defining the z/OSMF started procedures to the STARTED class. Figure 2 shows the commands that are provided in the exec.

```

/* Define the STARTED profiles for the z/OSMF server */
CALL RacfCmd "RDEFINE STARTED IZUSVR1.* UACC(NONE) STDATA(USER(IZUSVR)
GROUP(IZUADMIN) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))"
CALL RacfCmd "RDEFINE STARTED IZUANG1.* UACC(NONE) STDATA(USER(IZUSVR)
GROUP(IZUADMIN) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))"

```

Figure 2. RACF commands for defining the started procedures to the STARTED class

Migration actions from z/OS V1R13: z/OSMF

You can create more specific profiles to associate the started tasks with particular job names. Doing so allows you to run the started tasks under another user ID, as needed, based on job name. Use this method to control the started tasks behavior, rather than modifying the started procedures directly. Note that any user ID that is used for running the started tasks must have the same security authorizations as the started task user ID. By default, this user ID is IZUSVR.

With the STARTED class, you can modify the security definitions for started procedures dynamically, using the RDEFINE, RALTER, and RLIST commands.

Reference information

For more information about using started procedures, see *z/OS Security Server RACF Security Administrator's Guide*.

z/OSMF actions to perform after the first IPL of z/OS V2R2

This topic describes z/OSMF migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

Migrate to the new release of z/OSMF

Description

As in previous releases, migrating to the new release of z/OSMF includes running the script **izumigrate.sh**. In z/OS V2R2, this script is enhanced to create a customized IZUPRMxx parmlib member, based on the configuration settings from your current (old) system. The parmlib member replaces the interactive scripts that you used to configure z/OSMF in previous releases.

Table 130 on page 196 provides more details about this migration action. Use this information to plan your changes to the system.

Table 334. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	z/OSMF plug-ins and applications might have requirements for specific software. See each plug-in or application for its requirements.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

For ServerPac users, use the jobs and documentation supplied with your ServerPac order to create an initial instance of z/OSMF. Installations that install z/OSMF from a Custom-Built Product Delivery Option (CBPDO) software delivery package, or from a ServerPac order using the software upgrade method of installation, should follow the instructions in the migration chapter in *IBM z/OS Management Facility Configuration Guide*. This work includes running the **izumigrate.sh** script on the z/OS V2R2 system.

After you complete the ServerPac installation, you can add plug-ins to z/OSMF through the Configuration Workflow, as described in *IBM z/OS Management Facility Configuration Guide*.

Reference information

For more information, see the following references:

- For information about the ServerPac post-install jobs, see *ServerPac: Installing Your Order*.
- For information about configuring z/OSMF, see *IBM z/OS Management Facility Configuration Guide*.

Review the new z/OSMF service process

Description

In previous releases of z/OSMF, applying service sometimes required that you run the `izusetup.sh` script with the `-service` option. This action was needed to update the Enterprise Archive (EAR) files in z/OSMF.

As of z/OSMF V2R1, you are no longer required to perform this step. Instead, you need only restart the z/OSMF server. With this change, the `-service` option is deprecated and will likely be removed from z/OSMF in a future release. For instructions on applying z/OSMF service items, see the associated APAR cover letter.

Table 335 provides more details about this migration action. Use this information to plan your changes to the system.

Table 335. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, to understand that the <code>-service</code> option is no longer used.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Be aware that service installation no longer uses the `-service` option.

Reference information

For information about configuring z/OSMF, see *IBM z/OS Management Facility Configuration Guide*.

Notify users of the correct URL to use for z/OSMF

Description

When you migrate to z/OSMF in z/OS V2R2, the product URL is changed. Be sure to provide users with the new URL to use for accessing z/OSMF through a web browser. Users can add the URL to the

Migration actions from z/OS V1R13: z/OSMF

browser bookmarks list. Similarly, when the prior z/OSMF release is no longer in use at your installation, ask users to remove the URL bookmark for the prior release.

Table 336 provides more details about this migration action. Use this information to plan your changes to the system.

Table 336. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

To find the URL for z/OSMF on your system, see message IZUG349I, which was logged when you ran the **izusetup.sh** script with option **-finish** during the configuration process. This log file is in the format: `<IZU_LOGFILE_DIR>/izusetup_finish.mm.dd.yy.hh.mm.ss.tt.log`

where `<IZU_LOGFILE_DIR>` is the log file directory for your installation. By default, this directory is `/var/zosmf/configuration/logs/`.

The URL for the z/OSMF Welcome page has the following format:

`https://hostname:port/zosmf/`

where:

- *hostname* is the hostname or IP address of the system in which z/OSMF is installed
- *port* is the secure application port for the z/OSMF configuration. *port* is optional. If you specified a secure port for SSL encrypted traffic during the configuration process (through variable `IZU_HTTP_SSL_PORT`), that value is required to log in. Otherwise, it is assumed that you are using port 443, the default.

Reference information

For information about configuring z/OSMF, see *IBM z/OS Management Facility Configuration Guide*.

Recreate all table filters in the z/OSMF user interface Description

To display a subset of the items in a table in the IBM z/OS Management Facility (z/OSMF) user interface, you must define filter rules that show only the items in which you are interested. Before z/OS V2R2, the filter rules you set were saved and reapplied for subsequent views of the table. Starting with z/OS V2R2, z/OSMF provides a modern, intuitive interface that is consistent with other IBM products. The enhanced user interface does not support the filter rules that were preserved in previous z/OSMF

releases; therefore, when you display a table in z/OSMF V2R2, you might see more data or different data than you are accustomed to seeing. To show only the items in which you are interested, recreate the filter rules you set in previous releases of z/OSMF.

Table 132 on page 198 provides more details about this migration action. Use this information to plan your changes to the system.

Table 337. Information about this migration action

Element or feature:	z/OSMF
When change was introduced:	z/OS V2R2
Applies to migration from:	z/OSMF V2R1 and z/OSMF V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if users want to view only a subset of the data included in a table.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Log into the z/OSMF V2R2 user interface.
2. Navigate to the tables for which you previously set filters.
3. In the filter row in the table, click the *Filter* link. The Build Filter window is displayed.
4. In the columns field (the first field), select the name of the column to be filtered, if needed. This field lists all the columns in the table that are visible and filterable, and it includes an *Any Column* option so that you can apply the filter rule to any column in the table.
5. In the filter condition field (the second field), select the filter condition.
6. In the value field, select or specify the value for which to filter. All the fields that follow the filter condition field are value fields. The number of value fields displayed depends on the type of data being filtered and the filter condition. If a value field is enabled, a value is required.
To filter a single column for multiple values, create a separate filter rule for each value.
7. To create additional rules, click the add filter rule icon -- a plus (+) sign -- and specify the column, condition, and value for the new rule.
8. To remove a rule, click the remove rule icon -- a minus (-) sign. If the remove rule icon is disabled, the rule cannot be removed.
9. If you specified more than one filter rule, in the **Match** field, indicate whether all the rules (**All rules**) or at least one rule (**Any rule**) must be satisfied for an item to be displayed in the table. By default, **All rules** is selected.
If the **Match** field is disabled (grayed out), you cannot change the relationship between the rules. In this case, all rules must be satisfied.
10. If you want the filter criteria to be case sensitive for all the rules you specified, select **Match case**. Otherwise, case is ignored.
11. Click **Filter** to filter the table.

Migration actions from z/OS V1R13: z/OSMF

Reference information

For more information, see the following references:

- For information about configuring z/OSMF, see *IBM z/OS Management Facility Configuration Guide*.
- For information about z/OSMF tables, see the *Getting Started with z/OSMF* section in the help system that is shipped with z/OSMF.

ICKDSF (Device Support Facility)

This topic describes migration actions for the base element ICKDSF (Device Support Facility).

ICKDSF actions to perform before installing z/OS V2R2

This topic describes ICKDSF migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

ICKDSF actions to perform before the first IPL of z/OS V2R2

This topic describes ICKDSF migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

None.

ICKDSF actions to perform after the first IPL of z/OS V2R2

This topic describes ICKDSF migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

ICKDSF: Accommodate new default for INIT and REFORMAT commands

Description

The VERIFYOFFLINE parameter of the INIT and REFORMAT commands verifies that the device is offline to all other systems before the command is attempted. Beginning with ICKDSF APAR PI25913, if the UNIT parameter is specified for the INIT or REFORMAT command, and the required storage control microcode support and software support exists, and the device is not a minidisk, the VERIFYOFFLINE parameter is the default, meaning that verification that the device is offline occurs even if VERIFYOFFLINE is not specified. Prior to ICKDSF APAR PI25913, verification occurred only when VERIFYOFFLINE was specified.

If the VERIFYOFFLINE parameter is processed as the default, and the device is online to another system, the command terminates, with message ICK31306I in the job output.

To request that verification not take place, you can use a new NOVERIFYOFFLINE parameter.

Note: The VERIFYOFFLINE parameter of the INIT and REFORMAT commands was introduced by ICKDSF APAR PM76231

Table 133 on page 199 provides more details about this migration action. Use this information to plan your changes to the system.

Table 338. Information about this migration action

Element or feature:	ICKDSF
---------------------	--------

Table 338. Information about this migration action (continued)

When change was introduced:	APAR PI25913 (on ICKDSF R17) for both z/OS V2R1 and z/OS V1R13.
Applies to migration from:	z/OS V2R1 and z/OS V1R13 (on ICKDSF R17), both without APAR PI25913.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you require that the new default not be used.
Target system hardware requirements:	DS8870 R7.1 GA, Bundle 87.10.87.0, LIC 7.7.10.287 DS8700 R6.3 SP6, Bundle 76.31.79.0, LIC 6.6.31.670 DS8800 R6.3 SP6, Bundle 86.31.95.0, LIC 7.6.31.1150
Target system software requirements:	The software support is provided in APAR OA40719 for z/OS V2R1 and V1R13, and incorporated into z/OS V2R2.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	If the VERIFYOFFLINE parameter is specified either explicitly or by default, and the device is online to any other systems, message ICK31306I VERIFICATION FAILED: DEVICE FOUND TO BE GROUPED is issued and the command is terminated. If the NOVERIFYOFFLINE parameter is specified and the device is online, command processing continues.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you do not want INIT and REFORMAT commands with the UNIT parameter to verify that the device is offline to all other systems before the command is attempted, add the new NOVERIFYOFFLINE parameter to those commands.

Reference information

For more information, see the descriptions of the INIT and REFORMAT commands in *Device Support Facilities (ICKDSF) User's Guide and Reference*.

Infoprint Server migration actions

This topic describes migration actions for optional feature Infoprint Server.

Infoprint Server actions to perform before installing z/OS V2R2

This topic describes Infoprint Server migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Discontinue use of the Infoprint Server SNMP subagent Description

In z/OS V2R2, the Simple Network Management Protocol (SNMP) subagent is no longer provided with Infoprint Server, so you must take steps to stop using it. The SNMP subagent lets network management systems (such as Ricoh Network Printer Manager for the web) communicate with PSF-controlled printers that do not have internal SNMP agents. However, because most newer printers contain internal SNMP agents, network management systems can communicate directly with these printers.

Migration actions from z/OS V1R13: Infoprint Server

As an alternative to using a network management system to monitor PSF-controlled printers, you can use Infoprint Central, a web-based print management system. Infoprint Central can display the status of all your PSF-controlled printers. In addition, Infoprint Central lets you stop and start the printers, change printer work-selection criteria, and turn TCP/IP-connected printers online and offline.

Table 134 on page 201 provides more details about this migration action. Use this information to plan your changes to the system.

Table 339. Information about this migration action

Element or feature:	z/OS Infoprint Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use the SNMP subagent. You are using the SNMP subagent if the start-daemons={snmpd} attribute is specified in the Infoprint Server configuration file. The configuration file's default location is <code>/etc/Printsrv/aopd.conf</code> . However, you might have specified a different location in environment variable <code>AOPCONF</code> in the aopstart EXEC.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. If you use a network management system to monitor PSF-controlled printers, do one of these:
 - Configure the network management system to communicate with the printers directly.
 - Use Infoprint Central to manage the printers. To use Infoprint Central, you must customize PSF to use the Infoprint Server Printer Inventory.
2. Stop the SNMP subagent daemon:
 - a. (Optional) Edit the Infoprint Server configuration file (`aopd.conf`) to remove the **snmp** value from the **start-daemons** attribute. This step is optional because Infoprint Server will ignore the **snmp** value.
 - b. If Infoprint Server is running, stop the SNMP subagent daemon (**aopsnmpd**). For example, enter this MVS START command to run the AOPSTOP procedure to stop daemon **aopsnmpd**:

```
START AOPSTOP,OPTIONS='-d snmpd'
```

Reference information

For more information, see the following references:

- How to edit the Infoprint Server configuration file (`aopd.conf`) and how to customize Infoprint Central, see *z/OS Infoprint Server Customization*.
- How to use Infoprint Central and how to stop Infoprint Server daemons, see *z/OS Infoprint Server Operation and Administration*.

Upgrade web browser support for Infoprint Central

Description

In z/OS V2R2, the Infoprint Central component of Infoprint Server requires Microsoft Internet Explorer 9.0 or later or Mozilla Firefox 24 ESR or later.

Table 135 on page 202 provides more details about this migration action. Use this information to plan your changes to the system.

Table 340. Information about this migration action

Element or feature:	z/OS Infoprint Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use Infoprint Central.
Target system hardware requirements:	None.
Target system software requirements:	<p>If you use Infoprint Central to work with IP PrintWay extended mode print jobs and printers, you need:</p> <ul style="list-style-type: none"> • IBM HTTP Server - Powered by Apache base element of z/OS • The XML Toolkit for z/OS V1.10 (5655-J51) • One of these Java products: <ul style="list-style-type: none"> – IBM 31-bit SDK for z/OS, Java Technology Edition, V7.1 (5655-W43) – IBM 64-bit SDK for z/OS, Java Technology Edition, V7.1 (5655-W44) • Microsoft Internet Explorer 9.0 or later or Mozilla Firefox 24 ESR or later
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Install Microsoft Internet Explorer 9.0 or later, or Mozilla Firefox 24 ESR or later.

Reference information

For more information, see *z/OS Infoprint Server Operation and Administration* describes how to start and stop Infoprint Server and how to use Infoprint Central.

Upgrade Java support for IPP Server and Infoprint Central

Description

In z/OS V2R2, the Internet Printing Protocol (IPP) Server used in Infoprint Server and Infoprint Central require Java V7.1. If the JAVA_HOME environment variable specifies the location of an earlier version of Java, you must update the JAVA_HOME environment variable.

Table 136 on page 203 provides more details about this migration action. Use this information to plan your changes to the system.

Migration actions from z/OS V1R13: Infoprint Server

Table 341. Information about this migration action

Element or feature:	z/OS Infoprint Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use IPP Server or Infoprint Central and specify the JAVA_HOME environment variable. You are using IPP Server if start-daemons={ippd} is specified in the Infoprint Server configuration file. You are using Infoprint Central if the start-daemons={ssid} attribute is specified in the Infoprint Server configuration file. The configuration file's default location is /etc/Printsrv/aopd.conf. However, you might have specified a different location in environment variable AOPCONF.
Target system hardware requirements:	None.
Target system software requirements:	IBM 31-bit SDK for z/OS, Java Technology Edition, V7.1 (5655-W43); Infoprint Central can also use IBM 64-bit SDK for z/OS, Java Technology Edition, V7.1 (5655-W44).
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	z/OS V2R1 and V1R13 Infoprint Server will not operate with IBM HTTP Server - Powered by Apache. After you install z/OS V2R2, you must change the configuration of the z/OS V2R2 Infoprint Server to operate with IBM HTTP Server - Powered by Apache, which is included in z/OS V2R2 as a base element.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Install IBM 31-bit SDK for z/OS, Java Technology Edition, V7.1 (5655-W43) or IBM 64-bit SDK for z/OS, Java Technology Edition, V7.1 (5655-W44). IPP Server requires the 31-bit version of Java V7.1.
2. If you use the IPP Server, edit the **aopstart** EXEC to update the directory path specified in the JAVA_HOME environment variable to /usr/lpp/java/J7.1 or wherever you specified the location.

Note: If you installed Java V7.1 in the default Java directories, you do not need to specify the JAVA_HOME environment variable. If JAVA_HOME is not specified, IPP Server or Infoprint Central looks for Java files in the /usr/lpp/java/J7.1 directory.

Reference information

For more information, see the following references:

- For information about editing the **aopstart** EXEC, see *z/OS Infoprint Server Customization*.
- For information about Java products, see the Java Standard Edition Products on z/OS page: <http://www.ibm.com/systems/z/os/zos/tools/java/>.

Infoprint Server actions to perform before the first IPL of z/OS V2R2

This topic describes Infoprint Server migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Discontinue use of Infoprint Server **aophinvd**, **aoplogd**, and **aopsdbd** daemons

Description

In z/OS V2R2, the following daemons are no longer provided with Infoprint Server:

aophinvd

Historical Inventory daemon.

aoplogd

Common message log daemon.

aopsdbd

Search database daemon.

The functions that are previously provided by the **aophinvd**, **aoplogd**, and **aopsdbd** daemons are now performed by the **aopd** daemon. You do not need to take any steps to update your Infoprint Server configuration. However, if you use an automation product to monitor daemons, you might need to make configuration changes to the product.

Table 137 on page 204 provides more details about this migration action. Use this information to plan your changes to the system.

Table 342. Information about this migration action

Element or feature:	z/OS Infoprint Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use an automation product that monitors the aophinvd , aoplogd , and aopsdbd daemons, you need to make configuration changes for the product.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	You might see an increase in CPU consumption for the aopd daemon because it now handles additional workload from the removed daemons.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you use an automation product that monitors the **aophinvd**, **aoplogd**, and **aopsdbd** daemons, remove the daemons from your product configuration.

Reference information

For more information, see the following references:

- *z/OS Infoprint Server Customization.*

Migration actions from z/OS V1R13: Infoprint Server

- *z/OS Infoprint Server Operation and Administration.*
- *z/OS Infoprint Server Printer Inventory for PSF.*

Remount the Printer Inventory and copy files that were customized Description

When you migrate to the latest z/OS system, you must bring forward the customized data from your previous system.

Table 138 on page 205 provides more details about this migration action. Use this information to plan your changes to the system.

Table 343. Information about this migration action

Element or feature:	z/OS Infoprint Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

aopstart EXEC

If you modified the **aopstart** EXEC, copy it to the z/OS V2R2 system.

Configuration file

If you are using the ServerPac Full System Replace option and you have modified the Infoprint Server configuration file, copy the file to the z/OS V2R2 system. Its default location is `/etc/Printsrv/aopd.conf`. However, you might have specified a different location in environment variable `AOPCONF`.

Infoprint Central

When you are customizing the new script **bin/envvars** for IBM HTTP Server - Powered by Apache, you might want to refer to the old z/OS HTTP Server environment variables file as a reference. By default, the file was located at `/etc/httpd.envvars`.

IP PrintWay

If you currently use the IP PrintWay component of Infoprint Server, copy to the z/OS V2R2 system any IP PrintWay exit routines and data stream filters you have written. It is a good practice to recompile the exits and filters on z/OS V2R2.

NetSpool

If you currently use the NetSpool component of Infoprint Server, copy to the z/OS V2R2 system any NetSpool exit routines you have written. It is a good practice to recompile the exits and filters on z/OS V2R2.

Printer Inventory

Migration actions from z/OS V1R13: Infoprint Server

- Remount the /var/Printsrv directory from the earlier system on the z/OS V2R2 system. The /var/Printsrv directory contains the Printer Inventory as well as other Infoprint Server files. The default directory is /var/Printsrv. However, you might have changed the directory name in the base-directory attribute in the aopd.conf configuration file.

Notes:

1. After you start Infoprint Server on the z/OS system, you should use the Infoprint Server **pidu** command to export the Printer Inventory on the z/OS V2R2 system so that you have a backup of the Printer Inventory.
 2. If /var/Printsrv is not mounted at a separate mount point, use the Infoprint Server **pidu** command to export the Printer Inventory on the original system; restore it on the z/OS V2R2 system after the first IPL. Do not use other copy commands to copy the Printer Inventory. (Mounting /var/Printsrv at a separate mount point can result in better management of disk space and easier migration.)
- Configure the Infoprint Server environment variables (for example, AOPCONF, PATH, LIBPATH, NLSPATH, MANPATH) in /etc/profile.

Print Interface

If you currently use the Print Interface component of Infoprint Server, take these actions:

- If you have written any data stream filters, copy them to the z/OS V2R2 system. You do not need to recompile them.
- If you run the SAP R/3 application server on the z/OS system, copy the SAP callback daemon configuration file to the z/OS V2R2 system. Its default location is /etc/Printsrv/aopsapd.conf. However, you might have specified a different location in environment variable AOPSAPD_CONF.

Reference information

For more information, see *z/OS Infoprint Server Customization*.

Infoprint Server actions to perform after the first IPL of z/OS V2R2

This topic describes Infoprint Server migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

Run aopsetup

Description

When migrating to z/OS V2R2 Infoprint Server, you must run the **aopsetup** shell script to establish the correct file permissions for Infoprint Server directories and files.

Table 139 on page 206 provides more details about this migration action. Use this information to plan your changes to the system.

Table 344. Information about this migration action

Element or feature:	z/OS Infoprint Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.

Migration actions from z/OS V1R13: Infoprint Server

Table 344. Information about this migration action (continued)

Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Run the **aopsetup** shell script from an **rlogin** shell, from an OMVS session, or with the BPXBATCH command. Specify the names of the RACF groups that you defined for Infoprint Server operators and administrators as arguments to **aopsetup**. For example, if you defined group AOPOPER for operators and group AOPADMIN for administrators, enter:

```
/usr/lpp/Printsrv/bin/aopsetup AOPOPER AOPADMIN
```

Rule: You must run **aopsetup** from a user ID with a UID of 0. You can use the **su** command to switch to an effective UID of 0 if you have READ access to the BPX.SUPERUSER profile in the RACF FACILITY class.

Tip: You can run **aopsetup** from the driving system (instead of the target system) if all of these are true:

- You have the target system's /var/Printsrv directory accessible.
- You reference the target system's /usr/lpp/Printsrv directory mounted under a /service directory as described in the comments at the beginning of the **aopsetup** shell script.
- The RACF database groups for operators and administrators are the same on the driving and target system.

Reference information

For information about running **aopsetup**, see *z/OS Infoprint Server Customization*.

Configure IBM HTTP Server - Powered by Apache Description

In z/OS V2R1 and earlier versions, the Infoprint Central component of Infoprint Server was designed to work only with the IBM HTTP Server powered by Domino. In z/OS V2R2, IBM removed support for IBM HTTP Server powered by Domino and only IBM HTTP Server - Powered by Apache, a base element of z/OS V2R2, is supported. You must now use the IBM HTTP Server powered by Apache 31-bit.

Table 140 on page 207 provides more details about this migration action. Use this information to plan your changes to the system.

Table 345. Information about this migration action

Element or feature:	z/OS Infoprint Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use the Infoprint Central component of Infoprint Server. You are using Infoprint Central if start-daemons={ssid} is specified in the Infoprint Server configuration file, which has a default location of /etc/Printsrv/aopd.conf. However, you might have specified a different location in environment variable AOPCONF in the aopstart EXEC.
Target system hardware requirements:	None.

Table 345. Information about this migration action (continued)

Target system software requirements:	IBM HTTP Server - Powered by Apache.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

See “Customizing IBM HTTP Server - Powered by Apache” in *z/OS Infoprint Server Customization*.

Reference information

For information about how to configure Infoprint Server and Infoprint Central, see *z/OS Infoprint Server Customization*.

Integrated Security Services migration actions

This topic describes migration actions for base element Cryptographic Services. Included are the components Enterprise Identity Mapping (EIM), Network Authentication Service for z/OS, and Open Cryptographic Enhanced Plug-ins (OCEP).

Integrated Security Services actions to perform before installing z/OS V2R2

This topic describes Integrated Security Services migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

Integrated Security Services actions to perform before the first IPL of z/OS V2R2

This topic describes Integrated Security Services migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

NAS: Allow GSS-API application programs to access the CSFRNG resource of the CSFSERV class

Description

GSS-API applications that use either the LIPKEY or SPKM mechanism call System SSL APIs and trigger System SSL DLLs to be loaded. Starting in z/OS V2R1, when System SSL DLLs are loaded, it uses ICSF random number generation support if ICSF is available. If the context initiator (client) or context acceptor (server) in these mechanisms does not have access to the CSFRNG resource of the CSFSERV class, ICH408I (which indicates insufficient authorization) might be issued to the console, but the application continues. The System SSL software implementation is used instead.

Table 346 on page 440 provides more details about this migration action. Use this information to plan your changes to the system.

Migration actions from z/OS V1R13: Integrated Security Services

Table 346. Information about this migration action

Element or feature:	Network Authentication Service
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before first IPL of z/OS V2R2.
Is the migration action required?	Yes, if the following conditions are true: <ul style="list-style-type: none">• Your installation uses ICSF.• The CSFSERV general resource class is active.• A profile that covers the CSFRNG resource of the CSFSERV class is defined and does not grant READ access to the user IDs that use the LIPKEY or SPKM mechanism.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	The system issues informational message ICH408I that indicates insufficient authorization might be issued to the console.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Determine whether the CSFSERV class is active. When active, this class restricts access to the ICSF programming interface. If it is not active, access to the ICSF programming interface (and specifically the CSFRNG callable service) is unrestricted. No configuration is necessary.

To determine which RACF classes are currently active, enter the SETROPTS command with the LIST parameter specified:

```
SETROPTS LIST
```

- If the SETROPTS LIST command shows that the CSFSERV class is active, identify the profile that covers the CSFRNG resource. This might be a discrete profile named CSFRNG or, if generic profile checking is activated, a generic profile.

To determine whether a profile is defined to protect the CSFRNG resource, enter the following RLIST command:

```
RLIST CSFSERV CSFRNG
```

When you enter this command, RACF lists information for the discrete resource profile CSFRNG. If there is no matching discrete profile, RACF lists the generic profile that most closely matches the resource name.

- If the RLIST command output reveals that there is a discrete or generic profile defined that covers the CSFRNG resource, examine the command output to ensure that the GSS-API context initiator (client) and acceptor (server) user IDs that use either the SPKM or LIPKEY mechanisms have at least READ access to the CSFRNG resource. If necessary, use the PERMIT command to give them the appropriate access. For example, if a discrete profile CSFRNG exists, the following command would give user BAILEY access:

```
PERMIT CSFRNG CLASS(CSFSERV) ID(BAILEY) ACCESS(READ)
```

If you do make changes, refresh the in-storage RACF profiles for the CSFSERV class:

```
SETROPTS RACLIST(CSFSERV) REFRESH
```

Reference information

For more information, see “Using Cryptographic Features with System SSL” in *z/OS Cryptographic Services System SSL Programming*.

Integrated Security Services actions to perform after the first IPL of z/OS V2R2

This topic describes Integrated Security Services migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

JES2 migration actions

This topic describes migration actions for base element JES2.

JES2 actions to perform before installing z/OS V2R2

This topic describes JES2 migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Change JESJOBS profiles

Description

In z/OS V2R1, the new Job Modify SSI 85 defines additional resource names to the JESJOBS class. If any existing JESJOBS entity name matches one of the new resource names, it could result in unintended user authorization to modify job attributes. If necessary, update your JESJOBS profiles to avoid granting unintended user authority to modify jobs.

Table 347 provides more details about this migration action. Use this information to plan your changes to the system.

Table 347. Information about this migration action

Element or feature:	z/OS JES2.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if JESJOBS profiles could grant unintended authority to modify the job.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Search for JESJOBS profile names which match any of the new JESJOBS resource names:

Migration actions from z/OS V1R13: JES2

- SUBMIT.localnodeid.jobname.userid
- HOLD.nodename.userid.jobname
- RELEASE.nodename.userid.jobname
- PURGE.nodename.userid.jobname
- CANCEL.nodename.userid.jobname
- START.nodename.userid.jobname
- RESTART.nodename.userid.jobname
- SPIN.nodename.userid.jobname
- MODIFY.nodename.userid.jobname
- REROUTE.nodename.userid.jobname

For more information, see *z/OS JES2 Initialization and Tuning Guide*.

2. Ensure that your existing JESJOBS profiles grant the intended authority, given the new use of JESJOBS by the Job Modify SSI 85.
3. If any JESJOBS profile inadvertently allows user authority to Job Modify SSI 85 actions, update the profile or create a new profile, if necessary.

Reference information

For more information, see the following references:

- *z/OS JES2 Initialization and Tuning Guide*
- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Planning for Multilevel Security and the Common Criteria*

Activate z11 mode

Description

JES2 z/OS V2R1 is the last release level that will support z2 checkpoint mode. JES2 must be activated to z11 mode before migrating to z/OS V2R2. Activating z11 mode upgrades the JES2 checkpoint and enables JES2 function that is introduced in z/OS V1R11, including JOE data area extensions supported by BERTs. For more information on the JES2 functionality introduced in z/OS V1R11, see “Reference information” on page 209.

Table 141 on page 208 provides more details about this migration action. Use this information to plan your changes to the system.

Table 348. Information about this migration action

Element or feature:	JES2.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	You are able to fall back to z2 mode, if necessary, prior to z/OS V2R2. After z/OS V2R2, you cannot fall back to z2 mode.
System impacts:	None.

Table 348. Information about this migration action (continued)

Related IBM Health Checker for z/OS check:	Use check JES2_Z11_Upgrade_CK_JES2 to determine if your system is ready to upgrade the JES2 checkpoint to z11 mode. For more information, see <i>IBM Health Checker for z/OS User's Guide</i> .
--	---

Steps to take

Follow these steps:

- After migrating to z/OS V1R11 JES2, or later, on all systems in your MAS, determine your z11 checkpoint activation readiness:
 1. Use the **\$D ACTIVATE** command. This command indicates if activation to z11 mode will succeed.
 2. Review your current utilization of BERT data to determine if there are sufficient BERTS, as detailed in “Check BERT utilization” on page 209.
 3. If you issue the **\$ACTIVATE,LEVEL=z11** command, activation of LARGEDS support is required.
 4. An additional *mmm* 4K records for CKPT1 is required for z11 mode.
- Run the **JES2 \$ACTIVATE** command to verify non-configuration changes that must be accommodated before going to z11, and to activate z11 mode following the considerations for this command found in *z/OS JES2 Commands*.

Note: The SPOOLDEF LARGEDS=FAIL (default value) in JES2PARM parmlib member is not supported in z11 mode. In z11 mode, on a COLD start, JES2 defaults to LARGEDS=ALLOWED. However, you cannot issue the **\$ACTIVATE,LEVEL=z11** command in the environment of SPOOLDEF LARGEDS=FAIL.

By default, JES2 V1R13 and V2R1 restart in the same mode (z2 or z11) as other members of the MAS (if any are active) or the mode the last active JES2 member was in when it came down. To restart JES2 in z2 mode, specify UNACT on PARM=. On a cold start, JES2 starts in z11 mode unless overridden by OPTSDEF COLD_START_MODE or UNACT parameter.

Reference information

For more information, see the following references:

- For a list of the enhancements introduced in z/OS V1R11 for z11 mode, see *z/OS Introduction and Release Guide*.
- For **\$ACTIVATE**, **\$D ACTIVATE**, **\$D CKPTSPACE** and **\$JD HISTORY** command details, see *z/OS JES2 Commands*.

Check BERT utilization: Before issuing the **\$ACTIVATE,LEVEL=z11** command, review the current utilization of BERT data to determine whether there are sufficient BERTs. Additional BERTs are needed for each SYSOUT data set that has transaction data associated with it. These SYSOUT data sets can be seen using SDSF by setting APPC ON and examining SYSOUT data sets on the H and O panels; SYSOUT data sets with transaction data have nontraditional JES2 job IDs. Consider increasing the number of BERTs to correspond to two times the maximum number of transaction SYSOUT data sets on the system. BERT utilization should be monitored after the **\$ACTIVATE** to z11 mode to ensure there are sufficient BERTs for the jobs and SYSOUT in the MAS. There are several ways to determine your current BERT usage.

- The **\$D CKPTSPACE,BERTUSE** command displays a table of the types of control blocks in BERTs and how many BERTs are used by each control block type. The example shows the output of the command:

```

$HASP852 CKPTSPACE  CURRENT BERT UTILIZATION
$HASP852          TYPE           COUNT  CB COUNT
$HASP852          -----  -----
$HASP852          INTERNAL           11          1

```

Migration actions from z/OS V1R13: JES2

\$HASP852	JQE	211	108
\$HASP852	CAT	114	38
\$HASP852	WSCQ	1	1
\$HASP852	DJBQ	0	0
\$HASP852	JOE	0	0
\$HASP852	FREE	763	0

In the example, there are 108 JQEs that have a total of 211 BERTs associated with them. This example is for a system in z2 mode and does not have any BERTs associated with JOEs.

- The \$D ACTIVATE command displays the number of BERTs that are needed for activation to z11 mode. This is the number of BERTs that will be associated with JOEs after the \$ACTIVATE. The example shows the output of the \$D ACTIVATE command:

```
$HASP895 $DACTIVATE
$HASP895 JES2 CHECKPOINT MODE IS CURRENTLY Z2
$HASP895 THE CURRENT CHECKPOINT:
$HASP895 -- CONTAINS 1100 BERTS AND BERT UTILIZATION IS 30
$HASP895 PERCENT.
$HASP895 -- CONTAINS 158 4K RECORDS.
$HASP895 z11 CHECKPOINT MODE ACTIVATION WILL:
$HASP895 -- EXPAND CHECKPOINT SIZE TO 165 4K RECORDS.
$HASP895 -- REQUIRE 22 ADDITIONAL BERTS AND UTILIZATION
$HASP895 WOULD REACH 32 PERCENT.
$HASP895 z11 ACTIVATION WILL SUCCEED IF ISSUED FROM THIS MEMBER.
```

In the example, there are 22 additional BERTs that will be used after the \$ACTIVATE to z11 mode, for transaction data associated with JOEs.

Note: When the SPOOLDEF LARGEDS=FAIL (default value) is in effect in your JES2PARM parmlib member, the following message will be issued by the \$ACTIVATE command:

```
$HASP895 z11 ACTIVATION WILL FAIL IF ISSUED FROM THIS MEMBER.
$HASP895 THE FOLLOWING ISSUES PREVENT ACTIVATION:
$HASP895 -- LARGEDS SUPPORT MUST BE ACTIVATED.
```

- A general history of BERT usage can be obtained by using the \$JD HISTORY(BERT) command or by using the SDSF RM panel. This displays the usage of BERTs after the system was IPLed. The following example shows the output of the \$JD HISTORY(BERT) command:

```
$HASP9130 D HISTORY
$HASP9131 JES2 BERT      USAGE HISTORY
DATE      TIME          LIMIT  USAGE    LOW    HIGH  AVERAGE
-----
2009.086 16:00:00    1100    337    337    337    337
2009.086 15:50:09    1100    337    125    337    192
```

JES2 actions to perform before the first IPL of z/OS V2R2

This topic describes JES2 migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Review changes applicable to JES2 exits

Description

In z/OS V2R2, exit changes might be necessary, depending on which exits you are using and which JES2 data areas those exits are referencing.

Table 142 on page 210 provides more details about this migration action. Use this information to plan your changes to the system.

Table 349. Information about this migration action

Element or feature:	z/OS JES2.
---------------------	------------

Table 349. Information about this migration action (continued)

When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have any affected JES2 exits.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

See the "JES2 migration details" section of *z/OS JES2 Installation Exits*. This section details the changed information which you might need to accommodate. Generally, assembly errors in JES2 exits indicate that you were affected by a JES2 data area change.

Reference information

For more information, see *z/OS JES2 Installation Exits*.

Remove BRODCAST= from the OUTDEF initialization statement

Description

In z/OS V2R1, JES2 ignores any specifications of the BRODCAST= parameter on the OUTDEF initialization statement. If a TSO user is not currently logged on, notify messages are now issued locally (processing as with BRODCAST=YES) instead of being routed to the member that submitted the job (processing as with BRODCAST=NO). You can no longer use BRODCAST= to specify which member issues TSO notify messages when a user is not logged on. BRODCAST= specifications continue to have no effect on message processing when the TSO user is logged on.

Table 350 provides more details about this migration action. Use this information to plan your changes to the system.

Table 350. Information about this migration action

Element or feature:	z/OS JES2.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	No, but recommended to keep your initialization deck clean of outdated and obsolete specifications.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Migration actions from z/OS V1R13: JES2

Steps to take

Follow these steps:

1. Check the OUTDEF statement in the JES2 initialization deck for BROADCAST= specifications.
2. Remove BROADCAST= specifications from the OUTDEF statement. Any value that you provide on BROADCAST= will be ignored. The system will issue notify messages for a TSO user that is not logged on, on the member that requested the message. The message will be placed in the broadcast data set by TSO on that member.

Reference information

For more information, see the following references:

- *z/OS JES2 Messages*
- *z/OS JES2 Initialization and Tuning Reference*
- *z/OS JES2 Diagnosis*.

Remove JCLERR= from the JOBDEF initialization statement

Description

Before z/OS V2R1, for JCL job card errors that were detected during the input phase that the converter also detected, you could either have JES2 fail the job during input phase (JCLERR=YES) and the job never was sent to conversion, or you could have JES2 ignore the errors (JCLERR=NO) and send the job to the conversion phase where the converter could detect them. Starting with z/OS V2R1, input phase still detects errors, but jobs are always queued to the conversion phase and the input errors are added to those found by conversion and reported in the same way. The message id associated with the message indicates where the error occurred.

In z/OS V2R2, JES2 ignores any specifications of the JCLERR= parameter. If an error on the JOB card is encountered during the INPUT phase, the job is sent to the converter for INPUT phase error message processing. You can no longer use JCLERR=YES to specify for the job to be failed under these conditions.

Table 351 provides more details about this migration action. Use this information to plan your changes to the system.

Table 351. Information about this migration action

Element or feature:	z/OS JES2.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	No, but recommended to keep your initialization deck clean of outdated and obsolete specifications.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Check the JOBDEF statement in the JES2 initialization deck for JCLERR= specifications.
2. Remove any JCLERR= specifications from the JOBDEF statement.

Notes:

1. With JES2 APAR OA41881, the output message \$HASP835 from \$DJOBDEF command no longer displayed the JCLERR=YES or JCLERR=NO value.
2. With JES2 APAR OA46199, JES2 now checks the value of a NOTIFY=&SYSUID specification on a JOB statement. If &SYSUID translates to what JES2 considers to be a special local route code (values of the form *Unmmn*), JES2 generates a JCL error, causing the job to fail. Prior to the APAR, JES2 did not check whether the &SYSUID variable resolved to a special local route code. The specification was accepted, but ignored. No notification was generated and the error was not flagged.

Reference information

For more information, see the following references:

- *z/OS JES2 Messages*
- *z/OS JES2 Initialization and Tuning Reference*
- *z/OS JES2 Diagnosis*
- *z/OS JES2 Commands*

JES2 actions to perform after the first IPL of z/OS V2R2

This topic describes JES2 migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

JES3 migration actions

This topic describes migration actions for optional feature JES3.

JES3 actions to perform before installing z/OS V2R2

This topic describes JES3 migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

JES3 actions to perform before the first IPL of z/OS V2R2

This topic describes JES3 migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Change JES3 release level format

Description

In z/OS V2R1 SSI 54, SSI 82, and SSI 83 report the JES3 release level using the JES2 format z/OS 2.1. In previous versions of z/OS, JES3 reported the release level using the format z 1.13.0. The SSI fields which are affected by the format change are:

- SSI 54: SSVIVERS field from macro IEFSSVI

Migration actions from z/OS V1R13: JES3

- SSI 82: JPXVERSN field from macro IAZJPLEX
- SSI 83: JPSYVERN field from macro IAZJPLXI.

Table 352 provides more details about this migration action. Use this information to plan your changes to the system.

Table 352. Information about this migration action

Element or feature:	z/OS JES3.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if code is dependent on the JES3 release level returned by SSI 54, SSI 82 or SSI 83.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Search for fields SSVIVERS, JPXVERSN and JPSYVERN in invocations of SSI 54, SSI 82 and SSI 83.
2. For any code that requires the z/OS 2.1 JES3 release level, change the expected format to 'z/OS 2.1' (z/OS #.#).

Reference information

For more information, see *z/OS MVS Using the Subsystem Interface*.

Remove DUMP=JES and DUMP=MVS from the OPTIONS initialization statement Description

For enhanced problem determination and availability in z/OS V2R1, JES3 has dropped support for the DUMP=JES and DUMP=MVS parameter specifications on the OPTIONS initialization statement. In z/OS V2R1, DUMP=PRDMP is the default value and the only supported DUMP parameter specification.

Table 353 provides more details about this migration action. Use this information to plan your changes to the system.

Table 353. Information about this migration action

Element or feature:	z/OS JES3.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R1.

Table 353. Information about this migration action (continued)

Is the migration action required?	No, but recommended to avoid warning messages. Any references to unsupported values are ignored, DUMP=PRDMP is used, a message is issued and initialization continues. For example, if DUMP=JES or DUMP=MVS is specified, the system issues one of the following messages, and JES3 initialization continues: IAT3255 WARNING: JES IS INVALID FOR KEYWORD DUMP, DEFAULT PRDUMP IS BEING USED IAT3255 WARNING: MVS IS INVALID FOR KEYWORD DUMP, DEFAULT PRDUMP IS BEING USED
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Check the OPTIONS statement in the JES3 initialization deck for DUMP=JES and DUMP=MVS specifications.
2. Remove the DUMP=JES and DUMP=MVS specifications from the OPTIONS statement, or change the values to DUMP=PRDMP.

Reference information

For more information, see the following references:

- *z/OS JES3 Initialization and Tuning Reference*
- *z/OS JES3 Messages*
- *z/OS JES3 Commands*
- *z/OS JES3 Diagnosis Reference*

Remove SDI from the OPTIONS initialization statement

Description

In z/OS V2R1, JES3 has removed the option to turn off Spool Data Integrity (SDI) functionality. If JES3 encounters the SDI keyword, command processing stops and a message is issued.

If SDI is specified in the inish deck, the system issues the following message, and JES3 initialization continues: IAT3256 SDI KEYWORD IGNORED, NO LONGER SUPPORTED. If SDI is used on a command (*F Q,SDI=), the system issues the following message, and the command is aborted: IAT8050 SDI IS AN INVALID FIELD.

Table 354 on page 450 provides more details about this migration action. Use this information to plan your changes to the system.

Migration actions from z/OS V1R13: JES3

Table 354. Information about this migration action

Element or feature:	z/OS JES3.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	No, but recommended to avoid warning messages and command errors.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Remove the SDI keyword from the OPTIONS statement in the JES3 initialization deck.
2. Remove or update any automated instances of the *F Q and *I Q commands that specify the SDI parameter.

Reference information

For more information, see the following references:

- *z/OS JES3 Initialization and Tuning Reference*
- *z/OS JES3 Messages*
- *z/OS JES3 Commands*
- *z/OS JES3 Diagnosis Reference*

Be aware that JES3 honors the DSI setting in SCHEDxx Description

Before z/OS V2R2, if data set integrity (DSI) was specified for the JES3 programs IATINTK or IATINTKF in your SCHEDxx parmlib member, ENQs would occur, but only for batch allocation of JES3 data sets that were identified in the JES3 start procedure with DD statements. If you did not specify IATINTK or IATINTKF in SCHEDxx, no ENQs would occur. The reason is that the value of NODSI for IATINTK and IATINTKF is coded in the IBM-supplied Program Properties Table (PPT, or IEFSDPPT). NODSI remains coded in IEFSDPPT in z/OS V2R2, as was done in previous releases.

Starting with z/OS V2R2, if you override the IBM-supplied PPT with a SCHEDxx entry of DSI for IATINTK or IATINTKF, ENQs occur for batch allocations of JES3 data sets identified in the JES3 start procedure with DD statements (as in previous releases). In addition, JES3 now also obtains ENQs for all dynamic allocations of JES3 data sets.

It is recommended that you take advantage of DSI protection by specifying DSI for IATINTK and IATINTKF in your SCHEDxx member. The SCHEDxx default when you specify a program name, is that the program name has DSI. Thus, if you do not specify any DSI value (DSI or NODSI) for a SCHEDxx program name, the program receives DSI protection. Therefore, it is recommended that you explicitly code a value of DSI in the SCHEDxx member for IATINTK and IATINTKF to avoid any confusion over which value is being used.

You can use the following PPT statements to add the DSI specification to SCHEDxx and maintain the attributes from the IBM-supplied default entries:

```
PPT PGMNAME(IATINTK) NOCANCEL NOSWAP SYST DSI KEY(1) NOHONORIEFUSIREGION
PPT PGMNAME(IATINTKF) NOSWAP SYST DSI KEY(1)
```

Table 143 on page 212 provides more details about this migration action. Use this information to plan your changes to the system.

Table 355. Information about this migration action

Element or feature:	JES3
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you previously set DSI in the SCHEDxx member; JES3 was ignoring it for dynamic allocations. When z/OS V2R2 is started, an ENQ results from the allocations, which might lead to unexpected consequences. It is recommended that you use DSI to prevent accidental damage to your data sets due to the lack of an ENQ.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	Use IBM Health Checker for z/OS check IBMJES3,JES3_DATASET_INTEGRITY, which determines whether DSI or NODSI is specified on the JES3 entries in the program properties table (PPT). The check generates an exception message when the current DSI setting does not match the specified setting. This check is provided as of z/OS V2R2.

Steps to take

Follow these steps:

- If you use DD allocations in your JES3 start procedure (not recommended), ensure that the DISP keyword specifies SHR, not OLD. Otherwise, the first JES3 that comes up locks out other JES3 address spaces in the same sysplex. All dynamic allocations by JES3 use DISP=SHR.
- Because an ENQ is held on the data set names, it is recommended that you use unique spool data set names to allow for offline allocation, unallocation, and formatting. Check your JES3 start procedure and your DSN specification on the DYNALLOC statement in your inish deck for duplicate names.

Reference information

For more information, see *z/OS MVS Initialization and Tuning Reference*.

JES3 actions to perform after the first IPL of z/OS V2R2

This topic describes JES3 migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

Migration actions from z/OS V1R13: JES3

Check code that references the JES3 Locate Response control block in IATYLRS Description

Starting with z/OS V2R2, the JES3 macro IATYLRS fixed entry is extended to support new generation data group (GDG) limits greater than 255. This change allows up to 999 active GDSs. The new format is called GDG Extended (GDGE). To support 999 active GDSs, the size of a JES3 Locator Response (LRS) fixed entry is extended and a new 2-byte GDG limit field is added.

Flag byte LRSFLG2 contains a new flag that indicates when an LRS with an extended fixed entry is used:

```
LRSFIXEX EQU      X'04'      LRS extended fixed entry is used
```

The LRS fixed entry size is being extended from 12 bytes as represented by the equate LRSFXLEN. Two fields are defined in the extended fixed entry:

```
LRSFXLN DS        H          Length of LRS fixed entry
LRSGDLME DS       H          GDG limit from catalog management (GDGLIMTE)
```

When flag LRSFIXEX is set, the extended format of the LRS fixed entry is present and the value of field LRSFXLN should be used for the length of the LRS fixed entry. Otherwise, the previous format of the LRS fixed entry is present and the existing equate LRSFXLEN is used for the length.

When existing flag LRSGDG is set, the LRS entry is for a GDG ALL request with a GDG limit value provided. When LRSFIXEX is set, the value of field LRSGDLME will contain the 2-byte GDG limit. Existing field LRSGDLIM is maintained and is set to the lesser of 255 and the value in LRSGDLME. When LRSFIXEX is not set, the value of field LRSGDLIM will contain the 1-byte GDG limit.

Table 144 on page 213 provides more details about this migration action. Use this information to plan your changes to the system.

Table 356. Information about this migration action

Element or feature:	JES3
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have code that references the JES3 Locate Response control block as defined in IATYLRS. No changes are required if only the LRS fixed entry fields are referenced and if the existing GDG limit field LRSGDLIM is not referenced.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Look for code, especially JES3 user exits, that refers to IATYLRS with the supplied address, referencing any of the following fields or equates from IATYLRS: LRSFXLEN, LRSGDLIM, or LRSDATA.

- Code using the length in equate LRSFXLEN to advance beyond the LRS fixed entry must be changed to use the value in field LRSFXLN when flag LRSFIXEX is set.
- Code directly referencing the LRS data entry using the label LRSDATA must be changed to advance beyond the LRS fixed entry using the length value in field LRSFXLN or equate LRSFXLEN based upon the flag LRSFIXEX.
- Code using the GDG limit in LRSGDLIM must be changed to use the new 2-byte GDG limit in field LRSGDLME when flag LRSFIXEX is set.

Reference information

For more information about the GDGE format, see the descriptions of the GDGLIMIT and GDGLIMTE fields in *z/OS DFSMS Managing Catalogs*.

Language Environment migration actions

This topic describes migration actions for base element Language Environment.

Language Environment actions to perform before installing z/OS V2R2

This topic describes Language Environment migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Convert to CEEPRMxx to set system-level default runtime options

Description

In the IBM z/OS V1R12 Software Announcement 210-235 dated 22 July 2010, IBM announced plans to remove the capability to change the default Language Environment runtime options settings using SMP/E installable USERMODs. As of z/OS V2R1 if you are still using assembler modules to specify your installation-wide default runtime options (CEEDOPT, CEECOPT, or CELQDOPT), you must convert to using the CEEPRMxx parmlib member to set your system-level default Language Environment runtime options. z/OS V1R13 was the last release to support the SMP/E USERMOD to customize the Language Environment run-time options.

Table 357 provides more details about this migration action. Use this information to plan your changes to the system.

Table 357. Information about this migration action

Element or feature:	Language Environment.
When change was introduced:	z/OS V2R1. (Previewed in IBM z/OS V1R12 Software Announcement 210-235, 22 July 2010.)
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you still use SMP/E USERMOD to customize the Language Environment runtime options.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	Use CEE_USING_LE_PARMLIB to check that default Language Environment runtime options are set within a CEEPRMxx parmlib member.

Migration actions from z/OS V1R13: Language Environment

Steps to take

Follow these steps:

- If you are no longer using the Language Environment runtime option assembler usermods, you do not have to take further action.
- If you are using the Language Environment runtime option assembler usermods, you must convert to CEEPRMxx parmlib member.

Reference information

For information about the CEEPRMxx parmlib member, see *z/OS Language Environment Customization*.

Ensure that the name of the debug tool event handler is recognized by Language Environment

Description

Before z/OS V2R2, the value for the debug tool event handler name that is specified by the `_CEE_DEBUG_FILENAME31` environment variable was not restricted. Starting in V2R2, the name must be `/bin/dbx31vdbg` or be defined in a file that contains a list of allowed values.

Table 145 on page 215 provides more details about this migration action. Use this information to plan your changes to the system.

Table 358. Information about this migration action

Element or feature:	Language Environment
When change was introduced:	z/OS V2R1, z/OS V1R13, and z/OS V1R12 (all with APAR PM99349 applied).
Applies to migration from:	z/OS V2R1 and z/OS V1R13 (both without APAR PM99349 applied).
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended if you use debuggers in certain circumstances. Many debuggers will not be affected for any of these reasons: <ul style="list-style-type: none">• They do not provide a debug tool event handler. (HLASM Toolkit Feature Interactive Debug Facility (ASMIDF), TSO/E TEST)• They do not install a debug tool event handler in z/OS UNIX file systems. (Debug Tool for z/OS, Rational Developer for System z Integrated debugger)• They use a debug tool event handler in the z/OS UNIX file system that is allowed by default. (dbx)
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Message CEE2532S is issued, indicating that use of the debug tool event handler specified by the <code>_CEE_DEBUG_FILENAME31</code> environment variable is not allowed.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Look for any vendor product or your own software that is a debugger and uses the environment variable `_CEE_DEBUG_FILENAME31` to identify a debug tool event handler in the z/OS UNIX file system.
- If any are found, create the file `/etc/_CEE_DEBUG_FILENAME31.list` and add the file name that is specified by the environment variable `_CEE_DEBUG_FILENAME31` to it.

Note: The file name `/bin/dbx31vdbg`, used by `dbx`, does not need to be added to this file.

After you complete the steps, the name of the debug tool event handler will be recognized by Language Environment.

Reference information

For more information about the `_CEE_DEBUG_FILENAME31` environment variable, see *z/OS Language Environment Vendor Interfaces*.

Language Environment actions to perform before the first IPL of z/OS V2R2

This topic describes Language Environment migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Update the CSD based on the newest CEECCSD Description

Each release, Language Environment adds or deletes load modules in the CICS system definition (CSD) file. Thus, you should update the file each release using the program definitions found in members `CEECCSD` and `CEECCSDX` found in the `SCEESAMP` data set. The CSD samples provided by Language Environment (`CEECCSD` and `CEECCSDX`) at the latest release can be used for systems at earlier releases that can co-exist with this level of z/OS.

Table 146 on page 216 provides more details about this migration action. Use this information to plan your changes to the system.

Table 359. Information about this migration action

Element or feature:	Language Environment.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use CICS.
Target system hardware requirements:	None.
Target system software requirements:	CICS.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	Failure to perform this migration action may result in several various program ABENDs, such as ABENDU4093 RC=3EC. Which ABEND you see will depend on which programming language (and which level of the programming language) you are using.

Migration actions from z/OS V1R13: Language Environment

Table 359. Information about this migration action (continued)

Related IBM Health Checker for z/OS check:	None.
--	-------

Steps to take

Update the CSD file using the program definitions in member CEECCSD (and member CEECCSDX if using CICS TS V3 or later) found in the hlq.SCEESAMP data set.

Note: The group containing the Language Environment runtime routines must be in the group list used during CICS startup.

Reference information

For more information, see *z/OS V2R1.0 Language Environment Runtime Application Migration Guide*.

Update Language Environment load modules in the LPA Description

Each release you must update the Language Environment load modules that you make accessible through the link pack area (LPA). In addition, each release you should review your list of Language Environment load modules in the LPA to determine if it is still suitable.

Table 147 on page 217 provides more details about this migration action. Use this information to plan your changes to the system.

Table 360. Information about this migration action

Element or feature:	Language Environment.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you need to make modules accessible through the link pack area (LPA).
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Review Language Environment load modules in the LPA.

To move load modules into the LPA, use the following sample members in the CEE.SCEESAMP data set:

- *AFHWMLP2*: This is a sample of all Language Environment Fortran component modules eligible for the LPA.
- *CEEWLPA*: This is a sample of a PROGxx member of SYS1.PARMLIB that includes all Language Environment CEE-prefixed runtime modules eligible for the LPA (that is, all Language Environment base modules) except the callable services stubs.
- *CELQWLPA*: This is a sample for AMODE 64 runtime support.

Migration actions from z/OS V1R13: Language Environment

- *EDCWLPA*: This is a sample of a PROGxx member of SYS1.PARMLIB that includes all Language Environment EDC-prefixed and CEH-prefixed runtime modules eligible for the LPA (that is, all XL C/C++ component modules) except locales and code page converters.
- *IBMALLP2* (or *IBMPLPA1* for Enterprise PL/I for z/OS): This is a sample of all Language Environment PL/I component modules eligible for the LPA.
- *IGZWMLP4*: This is a sample of all Language Environment COBOL component modules eligible for the LPA.

To see which modules are eligible for the LPA, refer to *z/OS Language Environment Customization*. The modules listed there can be put in the LPA or extended LPA (ELPA) depending on their RMODE value:

- If the RMODE is ANY, the module can reside in the LPA or in the ELPA (above or below the 16 MB line).
- If the RMODE is 24, the module can reside only in the LPA (below the 16 MB line).

If you are considering placing the modules listed in *z/OS Language Environment Customization* in the LPA or the ELPA, then IBM recommends that you place the SCEELPA data set in the LPA list (LPALSTxx). SCEELPA contains Language Environment load modules that are reentrant, that reside above the 16 MB line, and that are heavily used by z/OS.

In *z/OS Language Environment Customization* you will also see tables of modules eligible for the LPA and the ELPA above and beyond what is found in the SCEELPA data set. You will need to use the dynamic LPA or MLPA approach to move these modules into the LPA or ELPA. You do not need to include recommended modules if they contain functions your installation does not use. Language Environment modules not listed in these tables can be moved into the LPA or ELPA at your discretion.

Reference information

For more information, see the table “Language Environment sample IEALPAnn or PROGxx members in hlq.SCEESAMP” for the list of sample members and their changed content in *z/OS Language Environment Customization*. The table contains a list of eligible load modules for:

- Language Environment base modules
- Language Environment XL C/C++ component modules
- Language Environment COBOL component modules
- Language Environment Fortran component modules
- Language Environment PL/1 component modules

Determine if the region-level runtime option JCL requires changes

Description

Because of the changes introduced in “Accommodate removal of samples provided for system-level runtime usermods” on page 459, new region-level assembler samples are provided in the SCEESAMP data set. These samples are called CEERDOPT, CEERCOPT and CELQRDOP. Each sample contains the IBM-supplied default values for runtime options. The instructions in the CEEWROPT and CEEWQROP sample JCL parts for creating region-level runtime options load modules have been updated to refer to the new assembler samples.

Table 361 provides more details about this migration action. Use this information to plan your changes to the system.

Table 361. Information about this migration action

Element or feature:	Language Environment.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.

Migration actions from z/OS V1R13: Language Environment

Table 361. Information about this migration action (continued)

Is the migration action required?	No, but recommended if you need to create a new region-level runtime options module.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

No action is needed for existing CEEROPT modules or for JCL job which already contain a copy of the old assembler samples. If you need to create a new region-level runtime options module, use the updated JCL and sample assembler parts.

Reference information

For more information about creating region-level runtime option load modules, see *z/OS Language Environment Customization*.

Update programs that read the Language Environment options report Description

The Language Environment options reports, which may be obtained by specifying RPTOPTS(ON), with the CLER CICS transaction, with a CEEDUMP or using VERBX LEDATA in an IPCS readable dump, will no longer show "Installation Default" as the last where set field. If the runtime option defaults shipped with Language Environment have not been changed, the last where set field will show "IBM-supplied default". Also, the last where set value of "Installation non-overrideable" is no longer used.

Table 362 provides more details about this migration action. Use this information to plan your changes to the system.

Table 362. Information about this migration action

Element or feature:	Language Environment.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have an application that reads the output of an options report
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you have programs that attempt to read the output from these reports, your programs should be updated accordingly. Similarly, if you were outputting an options report you should use “IBM-supplied default” for a where set value that formerly matched “Installation default”.

Reference information

For more information, see the following references:

- *z/OS Language Environment Debugging Guide*
- *z/OS Language Environment Customization*
- *z/OS V2R1.0 Language Environment Programming Guide for 64-bit Virtual Addressing Mode*

Accommodate removal of samples provided for system-level runtime usermods Description

In z/OS V1R12, Language Environment issued a statement of direction indicating that the preferred method of setting default system-level runtime options is using the CEEPRMxx support. The statement of direction further indicated that the ability to change installation-level runtime options with SMP/E installable usermods would be removed in a future release. Starting in z/OS V2R1, that ability is removed. See “Convert to CEEPRMxx to set system-level default runtime options” on page 453.

The CEEWDOPT, CEEWCOPT, and CEEWQDOP sample JCL jobs that were used to install Language Environment runtime option usermods are no longer included in the SCEESAMP dataset. The corresponding CEEDOPT, CEECOPT, and CELQDOPT assembler source code samples, which contained the IBM-supplied runtime option, are also no longer included in the SCEESAMP dataset. Additionally, the CEELOPT macro has been updated to issue an MNOTE if the generation of a CEEDOPT or CELQDOPT CSECT is requested.

Table 363 provides more details about this migration action. Use this information to plan your changes to the system.

Table 363. Information about this migration action

Element or feature:	Language Environment.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you still use the assembler language usermods to modify installation-wide runtime options.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

If you used the CEEWDOPT, CEEWCOPT, and CEEWQDOP sample JCL jobs in releases earlier than z/OS V2R1, you can no longer do so. You must now migrate to using the CEEPRMxx support. See “Convert to CEEPRMxx to set system-level default runtime options” on page 453.

Migration actions from z/OS V1R13: Language Environment

Reference information

For more information about setting system-level default runtime options, see *z/OS Language Environment Customization*.

Language Environment actions to perform after the first IPL of z/OS V2R2

This topic describes Language Environment migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

Library Server migration actions

This topic describes migration actions for base element Library Server.

Library Server actions to perform before installing z/OS V2R2

This topic describes Library Server migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

Library Server actions to perform before the first IPL of z/OS V2R2

This topic describes Library Server migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Copy Library Server configuration files Description

The Library Server configuration files (`bookmgr.80`, `booksrv.80`) contain information about your environment and preferences. The information in `bookmgr.80` includes the names of bookshelf lists for bookshelves in z/OS data sets and the names of the file system directories that Library Server reads and writes during execution. The information in `booksrv.80` includes the file system directory names of book collections, shelves, and bookcases, as well as product option settings configured via the Library Server Administration Page. There are default values but normally you would customize them. In order to bring the customized values over to your new system, you have to copy them. (Note that port number suffix `.80`, used in `bookmgr.80` and `booksrv.80`, is an example. Your port number suffix might be different.)

Table 148 on page 219 provides more details about this migration action. Use this information to plan your changes to the system.

Table 364. Information about this migration action

Element or feature:	Library Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you intend to preserve your Library Server configuration.
Target system hardware requirements:	None.
Target system software requirements:	None.

Table 364. Information about this migration action (continued)

Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Copy your current (customized) configuration files, usually `bookmgr.80` and `booksrv.80`, to your new system and add any configuration parameters that are new since the z/OS release from which you are migrating. Otherwise Library Server will run with default values, not the values you're used to. A suggested (but not required) place for these configuration files is `/etc/booksrv`. Library Server will also search `/etc` and the original `cgi-bin` for them. If you place the files in any other directory, use the `EPHConfigPath` environment variable to tell Library Server where to find them.

Reference information

For description of each parameter of the Library Server configuration files, see *z/OS Program Directory* at the z/OS installation related information website.

Copy Library Server notes files

Description

Users can make comments in book topics by creating notes that are appended to the end of each topic. If you do not copy these notes to the new system, they will be lost.

Table 149 on page 219 provides more details about this migration action. Use this information to plan your changes to the system.

Table 365. Information about this migration action

Element or feature:	Library Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you intend to preserve notes from release to release.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Copy all the files from your existing notes directory to the new one. The default directory for saving book notes is `/usr/lpp/booksrv/public/bookmgr/notes`. You can override this default by specifying a directory on the `NOTEDIR` parameter of the `bookmgr.80` configuration file.

Migration actions from z/OS V1R13: Library Server

Reference information

For a description of each parameter of the Library Server configuration files, see *z/OS Program Directory* at the z/OS installation related information website.

Migrate the Library Server configuration to work with IBM HTTP Server - Powered by Apache Description

Starting with z/OS V2R2, the web server is IBM HTTP Server - Powered by Apache. As a result, the HTTP Server configuration required by Library Server, particularly the configuration file directives, is significantly different than that required for the Domino-based HTTP Server used prior to z/OS V2R2.

If Library Server on your z/OS V2R1 or V1R13 system was not already configured to use an Apache-based HTTP Server, you must change the configuration of the z/OS V2R2 Library Server to operate with IBM HTTP Server - Powered by Apache. z/OS V2R2 includes IBM HTTP Server - Powered by Apache as a base element.

Table 150 on page 220 provides more details about this migration action. Use this information to plan your changes to the system.

Table 366. Information about this migration action

Element or feature:	Library Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if Library Server on your z/OS V2R1 or V1R13 system was not already configured to use an Apache-based HTTP Server.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

The following steps summarize the Library Server changes to consider when migrating from IBM HTTP Server powered by Domino to IBM HTTP Server - Powered by Apache in z/OS V2R2:

1. The envvars file of environment variable settings moves from conf/httpd.envvars to bin/envvars.
2. For each environment variable set in bin/envvars, a **PassEnv** directive is needed in conf/httpd.conf.
3. All **Pass** directives are required to become **Alias** directives in conf/httpd.conf.
4. All **Exec** directives are required to become **ScriptAlias** directives in conf/httpd.conf.
5. Multiple port support is configured in a single conf/httpd.conf using the VirtualHost directive, such as **<VirtualHost *:8080>**.
6. A **Listen port#** directive must be specified for each port (default and VirtualHost) configured in conf/httpd.conf.
7. A **<LocationMatch>** directive is required in conf/httpd.conf to prevent EBCDIC to ASCII translation when downloading CSS files.

8. If configuring an SSL port in `conf/httpd.conf`, the `LoadModule ibm_ssl_module modules/mod_ibm_ssl.so` directive must be enabled.
9. A self-identifying `ServerName` directive, such as `ServerName MYMVS.ibm.com:80`, should be specified in `conf/httpd.conf`.
10. Other directives such as `ErrorLog`, `CustomLog`, and `ServerAdmin` should be configured as needed in `conf/httpd.conf`.

Add the new directives mentioned here to the `conf/httpd.conf` file that is installed with IBM HTTP Server - Powered by Apache, and base them on the corresponding directives, if applicable, from your `conf/httpd.conf` file that was previously used with IBM HTTP Server powered by Domino. Examples of the new directives are provided in the HTTP server customization topic of the *Library Server Customization Considerations* section in the *z/OS Program Directory*.

Reference information

For more information, see the following references:

- For Library Server customization considerations, see *z/OS Program Directory* at the z/OS installation related information website
- For information about how to plan for, install, configure and use IBM HTTP Server - Powered by Apache, see *z/OS V2R2.0 HTTP Server - Powered by Apache User's Guide*.

Library Server actions to perform after the first IPL of z/OS V2R2

This topic describes Library Server migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

Reconfigure Library Server information centers

Description

Starting with z/OS V2R1, the Library Server element requires the Location value (ICPATH=) value of InfoCenters to be configured differently than it was in the past. Thus, for any existing information center configurations migrated from the previous version, you must delete, configure, and process the configured information centers.

Table 367 provides more details about this migration action. Use this information to plan your changes to the system.

Table 367. Information about this migration action

Element or feature:	Library Server
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you intend to preserve configured information centers from the previous version
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Migration actions from z/OS V1R13: Library Server

Steps to take

Follow these steps:

1. Migrate your current customized booksrv.80 as described in **Description**.
2. Configure and start your HTTP server as required for Library Server as described in the *z/OS Program Directory*.
3. Using the Library Server Administrative Interface, delete any existing information center configuration entries.
4. Using the Library Server Administrative Interface, configure (that is, create new) each deleted information center, using for its *Location* field the fully qualified root plugin directory name, or jar file name, of the information center. (Note that the root plugin is a child of the information center parent directory and is typically distinguishable as the plug-in that contains the plugin_customization.ini file for the information center.)
5. Using the Library Server Administrative Interface for managing information centers, for each configured information center, use the Prepare InfoCenter Plugins function to prepare its plug-ins for subsequent creation of the information center search index.
6. Using the Library Server Administrative Interface for managing information centers, for each configured information center, use the Receive InfoCenter Plugins function to copy/catalog all the prepared information center plug-in objects (for example, TOC files and plug-in card files) into the Library.
7. Using the Library Server Administrative Interface for managing information centers, for each configured information center, use the Create InfoCenter Search Index function to create the search index which enables searching across all the plug-ins for the information center.

Reference information

For a description of each parameter of the Library Server configuration files, see *z/OS Program Directory* at z/OS installation related information.

RMF migration actions

This topic describes migration actions for optional feature Resource Measurement Facility (RMF).

RMF actions to perform before installing z/OS V2R2

This topic describes RMF migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

RMF actions to perform before the first IPL of z/OS V2R2

This topic describes RMF migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Control the invocation of data reduction exit routines

Description

As of z/OS V2R1, if you are running unauthorized applications that invoke the RMF Monitor II Sysplex Data Gathering service (ERB2XDGS) or the RMF Monitor III Sysplex Data Retrieval service (ERB3XDRS), you must take certain actions to allow the applications to make use of data reduction exit routines.

Table 368 provides more details about this migration action. Use this information to plan your changes to the system.

Table 368. Information about this migration action

Element or feature:	RMF.
When change was introduced:	z/OS V2R1. This function is rolled back to z/OS V1R13, z/OS V1R12, and z/OS V1R11 with APAR OA38022 for RMF Monitor II service and APAR OA37965 for RMF Monitor III.
Applies to migration from:	z/OS V1R13 without the PTFs for APARs OA38022 and OA37965 applied.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have unauthorized applications that invoke ERB2XDGS (RMF Monitor II Sysplex Data Gathering service) or ERB3XDRS (RMF Monitor III Sysplex Data Retrieval service).
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Steps to take

To allow your applications to make use of data reduction exit routines specified with the ERB2XDGS or ERB3XDRS services, take the following actions:

- If the application has been designed to run authorized, you must adapt the application or program so that it runs in supervisor state, system state, or be APF authorized.
- You can approve the exit by adding RACF resource ERBSDS.MON2EXIT.<exit_name> or ERBSDS.MON3EXIT.<exit_name> to the RACLISTed class FACILITY and by granting read access to the profile for the user ID that invokes the Sysplex Data Server API.
- If you are running an unauthorized application that invokes RMF Monitor II Sysplex Data Gathering service ERB2XDGS/ERB2XD64 or Monitor III Sysplex Data Retrieval service ERB3XDRS/ERB3XD64, you must take one of the following actions to allow the application to make use of data reduction exits.
 1. If the application is properly designed and secure to run authorized, you must adapt the application or program so that it runs in supervisor state, system state, or APF authorized.
 2. You can approve the exit by adding RACF resource ERBSDS.MON2EXIT <exit_name> or ERBSDS.MON3EXIT <exit_name>.RACLISTed class FACILITY and by granting read access to the profile for the user ID invoking the Sysplex Data Server API.

Reference information

For information about the RMF sysplex data services, see *z/OS RMF Programmer's Guide*.

Check your GPMSERVE and GPM4CIM options for TCP/IP address regular expressions

Description

Starting with z/OS V2R1, RMF GPMSERVE honors IPv6 address syntax when parsing the option settings from a parmlib member. The same applies to GPM4CIM parsing options from a configuration file.

Migration actions from z/OS V1R13: RMF

Table 369 provides more details about this migration action. Use this information to plan your changes to the system.

Table 369. Information about this migration action

Element or feature:	RMF
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use GPMSEVERVE or GPM4CIM with IPv6 address regular expressions.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None

Steps to take

If you use GPMSEVERVE or GPM4CIM in an IPv6 or dual mode IPv6/IPv4 network environment, check one or more of your options parmlib members for options containing regular expressions representing IP addresses (for example, the options HTTP_ALLOW or HTTP_NOAUTH). Make sure that the regular expressions adhere strictly to the format of the IP addresses in your network. Examples include the following:

Table 370. Examples of IP matches

IP address expression	Match	Examples of full IP address match
'6.*'	Matches any IP address starting with '6.'	6.19.107.32' or '6.34.88.103'
::ffff:6.*'	Matches any (mapped) IP address starting with '::ffff:6.'	::ffff:6.19.107.32' or '::ffff:6.9.50.7'
6.'	Matches any IP address containing a substring '6.'	::ffff:6.9.50.7' or '6.19.107.32'

Reference information

For more information, see *z/OS RMF User's Guide*.

Define the RACF definitions to enable the GPMSEVERVE Started Task for Authorization Code zero (AC=0)

Description

Starting with z/OS V2R1, the RMF GPMSEVERVE Started Task runs as a module linked with Authorization Code zero (AC=0).

Table 371 on page 467 provides more details about this migration action. Use this information to plan your changes to the system.

Table 371. Information about this migration action

Element or feature:	RMF
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Define READ Access to the BPX.SERVER Facility for the GPMSERVE userid:

```
PERMIT BPX.SERVER CLASS(FACILITY) ID(GPMSERVE) ACCESS(READ)
```

2. Ensure that all programs loaded by GPMSERVE are defined to PROGRAM CONTROL:

```
RDEFINE PROGRAM GPM* ADDMEM('SYS1.SERBLINK'//NOPADCHK) UACC(READ)
RDEFINE PROGRAM ERB* ADDMEM('SYS1.SERBLINK'//NOPADCHK) UACC(READ)
RDEFINE PROGRAM CEEBINIT ADDMEM('CEE.SCEERUN'//NOPADCHK) UACC(READ)
RDEFINE PROGRAM IEEMB878 ADDMEM('SYS1.LINKLIB'//NOPADCHK) UACC(READ)
RDEFINE PROGRAM CELHV003 ADDMEM('SYS1.SCEERUN2'//NOPADCHK) UACC(READ)
RDEFINE PROGRAM C128 ADDMEM('SYS1.SCEERUN2'//NOPADCHK) UACC(READ)
RDEFINE PROGRAM CELHDCPP ADDMEM('SYS1.SCEERUN2'//NOPADCHK) UACC(READ)
SETROPTS WHEN(PROGRAM) REFRESH
```

This action is only needed when GPMSERVE is not already defined to PROGRAM CONTROL. In previous RMF Releases this was recommended but not required since the GPMSERVE module was linked with Authorization Code one (AC=1).

3. Define READ access to the BPX.STOR.SWAP FACILITY class profile for the GPMSERVE userid.

```
PERMIT BPX.STOR.SWAP CLASS(FACILITY) ID(GPMSERVE) ACCESS(READ)
```

Reference information

For more information, see *z/OS RMF User's Guide*.

RMF actions to perform after the first IPL of z/OS V2R2

This topic describes RMF migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

Update programs that use ERBZFST3 or ERBZFAT3

Description

Before z/OS V2R2, RMF provided ZFSSUM or ZFSACT reports, which stored results in Monitor III tabular report data tables ERBZFST3 and ERBZFAT3. Starting with z/OS V2R2, RMF provides ZFSOVW or ZFSFS reports, which store results in Monitor III tabular report data tables ERBZFOT3 and ERBZFOT3. This change will affect any user written programs and applications that reference ERBZFST3 or ERBZFAT3.

Migration actions from z/OS V1R13: RMF

Table 152 on page 223 provides more details about this migration action. Use this information to plan your changes to the system.

Table 372. Information about this migration action

Element or feature:	RMF
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you modified any of the four Monitor III reporter session phases to refer to any of the fields in ERBZFST3 or ERBZFAT3, or have programs or applications that refer to any of the fields in ERBZFST3 or ERBZFAT3.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- If you have used the RMF Monitor III utility to modify any of the four Monitor III reporter session phases, search the programs or applications provided as user exits for these Monitor III phases for fields from the RMF Monitor III tabular report data tables ERBZFST3 and ERBZFAT3.

Likewise, look for Monitor III reports that have been modified or created with the Monitor III utility that make use of any of the fields in ERBZFST3 or ERBZFAT3.

The RMF Monitor III tabular report data tables ERBZFST3 and ERBZFAT3 will be empty (the tables exist, but contain no data) when running RMF Monitor III in V2R2, because zFS performance data will be stored to ERBZFOT3 and ERBZFFT3. Programs or applications using values from ERBZFST3 or ERBZFAT3 will always find empty fields (no data contained).

To access zFS performance data with your existing user exits or modified Monitor III reports, you must use ZFSOVW and ZFSFS instead of ZFSSUM and ZFSACT. You must also replace the field names from ERBZFST3 and ERBZFAT3 you have identified in the previous step with the corresponding fields from ERBZFOT3 and ERBZFFT3.

- Look for applications requesting ZFSSUM or ZFSACT data from the RMF Distributed Data Server using the HTTP API (a request for a complete ZFSSUM or ZFSACT report or requests for metrics based on one of these reports), such as:

```
http://hostname:8803/gpm/reports/ZFSSUM?resource=",S4,MVS_IMAGE"
```

or

```
http://hostname:8803/gpm/perform.xml?resource="S4,*,ZFS"&id=8D2AC0
```

HTTP applications requesting data based on ZFSSUM or ZFSACT will receive an HTTP response containing a GPM0630I message stating that no data is available for this request. Therefore HTTP applications must be changed to use requests for ZFSOVW or ZFSFS reports and requests for metrics based on these reports, if you want to monitor zFS performance data.

Reference information

For more information, see the following references:

- For information about ZFSOVW and ZFSFS reports, see *z/OS RMF Report Analysis*.
- For information about Monitor III tabular report data tables ERBZFOT3 and ERBZFFT3, see *z/OS RMF Programmer's Guide*.

Use an RMF Monitor III reporter version equal to or later than your RMF Monitor III gatherer version

Description

To avoid problems when reporting Monitor III data, use an RMF reporter version that is equal to or later than the latest RMF gatherer version used to collect the data to be reported. For example, it is safe to use an RMF reporter version from z/OS V2R2 for data collected with an RMF gatherer from z/OS V1R13, but not vice versa.

Mixed (and therefore problematic) levels of collected data can occur in the following scenarios:

- *Single system*: You install and test a new release, then fall back to an earlier one; your data sets might contain data collected with different versions of the RMF gatherer.
- *Sysplex*: You migrate to a new release on one system in a sysplex but try to use an earlier reporter version from another system to report on the migrated system's data.

Table 153 on page 224 provides more details about this migration action. Use this information to plan your changes to the system.

Table 373. Information about this migration action

Element or feature:	RMF.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you had planned to use an earlier level RMF reporter on data that was collected with a later level RMF gatherer.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	See "Steps to take" on page 224.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Always use an RMF Monitor III reporter version that is equal to or later than the gatherer version used to collect the data from which you want to produce a report.

Note: Monitor III notifies users by issuing information message ERB948I when a reporter session is started on a system in a sysplex that is not running with the highest RMF level available in the sysplex. The message helps users to avoid reporting problems.

Migration actions from z/OS V1R13: RMF

Reference information

For more information, see *z/OS RMF User's Guide*.

Determine need of SMF data collection for Postprocessor PCIE Activity report Description

Starting with z/OS V2R1, RMF provides a new Postprocessor PCIE Activity report based on the SMF 74.9 record. If you do not need this report, you should turn off data collection for SMF record 74 subtype 9.

Table 374 provides more details about this migration action. Use this information to plan your changes to the system.

Table 374. Information about this migration action

Element or feature:	RMF.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	No, but recommended if you do not want to collect SMF data for the Postprocessor PCIE Activity report.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Determine whether you want to use the new Postprocessor PCIE Activity report. SMF data required for this report is gathered by default. If you do not want to use this report, you should suppress the SMF data collection for the new record type 74 subtype 9. You achieve this by specifying NOTYPE for this SMF record type in the SMF parmlib member SMFPRMxx.

Another method to suppress the data gathering of record 74.9 for the Postprocessor PCIE Activity report is to use the SUBSYS parameter in the SMFPRMxx parmlib member for the STC subsystem (started tasks, where RMF is one of them). To exclude data gathering for SMF record 74.9, specify **SUBSYS(STC,NOTYPE(74(9)), ...)**.

The SUBSYS specification overrides the SYS specification. So for example, if you have defined **SYS(TYPE(...,74,...))** in your SMFPRMxx parmlib member, you can use **SUBSYS(STC, NOTYPE(74(9)))** to make exceptions to your SYS specification and just exclude gathering of SMF record 74.9 for started tasks like RMF.

Reference information

For more information about specifying SMF data collection, see *z/OS MVS Initialization and Tuning Reference*.

SDSF migration actions

This topic describes migration actions for optional feature SDSF.

SDSF actions to perform before installing z/OS V2R2

This topic describes SDSF migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

SDSF actions to perform before the first IPL of z/OS V2R2

This topic describes SDSF migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Review and reassemble user exit routines

Description

If you have written user exit routines, review them to ensure they are still appropriate for the current environment, and make changes as necessary. All user exit routines must be reassembled with the z/OS V2R2 level of the SDSF macro library.

Table 154 on page 225 provides more details about this migration action. Use this information to plan your changes to the system.

Table 375. Information about this migration action

Element or feature:	SDSF.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if user exit routines are in use.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Review user exit routines to ensure they are appropriate for z/OS V2R2. Make changes as necessary. Regardless of whether you have made changes, reassemble the user exit routines with the z/OS V2R2 level of the SDSF macro library.

Tip: A PROPLIST statement, along with PROPERTY statements, both in the ISFPRMxx parmlib member, defines customized values for certain SDSF properties. It provides an alternative to writing user exit routines to customize those properties. A user exit routine that customizes the same property as a PROPERTY statement overrides the value on the PROPERTY statement.

Reference information

For more information, see *z/OS SDSF Operation and Customization*.

Migration actions from z/OS V1R13: SDSF

Use dynamic statements for ISFPARMS to avoid reassembly

Description

ISFPARMS in SDSF is used for specifying global options, the format of panels, and security for SDSF functions. SDSF provides two alternatives for ISFPARMS:

- Assembler macros that you define, assemble, and then link into the SDSF load library. This is the original format for defining ISFPARMS and it continues to be supported for compatibility.
- Dynamic statements, which are in parmlib member ISFPRMxx. Dynamic statements are the recommended format. They are easier to code and are more dynamic than the assembler macros; they can be updated without reassembling or link-editing. The statements are processed by an SDSF server, which is controlled by MVS operator commands.

Table 155 on page 226 provides more details about this migration action. Use this information to plan your changes to the system.

Table 376. Information about this migration action

Element or feature:	SDSF.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	No, but recommended to avoid the migration action of reassembling your customized ISFPARMS for each z/OS release. (If you do not use dynamic statements for ISFPARMS, reassembly of your customized ISFPARMS is required on each release.)
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Table 376. Information about this migration action (continued)

<p>Related IBM Health Checker for z/OS check:</p>	<p>Use check SDSF_ISFPARMS_IN_USE to verify that SDSF dynamic statements in ISFPRMxx are being used rather than the assembler macros. If the check determines that the assembler macro ISFPARMS is in use instead, and that it has been modified, the check generates an exception. If the assembler macro ISFPARMS is in use but it has not been modified, so that all defaults are in effect, the check does not generate an exception.</p> <p>SDSF registers this check with the IBM Health Checker for z/OS infrastructure when the SDSF server address space is initialized. However, one of the items this check verifies is that the SDSF server itself is in use, so you have to manually add this check (particularly if you do not use the SDSF server) so that the IBM Health Checker for z/OS infrastructure will invoke the check. To add the check, put the following statement in your PROGxx parmlib member: EXIT ADD EXITNAME(HZSADDCK) MODNAME(ISFHCADC).</p> <p>SDSF health checks are distributed in ISF.SISFLOAD for installations running SDSF in the LNKLST. The checks are also distributed in ISF.SISFLINK for installations that do not run SDSF in the LNKLST. For those installations, ISF.SISFLINK must be added to the LNKLST.</p> <p>Note: To avoid a possible ABEND 290 with reason code 02014007 issued by HZSADDCK:</p> <ul style="list-style-type: none"> Specify the proper check routine name. The check routine module must be in an APF-authorized library. The system must be able to locate the check routine within the joblib, the steplib of the IBM Health Checker for z/OS address space, the LPA, or the LNKLST. Specify the proper message table name. The message table module must be in an APF-authorized library. The system must be able to locate the message table within the joblib, the steplib of the IBM Health Checker for z/OS address space, the LPA, or the LNKLST.
---	---

Steps to take

If you are already using dynamic statements for ISFPARMS, there is no migration action to perform.

If you are using assembler macros for ISFPARMS, do one of the following:

- Convert your existing ISFPARMS to dynamic statements by using a conversion utility that you invoke with the ISFACP command.
- Reassemble your customized ISFPARMS for use with z/OS V2R2. Reassembly must be done whenever you change your z/OS release. Before reassembling ISFPARMS, you might want to update it for new function. The assembler ISFPARMS cannot be shared with any other release of SDSF. Only use ISFPARMS for the release on which it is assembled.

Note: If you have an SMP/E usermod that specifies modifications to assembler macro ISFPARMS, change the usermod to indicate that module ISFPARMS is now owned by the z/OS base V2R2 SDSF FMID (HQX77A0). The correct SMP/E syntax is ++VER(Z038) FMID(HQX77A0)

Migration actions from z/OS V1R13: SDSF

Also, in the SMP/E usermod, change the distlib to reference DISTLIB(AISFSRC). The correct SMP/E syntax is ++VER(Z038) FMID(HQX77A0). Your ++SRC or ++SRCUPD statement must specify DISTLIB(AISFSRC).

Reference information

For information about invoking the conversion utility with the ISFACP command, and the ISFPARMS and the ISFPRMxx parmlib members, see *z/OS SDSF Operation and Customization*.

SDSF actions to perform after the first IPL of z/OS V2R2

This topic describes SDSF migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

Control how SDSF handles extended consoles

Description

As of z/OS V2R1, the behavior for obtaining an extended console (used for issuing system commands) has changed. Before z/OS V2R1, when SDSF attempted to obtain an extended console and the default extended console name was already in use, SDSF shared that console. For example, if you used ISPF split screen and accessed SDSF in multiple logical screens, SDSF shared the console activated in the first logical screen with subsequent logical screens. As a result, the user log in the first logical screen contained system messages for all of the logical screens.

Starting with V2R1, when SDSF attempts to activate an extended console and the default console name is in use, SDSF activates a new console with a different name. The new name is derived by appending a single-character suffix to the default name. SDSF tries up to 32 different characters to create a unique console name.

Note: This new behavior also applies to the extended console name that is assigned by the SET CONSOLE command. However, the extended console name that has the maximum length of 8 characters is not modified.

If you want SDSF to share the extended console, rather than obtaining a new console with a name derived by modifying the default console name, you can disable console name modification. You can also define which characters should be used for the suffix that modifies the default console name.

Table 377 provides more details about this migration action. Use this information to plan your changes to the system.

Table 377. Information about this migration action

Element or feature:	SDSF.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you want SDSF to share the extended console, as in previous releases.
Target system hardware requirements:	None.
Target system software requirements:	None.

Table 377. Information about this migration action (continued)

Other system (coexistence or fallback) requirements:	The new custom properties will be ignored in the down-level systems when the toleration APAR PM78102 is applied. Message ISF862I is issued for each non-supported property: KEYWORD <i>keyword</i> VALUE <i>value</i> IGNORED, NOT SUPPORTED IN THIS RELEASE.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

To disable console name modification, so that, as in previous releases, SDSF shares the extended console when the default name is already in use, you can use:

- The SET CONMOD (OFF) command
- The custom property Console.EMCS.NoConMod in ISFPARMS with VALUE(TRUE)
- In a REXX exec, the ISFCONMOD special variable
- In a Java program, ISFRequestSettings.

Note: When the SDSF Server is started with the PROPERTY NAME(Console.EMCS.NoConMod),VALUE(TRUE) statement in the ISFPRMxx parmlib member, the SET CONMOD ON command will fail with message OPTION LOCALLY DISABLED.

To specify which characters can be used as a suffix to modify the default extended console name, use custom property Console.EMCS.ConModChars in ISFPRMxx parmlib member. By default, the characters are \$#@12345.

Reference information

For more information about setting custom properties in ISFPARMS, see the discussion of the PROPLIST nad PROPERTY statements in *z/OS SDSF Operation and Customization*.

Security Server migration actions

This topic describes migration actions for optional feature Security Server.

Security Server actions to perform before installing z/OS V2R2

This topic describes Security Server migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Accommodate the removal of default passwords on RACF commands

Description

- | As of z/OS V2R2, the RACF commands **ADDUSER**, **ALTUSER**, and **PASSWORD** no longer set a default password for the target user ID. In previous releases, these commands used the user's default group name as the password by default.
- | Specifically, the commands are changed as follows to remove the generation of default passwords:
- | • Command **ADDUSER** defaults to PROTECTED when no password or phrase is specified.

Migration actions from z/OS V1R13: Security Server

- Commands **ADDUSER**, **ALTUSER**, and **PASSWORD** no longer set a default password for the target user ID.

Table 156 on page 228 summarizes the new RACF command behavior in z/OS V2R2.

Table 378. New RACF command behavior in z/OS V2R2

Command	Condition	New behavior with z/OS V2R2 with APAR OA48667 applied
ADDUSER <i>user</i>	PASSWORD keyword is omitted.	The user is defined as a PROTECTED user, unless a PHRASE or OIDCARD value is specified. Also, message ICH01024I is issued, stating that the user is defined as PROTECTED.
ADDUSER <i>user</i> PASSWORD	PASSWORD keyword is specified, but its value is omitted.	PASSWORD keyword is ignored with message ICH01025I and the user ID is defined as PROTECTED.
ALTUSER <i>user</i> PASSWORD	PASSWORD keyword is specified, but its value is omitted.	PASSWORD keyword is ignored with message ICH21045I.
PASSWORD USER(<i>user</i>)	INTERVAL NOINTERVAL keyword is omitted.	USER keyword is ignored and message ICH08027I is issued.

Notes:

1. As in previous releases, when a new RACF database is initialized through the IRRMIN00 utility, the IBMUSER user ID is created with a password value of 'SYS1'
2. In previous releases, if the **ADDUSER** command was issued without the PASSWORD keyword:
 - RACF common command exit (IRREVX01) received the **ADDUSER** command with the PASSWORD keyword, but without a value for PASSWORD. As of z/OS V2R2, the PASSWORD keyword is not passed to the exit.
 - Type 80 record for the ALTUSER event code indicated that the PASSWORD keyword was specified. As of z/OS V2R2, the Type 80 record no longer indicates that the PASSWORD keyword was specified.

Table 157 on page 229 provides more details about this migration action. Use this information to plan your changes to the system.

Table 379. Information about this migration action

Element or feature:	Security Server.
When change was introduced:	z/OS V2R2 with APAR OA48667 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13 (with APAR OA48667 applied or without APAR OA47396 applied).
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you rely on RACF to create a default password.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Identify any programs or jobs that issue RACF commands with the following conditions:
 - **ADDUSER** command that does not specify the **PASSWORD** keyword.
 - **ADDUSER** and **ALTUSER** commands that specify the **PASSWORD** keyword, but omit an explicit password value.
 - Programs that call the **ADMN_RUN_COMD** function of the **R_admin** SAF callable service (**IRRSEQ00**) on the **ADDUSER**, **ALTUSER**, or **PASSWORD** commands, as described here.
 - Programs that call the **ADMN_ADD_USER** or **ADMN_ALT_USER** functions of the **R_admin** SAF callable service (**IRRSEQ00**) with input parameter lists that are functionally equivalent to the **ADDUSER**, **ALTUSER**, or **PASSWORD** commands, as described here.
2. Depending on the condition listed above, either remove the command, change it to one that specifies an explicit password value, or leave it as-is and tolerate the change of behavior, as appropriate.

Example: Before z/OS V2R2, the following **ALTUSER** command would reset the password for user **BECKYH** to the user's default group name: **ALTUSER BECKYH PASSWORD**. In z/OS V2R2 with **OA48667** applied, the **PASSWORD** operand is ignored. To reset a password, you must provide a temporary password explicitly: **ALTUSER BECKYH PASSWORD(TEMP1234)**.

Reference information

For more information, see *z/OS Security Server RACF Command Language Reference*.

Security Server actions to perform before the first IPL of z/OS V2R2

This topic describes Security Server migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Check for duplicate class names

Description

When new classes are shipped with RACF, you should verify that any installation-defined class names that have been added to the class descriptor table (CDT) do not conflict with the new classes. For a list of new classes shipped with RACF, see *z/OS Summary of Message and Interface Changes*.

Table 158 on page 230 provides more details about this migration action. Use this information to plan your changes to the system.

Table 380. Information about this migration action

Element or feature:	Security Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have user-defined classes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Migration actions from z/OS V1R13: Security Server

Table 380. Information about this migration action (continued)

Related IBM Health Checker for z/OS check:	None.
--	-------

Steps to take

Verify that any installation-defined class names that have been added to the class descriptor table (CDT) do not conflict with the new classes.

- If you have duplicate class names, RACF issues the following message and enters failsoft mode:
ICH564A RACF DETECTED AN ERROR IN THE INSTALLATION CLASS DESCRIPTOR TABLE,
ENTRY *class_name*, ERROR CODE 7
- If a conflict in class names occurs, resolve it as follows:
 1. Delete the profiles in the installation-defined class with the conflicting name.
 2. Delete the CDT entry for the class.
 3. Add a CDT entry with a different name.
 4. Redefine the profiles.

Reference information

For more information, see *z/OS Security Server RACF System Programmer's Guide*.

Evaluate your use of the ICHDEX01 exit routine Description

Starting in z/OS V2R2, RACF no longer uses the masking algorithm (a weak form of encryption) by default to authenticate passwords and password phrases when the initial attempt using DES results in failure. To continue the use of masking, which is not recommended, your installation can do so only by using an ICHDEX01 (password authentication) exit routine. If no ICHDEX01 exit routine exists, RACF now uses only DES encryption for authentication.

The Key Derivation Function with AES (KDFAES) algorithm is the preferred method for authenticating passwords and password phrases. If your installation does not use KDFAES encryption, RACF performs authentication by using the DES algorithm, unless you supply an ICHDEX01 exit routine. In the ICHDEX01 exit routine, your installation can provide an encryption algorithm, or instruct RACF to use one of the following forms of authentication:

Return code 4

Use the masking algorithm.

Return code 8

Use the DES algorithm.

Return code 16

Attempt to use DES first. If DES processing fails, use masking. This was the default behavior before z/OS V2R2 if no ICHDEX01 exit routine was installed.

When the KDFAES algorithm is active, masking is never used, thus no migration action is needed. RACF continues to call ICHDEX01 to evaluate a legacy password, but no longer honors masking. When a password is changed under KDFAES, the ICHDEX01 exit is no longer called for that password.

If your installation uses KDFAES encryption, it is recommended that you remove the ICHDEX01 exit routine, if it is no longer needed. For example, if the exit routine was used previously to always pass return code 8 (DES only), you can achieve the same result in z/OS V2R2 by removing the exit routine.

If your installation uses DES encryption, and you suspect there might be masked passwords in your RACF database, and you need to avoid any application outages that would result from the change in the

default behavior, you must install an ICHDEX01 exit that sets return code 16. IBM recommends, however, that you attempt to identify such passwords and change them so that they are encrypted using DES.

Table 159 on page 231 provides more details about this migration action. Use this information to plan your changes to the system.

Table 381. Information about this migration action

Element or feature:	Security Server.
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you have masked passwords in the RACF database.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	The health check RACF_ENCRYPTION_ALGORITHM (provided in APAR OA45608) raises an exception if weaker (less secure than DES) encryption is allowed for logon passwords.

Steps to take

Check for the existence of the ICHDEX01 exit routine in your RACF configuration. If it is present, determine whether you still need it. If not, remove it.

Follow these steps:

1. Check for the existence of the ICHDEX01 exit routine in your RACF configuration. During IPL, message ICH508I identifies the active exits. Check the message output for the presence of an ICHDEX01 exit routine. Or, run health check RACF_ENCRYPTION_ALGORITHM, which can detect return codes from an active ICHDEX01 exit routine.
2. If an ICHDEX01 exit routine is present, determine whether you still need it. Be aware that the masking algorithm provides weaker protection, as compared to KDFAES or DES.
3. Remove the exit routine if it is no longer needed. As an extra precaution, check for user profiles with old password change dates, which might indicate masked passwords. In these cases, you should either reset the password or delete it, rather than using the ICHDEX01 exit to preserve the usage of weak passwords. Use the RACF **LISTUSER** command to determine when passwords were last updated. Otherwise, if your installation uses DES encryption, and you suspect there might be masked passwords in your RACF database, and you need to avoid any application outages that would result from the change in the default behavior, you must install an ICHDEX01 exit routine that sets return code 16, which mimics the current default behavior. Here is an example of the exit code that you can use:

```
LA 15,16
BR 14
```

Note: IBM recommends that you use KDFAES encryption, rather than DES encryption or masking. KDFAES provides improved cryptographic strength in RACF password algorithm processing, and helps

Migration actions from z/OS V1R13: Security Server

to protect RACF password data if a copy of a RACF database becomes inadvertently accessible. KDFAES encryption was introduced by APAR OA43999 for z/OS V1R12, V1R13, and V2R1, which is deactivated by default.

Reference information

For more information, see *z/OS Security Server RACF System Programmer's Guide*.

Determine whether you define CHOWN.UNRESTRICTED in the UNIXPRIV class Description

Starting with z/OS V2R1, z/OS UNIX imposes a new restriction on certain sensitive types of executable files, namely, that the files be owned by UID(0). Generally, this is acceptable because the ability to change a file's owner is restricted to privileged users (those with UID 0 or with READ access to SUPERUSER.FILESYS.CHOWN in the UNIXPRIV class). However, the POSIX standard allows a user to change ownership of any file to another user or group.

RACF supports the POSIX standard with the CHOWN.UNRESTRICTED profile in the UNIXPRIV class. If the profile exists, the alternate POSIX implementation applies, and any user can transfer ownership of files to other users or groups.

This change requires at least UPDATE access to CHOWN.UNRESTRICTED in order to give a file that you own to UID(0). To give your file to a user with a UID other than 0, or to a group to which you are not connected, requires READ access.

Currently, CHOWN.UNRESTRICTED most likely has a universal access (UACC) of NONE. Some documented examples of creating this profile specify UACC(NONE) explicitly. Others do not, but the default UACC is NONE.

Although highly unusual, a client might have defined the profile with any UACC and might permit any number of users and groups with any access level. Thus, the most likely result of this change is a complete reversal of the recommended behavior of the profile, in that nobody will have the authority to change the owner of their files. On an individual basis, clients can permit specific users or groups to this profile in order to grant the original capability. Alternatively, they can simply change its UACC to READ, but IBM does NOT recommend this action.

Table 382 provides more details about this migration action. Use this information to plan your changes to the system.

Table 382. Information about this migration action

Element or feature:	Security Server.
When change was introduced:	z/OS V2R1. z/OS V1R13 and z/OS V1R12, both with APAR OA41364.
Applies to migration from:	z/OS V1R13 without APAR OA41364 applied.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	No, but recommended for system security.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

- Check that the profile for CHOWN.UNRESTRICTED in the UNIXPRIV class is defined as discrete by using the following command:

```
RLIST UNIXPRIV CHOWN.UNRESTRICTED ALL
```
- If this profile does not exist, there is nothing more that you need to do.
- If the profile does exist, the recommendation is to delete it by issuing the following command:

```
RDELETE UNIXRIV CHOWN.UNRESTRICTED SETROPTS RACLIST(UNIXPRIV) REFRESH
```

If you have users with a genuine need to change file owners, they can request that a privileged user do this for them. If you trust a user enough to preserve their ability to perform this action, you can permit such a user, or group of users to CHOWN.UNRESTRICTED in order to restore the ability they previously had. Before doing so, verify that the profile does not currently allow any inadvertent access by making sure the UACC value is NONE, and that there are no entries on the access list. To do that issue the following commands:

```
PERMIT CHOWN.UNRESTRICTED CLASS(UNIXPRIV) RESET
RALTER UNIXRIV CHOWN.UNRESTRICTED UACC(NONE)
SETROPTS RACLIST(UNIXPRIV) REFRESH
```

You can now permit users and groups as appropriate for your installation. Note that CHOWN.UNRESTRICTED must currently exist as a discrete profile. With the change from a switch profile to an authorization profile, the requirement for it to be discrete will continue to be enforced, so that inadvertent access is not granted through an existing generic profile.

Reference information

For more information, see the following references:

- DOC APAR OA41466
- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Security Server RACF Callable Services*
- *z/OS UNIX System Services Planning*

Security Server actions to perform after the first IPL of z/OS V2R2

This topic describes Security Server migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

Update database templates

Description

To ensure that the RACF utilities function properly, use the IRRMIN00 utility to update the test and production RACF databases with the database templates for the current release level.

Table 160 on page 233 provides more details about this migration action. Use this information to plan your changes to the system.

Table 383. Information about this migration action

Element or feature:	Security Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	After the first IPL of z/OS V2R2.
Is the migration action required?	Yes.

Migration actions from z/OS V1R13: Security Server

Table 383. Information about this migration action (continued)

Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

To install the database template updates, run the IRRMIN00 utility with PARM=UPDATE.

Tip: The RACF database templates have been updated for z/OS V2R2. The templates contain a version string with a value of HRF77A0 00000194.00000022.

Note: If IRRMIN00 produces a return code of 4 and message IRR8025 PARM=UPDATE specified, but template update not required, you do not necessarily have a problem. Check that your JCL points to the new level of IRRMIN00. If it does, ignore the return code and warning message. A PTF might have already brought your templates up to the current level for the new release. If your JCL accidentally points to an old copy of IRRMIN00, correct the JCL and run IRRMIN00 again.

Reference information

For more information, see the following references:

- *z/OS Program Directory* at the z/OS installation related information website
- *ServerPac: Installing Your Order*
- *z/OS Security Server RACF System Programmer's Guide*

TSO/E migration actions

This topic describes migration actions for the base element Time Sharing Option/Extensions (TSO/E).

TSO/E actions to perform before installing z/OS V2R2

This topic describes TSO/E migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Consider the behavior of an empty data set in concatenation

Description

When EXECIO is used to read a DD consisting of a concatenation of 2 or more data sets, that concatenation might contain empty sequential data sets (as of V2R1) as long as any empty data sets are SMS managed.

- Before V2R1, REXX EXECIO would fail with RC=4 if EXECIO was used with DISKR or DISKRU to read a DD consisting of a concatenation of 2 or more data sets where one of the data sets was an empty (null) sequential data set.
- Starting with V2R1, REXX EXECIO can read (using DISKR or DISKRU) a DD even if one or more of the data sets within that DD concatenation is an empty data set, as long as all empty data sets within the concatenation are SMS managed empty data sets. If the DD concatenation contains a non-SMS managed empty data set, EXECIO will still fail the read request with RC=4 and messages IRX0670E and IRX0566E.

Table 384 provides more details about this migration action. Use this information to plan your changes to the system.

Table 384. Information about this migration action

Element or feature:	TSO/E
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you depend upon the behavior that occurred before z/OS V2R1.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

This item is intended to alert users of EXECIO to a behavioral change that might occur due to a relaxing of the restriction on null data sets within a concatenation being read by EXECIO DISKR or DISKRU. If your exec tests the EXECIO return code and handles RC=4, you will likely have no action that needs to be taken. The RC=4 that was previously returned when EXECIO detected a null data set within the DD concatenation being read by EXECIO is still a possible return code, if the concatenation contains a null data set which is not SMS managed. Yet, if the EXECIO read against a DD containing a null data set completes successfully (i.e. RC=0 or 2), you would typically have no exceptional action to take, since the read operation will have worked as if the empty data set were not even present.

On the other hand, if you have an exec that expects EXECIO to fail whenever it reads a concatenation containing a null data set, and you exec depends on this EXECIO read failure, you should now look for RC=0 or RC=2 to allow for the possibility of success.

For example, if you use EXECIO RC=4 and the associated message IRX0566E to determine whether a DD concatenation contains a null data set, this will no longer work if the null data set is an SMS managed sequential data set. The read would work (RC=0). You could still determine if a data set is empty by allocating that data set alone to a DD and reading it with EXECIO. RC=2 (or RC=0, if execio * were used) and zero records read would indicate that the data set was empty.

Note: Note that EXECIO against a single null data set that is not part of a multi data set concatenation has always worked successfully, regardless of whether or not the empty data set is SMS managed.

Reference information

For more information, see the following references:

- For details about EXECIO see, *z/OS TSO/E REXX Reference*
- For details about messages IRX0670E and IRX0566E, see *z/OS TSO/E Messages*.

TSO/E actions to perform before the first IPL of z/OS V2R2

This topic describes TSO/E migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Migration actions from z/OS V1R13: TSO/E

None.

TSO/E actions to perform after the first IPL of z/OS V2R2

This topic describes TSO/E migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

XL C/C++ migration actions

This topic describes migration actions for optional feature XL C/C++.

XL C/C++ actions to perform before installing z/OS V2R2

This topic describes XL C/C++ migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Review the XL C/C++ Migration Guide for the Application Programmer Description

Review the publication *z/OS XL C/C++ Compiler and Runtime Migration Guide for the Application Programmer* for any z/OS C/C++ migration actions. It is written for application programmers, whereas this publication (*z/OS Migration*) is written for system programmers. In some customer locations, job scope can overlap such that system programmers might find information in the XL C/C++ publication that is relevant to their responsibilities. For example, migration information related to the c89 utility in the XL C/C++ publication could be of interest.

Table 161 on page 234 provides more details about this migration action. Use this information to plan your changes to the system.

Table 385. Information about this migration action

Element or feature:	XL C/C++
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended if you use XL C/C++.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

For migration information that is relevant to your installation, see *z/OS XL C/C++ Compiler and Runtime Migration Guide for the Application Programmer* .

Reference information

For more information, see *z/OS XL C/C++ Compiler and Runtime Migration Guide for the Application Programmer*.

XL C/C++ actions to perform before the first IPL of z/OS V2R2

This topic describes XL C/C++ migration actions that you can perform only before you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

XL C/C++ actions to perform after the first IPL of z/OS V2R2

This topic describes XL C/C++ migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

z/OS Font Collection migration actions

This topic describes migration actions for the base z/OS Font Collection.

z/OS Font Collection actions to perform before installing z/OS V2R2

This topic describes z/OS Font Collection actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

z/OS Font Collection actions to perform before the first IPL of z/OS V2R2

This topic describes z/OS Font Collection migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Stop using old fonts and start using fonts from the z/OS Font Collection

Description

Starting with z/OS V2R1, z/OS contains a new base element: z/OS Font Collection. The z/OS Font Collection provides fonts that were previously marketed and serviced for z/OS, including both single-byte and double-byte fonts. The FMIDs for the earlier font products that z/OS Font Collection replaces are listed in *z/OS Planning for Installation*.

The z/OS Font Collection includes:

- AFP Font Collection for S/390 (5648-B33), includes Japanese, Korean, Traditional Chinese, and Simplified Chinese
- IBM Infoprint Fonts for z/OS (5648-E76), includes Japanese, Korean, Traditional Chinese, and Simplified Chinese
- PSF Compatibility Font feature (5655-M32), includes just the PSF feature for the compatibility fonts, not the executable code or the entire product
- World Type fonts that were not previously available in the z/OS environment. These fonts were part of the InfoPrint Font Collection V3.1 available on other platforms. A Subset of TrueType fonts from the World Type library are provided in Infoprint Transforms to AFP for z/OS V2.3 (5655-N60).

Migration actions from z/OS V1R13: z/OS Font Collection

- Selected object fonts (not source), Pi and Special (5771-ABC), Math and Science (5771-ADT)

Now that z/OS is assuming ownership of the z/OS Font Collection, you no longer need to order the previous standalone products as of z/OS V2R1.

Table 386 provides more details about this migration action. Use this information to plan your changes to the system.

Table 386. Information about this migration action

Element or feature:	z/OS Font Collection
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use any of the following stand-alone program products for fonts with your z/OS system: <ul style="list-style-type: none">• Print Services Facility (PSF), PN 5655-M32• AFP Conversion and Indexing Facility (ACIF), optional feature of PSF• IBM Print Transform from AFP to PCL for Infoprint Server for z/OS, PN 5655-TF2• IBM Print Transform from AFP to PDF for Infoprint Server for z/OS, PN 5655-TF1• IBM Print Transform from AFP to PostScript for Infoprint Server for z/OS, PN 5655-TF3
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

The z/OS Font Collection, for migration and compatibility with previously available font program products, will continue to use existing font libraries, and will have some new libraries. IBM recommends you use the latest level of the fonts available for z/OS, and therefore, those that are found in the z/OS Font Collection. For that reason, do not continue to use the standalone font program product data sets with z/OS releases after z/OS V1R13. No application or program changes are anticipated.

Do not expect to order separately available font program products with z/OS V2R2, or to install them into the z/OS V2R2 SMP/E zones. The z/OS Font Collection provides SMP/E statements to supercede, delete, or version the earlier standalone program product levels of the fonts.

Ensure that you are using the font libraries for z/OS Font Collection instead of the font libraries for the earlier font products. If you refer to the SYS1.FONTOLN font library for AFP outline fonts, replace the references with SYS1.SFNTILIB, which is the AFP outline font library for z/OS Font Collection. Look in these product locations for references:

PSF Startup procedure

ACIF FONTLIB DD statement

Print Transforms from AFP for Infoprint Server

Infoprint Server transform configuration file (aopxfd.conf)

Reference information

For information about how to edit font library locations, see:

- *PSF for z/OS: Customization, S550-0427*
- *AFP Conversion and Indexing Facility User's Guide, S550-0436*
- *IBM Print Transforms from AFP for Infoprint Server for z/OS, G325-2634*

For details about the z/OS Font Collection, see *z/OS Font Collection*.

For installation planning information, see *z/OS Planning for Installation*.

Use the font libraries that are shipped in z/OS V2R2 Description

z/OS Font Collection, a new element in z/OS V2R1, replaces earlier font products you might be using in z/OS V1R13. The FMIDs for the earlier font products that z/OS Font Collection replaces are listed in *z/OS Planning for Installation*.

Ensure that you are using the font libraries for z/OS Font Collection instead of the font libraries for the earlier font products. If you refer to the SYS1.FONTOLN font library for AFP outline fonts, replace the references with SYS1.SFNLIB, which is the AFP outline font library for z/OS Font Collection.

Table 162 on page 235 provides more details about this migration action. Use this information to plan your changes to the system.

Table 387. Information about this migration action

Element or feature:	z/OS Font Collection
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you reference the SYS1.FONTOLN font library for AFP outline fonts. These products might reference SYS1.FONTOLN: <ul style="list-style-type: none"> • Print Services Facility (PSF), PN 5655-M32 • AFP Conversion and Indexing Facility (ACIF), optional feature of PSF • IBM Print Transform from AFP to PCL for Infoprint Server for z/OS, PN 5655-TF2 • IBM Print Transform from AFP to PDF for Infoprint Server for z/OS, PN 5655-TF1 • IBM Print Transform from AFP to PostScript for Infoprint Server for z/OS, PN 5655-TF3
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Migration actions from z/OS V1R13: z/OS Font Collection

Steps to take

Replace all references to SYS1.FONTOLN with SYS1.SFNLIB. Look in these product locations for references:

PSF Startup procedure

ACIF FONTLIB DD statement

Print Transforms from AFP for Infoprint Server

Infoprint Server transform configuration file (aopxfd.conf)

Reference information

For information about how to edit font library locations, see:

- *PSF for z/OS: Customization, S550-0427*
- *AFP Conversion and Indexing Facility User's Guide, S550-0436*
- *IBM Print Transforms from AFP for Infoprint Server for z/OS, G325-2634*

For more information about the z/OS Font Collection, see *z/OS Font Collection*.

z/OS Font Collection actions to perform after the first IPL of z/OS V2R2

This topic describes z/OS Font Collection migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

z/OS OpenSSH migration actions

This topic describes migration actions for base element z/OS OpenSSH.

z/OS OpenSSH actions to perform before installing z/OS V2R2

This topic describes z/OS OpenSSH migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

None.

z/OS OpenSSH actions to perform before the first IPL of z/OS V2R2

This topic describes z/OS OpenSSH migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

None.

z/OS OpenSSH actions to perform after the first IPL of z/OS V2R2

This topic describes z/OS OpenSSH migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

Accommodate the OpenSSH ported level Description

Before z/OS V2R2 and IBM Ported Tools for z/OS V1R3, OpenSSH was version 5.0p1. Starting with z/OS V2R2 and IBM Ported Tools for z/OS V1R3, OpenSSH is version 6.4p1.

Before z/OS V2R2, OpenSSH was available from IBM Ported Tools for z/OS. Starting with z/OS V2R2, it is now available as a base element of z/OS.

Table 163 on page 237 provides more details about this migration action. Use this information to plan your changes to the system.

Table 388. Information about this migration action

Element or feature:	OpenSSH
When changes were introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13, both with IBM Ported Tools for OpenSSH V1R2.
Timing:	After the first IPL of z/OS V2R2.
Are the migration actions required?	Yes, if any of the changes in “Steps to take” on page 237 are applicable to your environment.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

The following is a list of potential migration actions for the OpenSSH base element:

- “Changes to the ssh-rand-helper command that might require a migration action” on page 237
- “Changes to the sftp command that might require a migration action” on page 238
- “Changes to the ssh command that might require a migration action” on page 238
- “Changes to the ssh, sftp or scp client commands that might require a migration action” on page 238
- “Changes to the ssh_config file that might require a migration action” on page 239
- “Changes to the sshd command that might require a migration action” on page 239
- “Changes to the ssh, sftp or scp client commands that might require a migration action” on page 238
- “Changes to the sshd_config file that might require a migration action” on page 239
- “Changes to the ssh-keygen command that might require a migration action” on page 240
- “Changes to the ssh-keyscan command that might require a migration action” on page 240
- “Changes to the users running ssh, sftp or scp client commands that might require a migration action” on page 240
- “Changes to /samples/ssh_smf.h and FOTSMF77 in SYS1.MACLIB that might require a migration action” on page 241

Changes to the sftp command that might require a migration action: Table 165 on page 238 lists the changes to the **sftp** command that might require a migration action and the accompanying actions.

Migration actions from z/OS V1R13: z/OS OpenSSH

Table 389. Changes to the sftp command that might require a migration action

What changed	Migration action needed?
<p>The -P option</p> <p>Previously, this option was used to specify the <code>sftp_server_path</code>. Now, this option is used to specify the port to connect to on the remote host.</p>	<p>Yes, if you specify the <code>sftp_server_path</code>. If you specify -P <code>sftp_server_path</code>, the following message is returned: FOTS1401 filename line number: Bad line number</p> <p>Action: Use the -D option to specify the <code>sftp_server_path</code>.</p>
<p>ln and symlink subcommands</p> <p>Previously, the ln and symlink subcommands created a symbolic link from <i>oldpath</i> to <i>newpath</i> on the remote host. Now, if the -s flag is specified, the created link is a symbolic link. Otherwise it is a hard link.</p>	<p>Yes, if you create a symbolic link.</p> <p>Action: Run the sftp ln subcommand with the -s flag to create a symbolic link or create a hard link without the flag.</p>

Changes to the ssh command that might require a migration action: Table 166 on page 238 lists the changes to the `ssh` command that might require a migration action and the accompanying actions.

Table 390. Changes to the ssh command that might require a migration action

What changed	Migration action needed?
<p>The -I option</p> <p>Previously, the argument was the device that <code>ssh</code> should use to communicate with a smart card used for storing the user's private RSA key. Now, the argument is the PKCS#11 shared library <code>ssh</code> should use to communicate with a PKCS#11 token providing the user's private RSA key.</p>	<p>No, because the option (-I <code>smartcard_device</code>) is not supported on z/OS systems.</p>
<p>The -R options</p> <p>Previously, the port argument "0" was not supported. Now, if the port argument is "0", the listen port will be dynamically allocated on the server and reported to the client at run time.</p>	<p>No, setting the port argument to 0 was considered to be illegal in the previous version.</p>

Changes to the ssh, sftp or scp client commands that might require a migration action: Table 167 on page 238 lists the changes to the `ssh` command that might require a migration action and the accompanying actions.

Table 391. Changes to the users running the ssh, sftp, or scp client commands that might require a migration action

What changed	Migration action needed?
<p>Users running <code>ssh</code>, <code>sftp</code>, or <code>scp</code> client commands when collecting SMF records.</p> <p>New SMF subtype records have been added, which requires additional setup.</p>	<p>Yes, if you use <code>ssh</code>, <code>sftp</code>, or <code>scp</code> client commands to collect SMF records.</p> <p>Set up the users who run <code>ssh</code>, <code>sftp</code>, or <code>scp</code> client commands to have READ access to the BPX.SMF SAF profile. For example:</p> <pre>RDEFINE FACILITY BPX.SMF UACC(NONE) PERMIT BPX.SMF CLASS(FACILITY) ID(userid) ACCESS(READ) SETROPTS RACLIST(FACILITY) REFRESH</pre>

Changes to the ssh_config file that might require a migration action: Table 168 on page 239 lists the changes to the `ssh_config` file that might require a migration action and the accompanying actions.

Table 392. Changes to the ssh_config file that might require a migration action

What changed	Migration action needed?
<p>The ControlPath keyword</p> <p>Previously, %l in the path was substituted by the local host name. Now, %l in the path is substituted by the local host name (including any domain name).</p>	<p>Yes, if you want to use substitute character to substitute the local host name without any domain name.</p> <p>Action: Use the %L in the path to substitute the first component of the local host name.</p>
<p>The RemoteForward keyword</p> <p>Previously, the port argument "0" was not supported. Now, if the port argument is "0", the listen port will be dynamically allocated on the server and reported to the client at run time.</p>	<p>No, set the port argument to 0 was considered to be illegal in the previous version.</p>
<p>The RhostsAuthentication keyword</p> <p>Previously, this option was supported for protocol version 1. Now this option is no longer supported for protocol version 1 on z/OS UNIX.</p>	<p>Yes, if you use RhostsAuthentication for protocol version 1 in your application. When setting this, you will receive the following message: filename line line_number: Deprecated option keyword.</p> <p>Action: Update your application.</p>

Changes to the sshd command that might require a migration action: Table 169 on page 239 lists the changes to the sshd command that might require a migration action and the accompanying actions.

Table 393. Changes to the sshd command that might require a migration action

What changed	Migration action needed?
<p>The -b option</p> <p>Previously, the default number of bits in the ephemeral protocol version 1 server key was 768. Now, the default number of bits in the ephemeral protocol version 1 server key is 1024.</p>	<p>Yes, if you use the ephemeral protocol version 1 server key which is 768 bits.</p> <p>Action: Start the sshd daemon with specifying -b 768.</p>

Changes to the sshd_config file that might require a migration action: Table 170 on page 239 lists the changes to the sshd_config file that might require a migration action and the accompanying actions.

Table 394. Changes to the sshd_config file that might require a migration action

What changed	Migration action needed?
<p>The RhostsAuthentication keyword</p> <p>Previously, this option was supported for protocol version 1. Now, this option is no longer supported for protocol version 1 on z/OS Unix.</p>	<p>Yes, if you use RhostsAuthentication for protocol version 1 in your application. When setting it, the following message is returned: FOTS2374 filename line line_number: Deprecated option keyword" is returned.</p> <p>Action: Update your application.</p>
<p>The ServerKeyBits keyword</p> <p>Previously, the default number of bits in the ephemeral protocol version 1 server key was 768. Now, the default number of bits in the ephemeral protocol version 1 server key is 1024.</p>	<p>Yes, if you use the ephemeral protocol version 1 server key which is 768 bits.</p> <p>Action: Start the sshd daemon with specifying -b 768, if you want to use the old default.</p>

Changes to the ssh-keygen command that might require a migration action: Table 171 on page 240 lists the changes to the ssh-keygen command that might require a migration action and the accompanying actions.

Migration actions from z/OS V1R13: z/OS OpenSSH

Table 395. Changes to the `ssh-keygen` command that might require a migration action

What changed	Migration action needed?
<p>-d option</p> <p>Previously, -d option as alias of -t dsa was supported. Now, it is not supported.</p>	<p>Yes, if you use ssh-keygen command with -d option. Specifying the -d option will return the following error message: unknown option -- d.</p> <p>Action: Replace -d by -t dsa.</p>
<p>-b option (used in conjunction with -G)</p> <p>Previously, the minimum value on the ssh-keygen -b option used with -G options was 768. Now the minimum value is 512.</p>	<p>No. Because minimum value 512 is less than 768.</p>
<p>-b option (for RSA)</p> <p>Previously, the maximum RSA key size on the ssh-keygen -b option was 32768. Now the maximum size is 16384.</p>	<p>Yes, if you are using ssh-keygen to generate RSA keys with a size that is between 16384 and 32768 bits. If you specify an RSA key size larger than 16384, the following error message will be returned: key bits exceeds maximum 16384.</p> <p>Action: Use ssh-keygen to generate new RSA keys based on the new size requirement.</p>

Changes to the `ssh-keyscan` command that might require a migration action: Table 172 on page 240 lists the changes to the `ssh-keyscan` command that might require a migration action and the accompanying actions.

Table 396. Changes to the `ssh-keyscan` command that might require a migration action

What changed	Migration action needed?
<p>The -t option</p> <p>Previously, if the -t option was not specified, ssh-keyscan searches only for SSH protocol version 1 keys ("rsa1") by default. Now, if the -t option is not specified, ssh-keyscan searches only for SSH protocol version 2 "rsa" and "ecdsa" keys by default.</p>	<p>Yes, if you search protocol version 1 keys ("rsa1") without specifying -t option.</p> <p>Action: Search protocol version 1 keys ("rsa1") with specifying -t rsa1 .</p>

Changes to the users running `ssh`, `sftp` or `scp` client commands that might require a migration action: Table 173 on page 240 lists the changes to the users running the `ssh`, `sftp`, or `scp` commands that might require a migration action and the accompanying actions.

Table 397. Changes to the users running `ssh`, `sftp` or `scp` client commands that might require a migration action

What changed	Migration action needed?
<p>Users running ssh, sftp or scp client commands when collecting SMF records.</p> <p>New SMF subtype records have been added which requires additional setup.</p>	<p>Yes, if you use ssh, sftp or scp client commands to collect SMF records.</p> <p>Action: Setup the users who run ssh, sftp or scp client commands to have READ access to the BPX.SMF SAF/RACF profile. For example:</p> <pre>RDEFINE FACILITY BPX.SMF UACC(NONE) PERMIT BPX.SMF CLASS(FACILITY) ID(userid) ACCESS(READ) SETROPTS RACLIST(FACILITY) REFRESH</pre>

Changes to the `ssh-rand-helper` command that might require a migration action: Table 164 on page 237 lists the changes to the `ssh-rand-helper` command that might require a migration action and the accompanying actions.

Table 398. Changes to the `ssh-rand-helper` command that might require a migration action

What changed	Migration action needed?
<p>The <code>ssh-rand-helper</code> command</p> <p>Now, the <code>ssh-rand-helper</code> is not supported.</p>	<p>Yes. If no migration action, the following message is returned: FOTS1949 PRNG is not seeded. Please activate the Integrated Cryptographic Service Facility (ICSF).</p> <p>Action: The new OpenSSH requires that a working <code>/dev/random</code> device be available to all OpenSSH client and server jobs. This requires that ICSF be configured to support <code>/dev/random</code> and that users have SAF authority to the CSFRNG service.</p>

Changes to `/samples/ssh_smf.h` and FOTSMF77 in SYS1.MACLIB that might require a migration action: Table 174 on page 241 lists the changes to `/samples/ssh_smf.h` and FOTSMF77 in SYS1.MACLIB that might require a migration action and the accompanying actions.

Table 399. Changes to `/samples/ssh_smf.h` and FOTSMF77 in SYS1.MACLIB that might require a migration action

What changed	Migration action needed?
<p><code>/samples/ssh_smf.h</code> and SYS1.MACLIB(FOTSMF77)</p> <p>Now, new Ciphers and MACs, new subtypes (Client Connection Started 94 and Server Connection Started 95), and SFTP target path have been updated to the <code>ssh_smf.h</code> and FOTSMF77.</p> <p>For more information, see the topic on SMF Type 119 records in <i>IBM Ported Tools for z/OS: OpenSSH User's Guide</i>.</p>	<p>Yes, if you use <code>ssh_smf.h</code> and FOTSMF77.</p> <p>Action: Update your application.</p>

z/OS UNIX migration actions

This topic describes migration actions for base element z/OS UNIX System Services (z/OS UNIX).

z/OS UNIX actions to perform before installing z/OS V2R2

This topic describes z/OS UNIX migration actions that you can perform on your current (old) system. You do not need the z/OS V2R2 level of code to make these changes, and the changes do not require the z/OS V2R2 level of code to run once they are made.

Remove ICLI component from z/OS

Description

IBM removed the Integrated Call Level Interface (ICLI) in z/OS V2R1. ICLI is used by those who have requested and obtained the ICLI API documentation and the C language header file. IBM believes that users of this interface have changed from using ICLI to standard IBM DB2 Connect for database connectivity and do not need it for z/OS V2R2. ICLI has not been enhanced since z/OS V1R6.

Table 400 provides more details about this migration action. Use this information to plan your changes to the system.

Table 400. Information about this migration action

Element or feature:	z/OS UNIX.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.

Migration actions from z/OS V1R13: z/OS UNIX

Table 400. Information about this migration action (continued)

Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use ICLI.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

The PTF UA67900 for APAR OA41143 provides the ability to track the usage of ICLI on your systems. On pre-z/OS V2R1 systems, the operator command `DISPLAY OPDATA,TRACKING` shows the following tracking information for the ICLI servers 3.1I, 4.0B, 4.5B and 4.6D when these servers have been started on your system after you have activated the tracking facility through the `SETCON TRACKING=ON` command:

```
ICLI server for SAP 3.1I .... FOME31IS ...
ICLI server for SAP 4.0B .... FOME40BS ...
ICLI server for SAP 4.5B .... FOME45BS ...
ICLI server for SAP 4.6D .... FOME46DS ...
```

You can display the tracking information to determine if your system is using an ICLI server, and whether you will be affected by its removal in z/OS V2R1.

Reference information

For more information, see *z/OS Planning for Installation*.

Ensure that your applications do not use removed z/OS UNIX APIs

Description

Before z/OS V2R1, certain z/OS UNIX application programming interfaces (APIs) were available. Starting with z/OS V2R1, they are no longer available.

Table 401 provides more details about this migration action. Use this information to plan your changes to the system.

Table 401. Information about this migration action

Element or feature:	z/OS UNIX.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if your installation has C/C++ or Assembler language applications that explicitly invoke z/OS UNIX application programming interfaces.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.

Table 401. Information about this migration action (continued)

System impacts:	This change does not affect the z/OS system itself but might cause applications or products other than z/OS to give erroneous results or behave unexpectedly.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Check three interfaces to see if the removed services are being used.

1. Scan the source code for use of the following z/OS UNIX application programming interfaces:
 - The `_osenv()` syscall
 - For Assembler language programs, search for BPX1OSE and BPX4OSE.
 - For C or C++ code, search for calls to the `_osenv()` service.
 - The `pthread_quiesce_and_get_np()` syscall
 - For Assembler language programs, search for BPX1PQG and BPX4PQG.
 - For C or C++ code, search for calls to the `pthread_quiesce_and_get_np()` service.
 - The `QUICK_FREEZE_EXIT_REG` option of `oe_env_np()`
 - For Assembler language programs, search for BPX1ENV and BPX4ENV.
 - There is no C/C++ interface that allows direct use of the `QUICK_FREEZE_EXIT_REG` option. If you find use of the BPX1ENV or BPX4ENV service, check whether the `QUICK_FREEZE_EXIT_REG` option is specified. If you do use this option, verify that you have code that invokes the `pthread_quiesce_and_get_np()` service (in XL C/C++) or calls BPX1PQG or BPX4PQG. If you do not have code that calls the `pthread_quiesce_and_get_np()` service, then you do not need to invoke the BPX1ENV or BPX4ENV service with the `QUICK_FREEZE_EXIT_REG` option. Remove that call from your application.
2. If your applications use any of these interfaces, update the applications to either eliminate the calls or handle the new return code and reason code that the removed interfaces will return.

Reference information

For more information, see the following references:

- *z/OS UNIX System Services Programming: Assembler Callable Services Reference*
- *z/OS XL C/C++ Runtime Library Reference*

Use the BPX.UNIQUE.USER profile instead of BPX.DEFAULT.USER

Description

Before z/OS V1R11, if the BPX.DEFAULT.USER profile in the FACILITY class was defined, users who accessed z/OS UNIX services who did not have an OMVS user or group segment were assigned the default OMVS segments for the length of the user session. All users of the default OMVS segments shared the same UID and GID. As of z/OS V1R11, if BPX.UNIQUE.USER has been defined, users who access z/OS UNIX services who do not have an OMVS user or group segment are automatically assigned an OMVS segment with a unique UID and GID. The new OMVS segments are added to the user and group profiles in the RACF database. As of z/OS V2R1, the support of BPX.DEFAULT.USER was removed.

Table 402 provides more details about this migration action. Use this information to plan your changes to the system.

Table 402. Information about this migration action

Element or feature:	z/OS UNIX.
---------------------	------------

Migration actions from z/OS V1R13: z/OS UNIX

Table 402. Information about this migration action (continued)

When change was introduced:	z/OS V2R1. See IBM United States Software Announcement 211-007, dated February 15, 2011.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you use BPX.DEFAULT.USER profile in the FACILITY class.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	You need AIM Stage 3 to use the BPX.UNIQUE.USER profile. You can run the IRRIRA00 utility to determine the current AIM Stage in your RACF database and increase the level to AIM Stage 3.
System impacts:	None.
Related IBM Health Checker for z/OS check:	Use check ZOSMIGV2R1_DEFAULT_UNIX_ID introduced in APAR OA37164. This check determines if you are relying on assigning default z/OS UNIX identities for users without OMVS segments.

Steps to take

Follow the steps in *z/OS UNIX System Services Planning* to set up the BPX.UNIQUE.USER profile. If BPX.DEFAULT.USER has not been deleted, BPX.UNIQUE.USER takes precedence when default OMVS segments are used.

To remove the BPX.DEFAULT.USER profile, use the following RACF commands:

```
RDELETE FACILITY BPX.DEFAULT.USER  
SETROPTS RACLIST(FACILITY) REFRESH
```

RACF APAR OA42554 provides assistance with the conversion to BPX.UNIQUE.USER on z/OS V1R13. With this APAR you can model the user's home directory path by specifying &racuid in the model user's OMVS segment. Then, when the user's OMVS segment is automatically created, RACF will substitute the correct user ID. For more information on this capability, see the information in APAR OA42554.

Reference information

For more information, see the following references:

- *z/OS UNIX System Services Command Reference*
- *z/OS Security Server RACF Security Administrator's Guide*

Accommodate the new Shell and Utilities version of the zlsnf utility

Description

Before z/OS V2R1, the **zlsnf** utility was obtained from the Tools and Toys section of the z/OS UNIX website. Starting with z/OS V2R1, Shell and Utilities support of the **zlsnf** utility has been added. The supported version differs from the Tools and Toys version in a number of ways. For example, the new **zlsnf** version includes support for displaying file lock holders and waiters when the byte range lock manager is used.

Table 403 on page 497 provides more details about this migration action. Use this information to plan your changes to the system.

Table 403. Information about this migration action

Element or feature:	z/OS UNIX.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you currently use the Tools and Toys version of the z1sof utility.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Look for current use of the Tools and Toys version of **z1sof**. If there is no current use of the Tools and Toys version of **z1sof**, then no actions or changes are required.

If there is current usage of the Tools and Toys version of **z1sof**, determine if the command is in `/bin`, or in another directory. Also, determine if you want to preserve the Tools and Toys version in addition to the officially shipped version. Note that **z1sof** can also reside in data sets where rexx execs can be run.

1. If you want to preserve the Tools and Toys version, ensure that you save it into a directory that z/OS V2R1 will not install into. z/OS V2R1 provides **z1sof** in the `/bin` directory.
2. If you do not want to preserve the Tools and Toys version and it is in `/bin`, then the installation of z/OS V2R1 automatically replaces the Tools and Toys version with the new officially supported version. If the Tools and Toys version is not in `/bin`, remove it from its current location.

Reference information

For more information about the **z1sof** command, see *z/OS UNIX System Services Command Reference*.

Migrate from HFS file systems to zFS file systems

Description

Before z/OS V1R7, the HFS file system was the primary hierarchical file system. As of z/OS V1R7, you can use any combination of HFS and zFS file systems. Because zFS has higher performance characteristics than HFS and is the strategic file system, you should migrate your HFS file systems to zFS.

The HFS and zFS file system types in mount statements and command operands are now generic file system types that can mean either HFS or zFS. Based on the data set type, the system will determine which is appropriate. But note that you must still specify a type (HFS or zFS and it cannot be defaulted), and if the type you specify is not correct for the file system being mounted, any associated parameter string setting in the mount statement or command is ignored, even though the system sets the type correctly and processes the mount.

Table 175 on page 241 provides more details about this migration action. Use this information to plan your changes to the system.

Table 404. Information about this migration action

Element or feature:	z/OS UNIX.
---------------------	------------

Migration actions from z/OS V1R13: z/OS UNIX

Table 404. Information about this migration action (continued)

When change was introduced:	z/OS Distributed File Service zFS became the strategic file system in z/OS V1R7.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	No, but recommended because the action is planned to become a requirement in a future release. zFS is the strategic file system for z/OS UNIX and continues to be enhanced to provide superior performance, reliability, and data integrity. z/OS V2R2 supports HFS file systems.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	<ul style="list-style-type: none">• Understand the zFS recommendations and limits. For more information, see “Minimum and maximum file sizes” in <i>z/OS Distributed File Service zFS Administration</i>• The DDNAME() keyword of the BPXPRMxx ROOT and MOUNT statements is not supported by zFS. Use the FILESYSTEM(<i>name</i>) keyword instead.
System impacts:	None.
Related IBM Health Checker for z/OS check:	Use check USS_HFS_DETECTED to verify all file systems mounted. This check issues exception message BPXH068E if any HFS file systems are found.

Steps to take

Follow these steps:

1. Before beginning the migration, do the following:
 - Ensure that the PTF for APAR OA46639 is installed on your system. This APAR corrects a problem that can occur when socket type files are copied.
 - Establish backout procedures.
 - Decide on naming conventions.
 - Decide on unavailability.
 - Understand any cloning or deployment changes required by zFS systems being linear data sets. Considerations would include any copy utility invocations, BPXPRMxx specifications for symbolics, and placement of zFS file systems on system volumes.
2. Perform the conversion from an HFS to zFS file system.

You can use the BPXWH2Z tool to perform the conversion. It is an ISPF-based tool that migrates HFS file systems to zFS file systems. Using its panel interface, you can alter the space allocation, placement, SMS classes, and data set names. A HELP panel is provided. With this tool, you can:

- Migrate HFS file systems (both mounted and unmounted) to zFS file systems. If the HFS being migrated is mounted, the tool automatically unmounts it and then mounts the new zFS file system on its current mount point.
- Define zFS aggregates by default to be approximately the same size as the HFS. The new allocation size can also be increased or decreased. In z/OS V1R13, ZFS could require up to four times (4X) the space that HFS did; therefore, for z/OS V2R1 be sure to allocate more space. See zFS: Accommodate new DASD space requirements.
- Have the migration run in TSO/E foreground or UNIX background.

You can use the JCL sample ISPBTCH in SYS1.SAMPLIB to invoke BPXWH2Z as an ISPF batch job. Before you run the job, read the Notes section. When you run BPXWH2Z on your z/OS system, make sure it uses that same z/OS level of the pax command. You can manually migrate from an HFS to zFS file system without using the tool. However, you would need to allocate and format the target zFS file systems.

You can use the JCL sample ISPBTCH in SYS1.SAMPLIB to invoke BPXWH2Z as an ISPF batch job. Before you run the job, read the notes section. When you run BPXWH2Z on your z/OS V1R13 system, it uses the z/OS V1R13 level of the **pax** command. This level was enhanced in z/OS V1R7 for sparse file support and other characteristics that are of concern when migrating from an HFS to zFS file system. You can manually migrate from an HFS to zFS file system without using the tool. However, you would need to allocate and format the target zFS file systems.

Requirement: The BPXWH2Z tool requires the zFS address space to be operational. Therefore, before attempting to migrate existing HFS to zFS file systems using BPXWH2Z, make sure that the zFS address space has been successfully configured and initialized.

Tip: You can dynamically migrate the HFS sysplex root in a shared file system configuration to zFS while the root is in use, without disrupting workloads. Although the shared file system configuration is required, the sysplex can be a single system. For the steps involved in migrating the sysplex root file system from HFS to zFS, see “Migrating the sysplex root file system from HFS to zFS after IPLing z/OS V1R12”.

3. Change policies and scripts, and so forth, to reflect the change from the HFS file system to zFS file system. Use the RMF Monitor III option to report on zFS activity. Refer to migration action “Monitor the zFS file system activity” for information on gathering zFS activity in RMF Monitor III.

Tip: Use the RMF Monitor III option to report on zFS activity.

4. The DDNAME(name) keyword of the BPXPRMxx ROOT and MOUNT statements is not supported by zFS. If you use them, change these statements to use the FILESYSTEM(name) keyword instead.

Migrating the sysplex root file system from HFS to zFS after IPLing your previous z/OS system:

Before you begin the migration:

- Ensure that the following requirements have been met:
 - All systems in the sysplex are at the V1R12 level.
 - The current sysplex root file system PFS, and the new sysplex root file system PFS, are up in all the systems in shared file system configuration.
- Be aware of the following restrictions:
 - The current sysplex root file system must be mounted as a read-only file system.
 - The systems that do not meet the requirements for this migration action cannot join the sysplex during the sysplex root file system migration processing, but they can join the sysplex after the sysplex root migration has completed.
 - The current sysplex root and the new sysplex root must be either HFS or zFS in any combination. If the new sysplex root is zFS, then it must be HFS-compatible.
 - The sysplex root or any directories on it cannot have been exported by the DFS or SMB server.
- Note the following:
 - Remote NFS mounts of the sysplex root or any directories on it are considered active use of the current sysplex root file system.
 - During the migration, the new zFS sysplex root file system must not be HSM-migrated, mounted, or in use.
 - Mount parameters are preserved during the migration or replacement of the sysplex root file system of the same file system type (PFS). They are dropped if the file system type is different.
 - Directories, data, files, and links are not copied from one file system to another.

Migration actions from z/OS V1R13: z/OS UNIX

Perform the migration as follows:

1. Ensure that a file system has been mounted read-only as the current sysplex root file system. When the root is mounted read-only, there are no function-shipping clients as long as physical paths to the DASD are available to each system. To verify that there are no function-shipping clients, issue:

```
D OMVS,F,NAME=root_file_system_name
```

You should see CLIENT=N on each system.

2. Allocate and set up the new zFS sysplex root file system:
 - a. Create a new zFS file system to be used as the new sysplex root file system. *z/OS Distributed File Service zFS Administration* discusses creating and managing zFS file systems.

Rules:

- The UID, GID and the permission bits of the root directory in the new sysplex root file system must be same as the root directory in the current sysplex root file system.
 - If the SECLABEL class is active and the MLFSOBJ option is active, the security label for the new zFS file system must match the assumed security label of the current sysplex root file system.
- b. On the new sysplex root file system, set up the active mount points and the symbolic links. The mount points and symbolic links must be the same as the ones on the current sysplex root file system. You can set them up either (1) manually or (2) by using the **pax** shell command to populate the new sysplex root file system using the existing sysplex root as a source. To do it manually, create a mount point in the existing sysplex root (for example, /newroot) and mount the new sysplex root file system in the MODE(RDWR) on that mount point. After mounting the new sysplex root file system, manually issue MKDIRS and ln -s to create the mount point directories and symbolic links similar to the existing sysplex root file system. Note that the new sysplex root file system must contain all active mount points and symbolic links exactly as on the existing sysplex root file system.
 - c. Use the **pax** shell command to populate the new file system, using the existing sysplex root as a source.

Example:

```
cd /  
pax -wr -pe -XCM ./ /newroot
```

For more information about using **pax** to copy data from an HFS file system to a zFS file system, see *z/OS Distributed File Service zFS Administration*.

- d. Unmount the new zFS file system.
3. On any system in the shared file system configuration, issue:

```
F OMVS,NEWROOT=new.root.file.system.name,COND=<Yes|No>
```

YES Proceed conditionally. The system checks for active usage in the current sysplex root file system and reports the active usage in a BPXF245I message. If file activity is found, the command fails with EBUSY return code and JrActivityFound reason code. If file activity is not found, the command continues processing to replace the sysplex root. YES is the default.

NO Proceed unconditionally. The system checks for active usage in the current sysplex root file system and reports the active usage in a BPXF245I message. Replacement of the sysplex root file system will continue.

The migration of the sysplex root file system will begin. During the migration, active connections to files and directories in the current sysplex root file system are broken.

After the migration completes:

- The root CWD('/') is updated on all systems in the sysplex to point to the new sysplex root file system.

- New opens go to the new sysplex root file system. The current sysplex root for the root directory is replaced for all processes in all systems. The current directory for root directory is replaced for any processes using it
 - Old connections in the previous sysplex root file system might get EIO errors.
4. Update the TYPE parameter and name of the sysplex root file system in the BPXPRMxx member of SYS1.PARMLIB. Because the DDNAME() keyword of the BPXPRMxx ROOT and CMOUNT statements is not supported by zFS, change these statements to use the FILESYSTEM(name) keyword instead.

Reference information

For more information, see the following references:

- For more information about the HFS and zFS file systems, see *z/OS UNIX System Services Command Reference*.
- To read about setting up zFS, see *z/OS Distributed File Service zFS Administration*.
- For information about the **pax** command, see *z/OS UNIX System Services Command Reference*.

Determine whether your system has z/OS UNIX program files with certain attributes

Description

Before z/OS V2R2 and without the PTFs for APAR OA45793 installed, the sticky attribute was honored when either the set-user-id or set-group-id attributes were set. Starting with z/OS V2R2, APAR OA45793 changes the behavior of the exec (BPX1EXEC or BPX4EXEC) and spawn (BPX1SPN or BPX4SPN) interfaces when the user-specified path name resolves to a file that has the sticky attribute and either the set-user-id or set-group-id attributes. The exec and spawn services now ignore the sticky attribute unless a new RACF FACILITY class profile indicates that the usage is acceptable. Ignoring the sticky attribute means that the MVS program search order will not be used to locate the target program; only the z/OS UNIX program file that is identified by the user-specified path name is used.

EC6 abends with reason code xxxxE055 occur if the program is found in the MVS program search and no matching FACILITY class profile is found. If the program is not found in the MVS program search order, the z/OS UNIX file is run, which is the current behavior of exec and spawn.

Table 176 on page 245 provides more details about this migration action. Use this information to plan your changes to the system.

Table 405. Information about this migration action

Element or feature:	z/OS UNIX
When change was introduced:	z/OS V2R1, z/OS V1R13, and z/OS V1R12, all with APAR OA45793 applied.
Applies to migration from:	z/OS V2R1 and z/OS V1R13 both without APAR OA45793 applied.
Timing:	Before installing z/OS V2R2.
Is the migration action required?	Yes, if you have a program that fits the criteria in the Steps to take section.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Migration actions from z/OS V1R13: z/OS UNIX

Table 405. Information about this migration action (continued)

Related IBM Health Checker for z/OS check:	None.
--	-------

Steps to take

Follow these steps:

1. Determine whether any of your program files have the sticky attribute and either the set-user-id or set-group-id attributes. For each program file that has the sticky attribute and either the set-user-id or set-group-id attribute, select one of the following actions:

- If you do not want the exec and spawn services to use the MVS search order to locate programs, you do not need to take any action.
- If you want the exec and spawn services to always use the MVS search order for certain programs, then specify:

```
BPX.STICKYSUG.YOURPGM  
BPX.STICKYSUG.MYPGM
```

- If you want the exec and spawn services to use the MVS search order for a group of commonly named programs, then define a generic profile:

```
BPX.STICKYSUG.MYP*
```

The exec and spawn services will use the MVS search order for any program that begins with the characters MYP. The minimum allowable generic file is BPX.STICKYSUG.*.

After you complete the steps, you have determined how program files that have the sticky attribute and either the set-user-id or set-group-id attributes are to be handled.

Reference information

For more information, see *z/OS UNIX System Services Programming: Assembler Callable Services Reference*.

z/OS UNIX actions to perform before the first IPL of z/OS V2R2

This topic describes z/OS UNIX migration actions that you can perform after you have installed z/OS V2R2 but before the first time you IPL. These actions might require the z/OS V2R2 level of code to be installed but do not require it to be active.

Remove files and directories in /var/man

Description

Before z/OS V2R2, the /var/man directory was used by the **man** command. Starting with z/OS V2R2, the **man** command does not use this directory. Instead, it uses the /tmp directory on a per-user basis.

Table 177 on page 246 provides more details about this migration action. Use this information to plan your changes to the system.

Table 406. Information about this migration action

Element or feature:	z/OS UNIX
When change was introduced:	z/OS V2R2.
Applies to migration from:	z/OS V2R1 and z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you use the man command to view the man pages.
Target system hardware requirements:	None.
Target system software requirements:	None.

Table 406. Information about this migration action (continued)

Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	For temporary directory considerations, see “Steps to take” on page 247.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Remove the `/var/man` directory and all subdirectories and files on your z/OS V2R2 system. These files are no longer used for the z/OS V2R2 `man` command.
2. The z/OS V2R2 `man` command uses the temporary directory for caching man pages. Each user has their own man page cache in the temporary directory. This change might increase the size of the temporary directory, depending on how much man command usage there is on your system. Monitor space usage for the temporary directory to ensure that there is adequate space for users to issue the `man` command. The temporary directory can be the directory referred to by the `TMPDIR` environment variable, or `/tmp` if `TMPDIR` is not defined.

Reference information

For more information about the `man` command, see *z/OS UNIX System Services Command Reference*.

Update applications that use SMF type 92 subtype 11 close records Description

Before z/OS V2R1, SMF type 92, subtype 11 close records were written when sockets or character special records were closed. Sockets and character special files have very high close rates and do not provide useful information in determining how often files and directories are used. Starting in z/OS V2R1, they are written as subtype 16 close records instead. The sockets and character special file close records will no longer appear in type 92 subtype 11 records. Instead, you need to include type 92 subtype 16 records in the `SMFPRMxx` parmlib member to collect them.

Note: APAR OA43426 changed the pipe and fifo close processing also to generate SMF type 92 subtype 16 records instead of subtype 11. As a result, SMF type 92 subtype 16 contains information written when a socket, character, special file, pipe, or fifo is closed.

Table 407 provides more details about this migration action. Use this information to plan your changes to the system.

Table 407. Information about this migration action

Element or feature:	z/OS UNIX.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	Yes, if you want continue to get close records for sockets and character special files.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.

Migration actions from z/OS V1R13: z/OS UNIX

Table 407. Information about this migration action (continued)

Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Follow these steps:

1. Determine whether you have applications that use SMF type 92 subtype 11 close records. For those applications, SMF92TYP is set to SMF92#CLOSE (11) for subtype 11. SMF92CTY is set to FT_SOCKET (7) for sockets and FT_CHARSPEC (2) for character special files.
2. Change the application to look at subtype 16 records. SMF92TYP will be set to SMF92#CLSSOCCHARSPEC (16).

Reference information

For more information, see *z/OS UNIX System Services Planning*.

Determine whether certain files are involved with link-edited programs with AC=1 (Part 1)

Description

Starting with z/OS V2R1, the invocation requirements for MVS load library programs invoked through the z/OS UNIX spawn, exec and attach_exec services have changed. These changes apply to the invocation of MVS programs link-edited AC=1 found in an APF-authorized library and for MVS load library programs that are to run as a z/OS UNIX set-user-id or set-group-id program. The following list describes the changes:

- If the z/OS UNIX *pathname* that is supplied to spawn, exec or attach_exec represents an external link that resolves to an MVS program found in an APF-authorized library and link-edited with the AC=1 attribute, the external link must have an owning UID of 0 and not be found in a file system that is mounted as NOSECURITY to allow this type of invocation.
- If the z/OS UNIX *pathname* that is supplied to spawn, exec, or attach_exec represents a regular file with the sticky bit attribute that resolves to an MVS program found in an APF-authorized library and link-edited with the AC=1 attribute, the sticky bit file must have an owning UID of 0 or have the APF extended attribute turned on to allow this type of invocation. Additionally, the sticky bit file must not be found in a file system that is mounted as NOSECURITY to allow this type of invocation.
- If the z/OS UNIX *pathname* that supplied to spawn, exec or attach_exec represents a symbolic link to a regular file with the sticky bit attribute and the sticky bit file has the set-user-id attribute, the symbolic link must have an owning UID of 0 or an owning UID equal to that of the sticky bit file. If the sticky bit file has the set-group-id attribute, the symbolic link must have an owning UID of 0 or an owning GID equal to that of the sticky bit file. Additionally, the symbolic link must not be found in a file system that is mounted as NOSECURITY to allow this type of invocation.

Table 408 provides more details about this migration action. Use this information to plan your changes to the system.

Table 408. Information about this migration action

Element or feature:	z/OS UNIX.
When change was introduced:	z/OS V1R13 and z/OS V1R12, both with APAR OA41101.
Applies to migration from:	z/OS V1R13 without APAR OA41101 applied.
Timing:	Before the first IPL of V2R2.

Table 408. Information about this migration action (continued)

Is the migration action required?	No, but recommended even though most, if not all, IBM and vendor products install their executable files into the z/OS UNIX file system with an owning UID of 0, so few, if any, executable files on your system should have a problem.
Target system hardware requirements:	None.
Target system software requirements:	See "Steps to take before the first IPL."
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take before the first IPL

If you are migrating a z/OS system from z/OS V1R13 with APAR OA41101 installed, then no migration actions need to be taken. In this case, it is assumed that you have taken all required actions related to this APAR. Also see the documentation APAR OA41490.

If you are migrating from a z/OS system that does not have OA41101 installed and use the following IBM products, then you should ensure that you have the latest service levels and have followed the most recent install documentation for these IBM products:

- IBM z/OS Problem Determination Tools File Manager Software V10 (see Doc APAR PM81080)
- IBM z/OS Problem Determination Tools File Manager Software V11.1.0 with upgrade subset HADLB10 (ensure that PTF UK91613 is installed)
- IBM z/OS Problem Determination Tools Common Component Software V1.6.0 with upgrade subset HVWR160 (ensure that PTF UK91612 is installed)
- IBM InfoSphere Data Replication (see Doc APAR PM81306)
- IBM Security zSecure Suite (See Technote 1625364)
- IBM Tivoli Security Information and Event Manager (see Technote 1626384)

You may have to change the installation of some z/OS UNIX files and links provided by these products.

Otherwise, if you follow the standard install process for z/OS UNIX software, then you should not need to make any further changes related to APAR OA41101. Exceptions to this would be:

- If you installed z/OS UNIX sticky bit files, symbolic links or external links for any of your own software without using SMP/E
- If you installed any IBM or other vendor provided z/OS UNIX sticky bit files, symbolic links or external links outside the normal SMP/E install process
- If you installed z/OS UNIX software using SMP/E from a user that is not running with UID 0 and is not permitted to BPX.SUPERUSER

If any of these exceptions exist on your system, then you might have to change the installation of these files and links. To identify all the sticky bit files, symbolic links and external links that need to change, you need to IPL with z/OS V2R2 installed. If any of these files or links are executed, you will then start seeing EC6-xxxxC04A abends along with message BXP028I in the system log, which identifies the files or links that must be changed. You can then use the documentation for message BXP028I to correct the files or links that are installed improperly.

For more information about message BXP028I, see *z/OS MVS System Messages, Vol 3 (ASB-BPX)*.

Migration actions from z/OS V1R13: z/OS UNIX

Steps to take after the first IPL

For steps to take after the first IPL, see “Determine whether certain files are involved with link-edited programs with AC=1 (Part 2)” on page 507.

Reference information

For more information, see *z/OS UNIX System Services Command Reference*.

Determine whether any programs UNIX-invoke other z/OS UNIX executable programs

Description

Starting with z/OS V2R1, the requirements for the execution or loading of z/OS UNIX executable programs through the z/OS UNIX spawn, exec, loadhfs, loadhfs extended and attach_exec services and the REXX external subroutine and function processing have changed. These changes apply only to the usage of these interfaces by z/OS UNIX set-user-ID or set-group-ID privileged programs. A set-user-ID or set-group-ID privileged program is installed in the z/OS UNIX file system with either the set-user-ID or set-group-ID bit turned on.

The affected interfaces, when invoked from a z/OS UNIX set-user-ID or set-group-ID privileged program, now require that a target z/OS UNIX program file have a file owning UID of 0 or a file owning UID that is equal to that of the set-user-ID program, or have the program control extended attribute turned ON. Additionally, the target z/OS UNIX program file cannot be located in a NoSecurity file system. If any part of the z/OS UNIX path name that resolves to the target z/OS UNIX program file is a symbolic link, the symbolic link also must meet the same requirements.

Table 409 provides more details about this migration action. Use this information to plan your changes to the system.

Table 409. Information about this migration action

Element or feature:	z/OS UNIX.
When change was introduced:	z/OS V2R1.
Applies to migration from:	z/OS V1R13.
Timing:	Before the first IPL of z/OS V2R2.
Is the migration action required?	No, but recommended even though most, if not all, IBM and vendor products install their z/OS UNIX executable files and associated links into the z/OS UNIX file system with an owning UID of 0.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take

Before you begin, note that the standard IBM product installation process (SMP/E) installs all product-related files and links with an owning UID of 0 with the possible exception of set-user-id program files.

z/OS UNIX actions to take before the first IPL of z/OS V2R2

- If you are migrating a z/OS system from z/OS V1R13 with APAR OA42093 installed, then no migration actions need to be taken. In this case, it is assumed that you have taken all required actions related to this APAR.
- If you are migrating from a z/OS system that does not have OA42093 installed and use the following IBM products, then you should ensure that you have the latest service levels and have followed the most recent install documentation for these IBM products:
 - IBM Infoprint Transforms to AFP for z/OS (Ensure that APAR OA42691 is installed)

Otherwise, if you follow the standard install process for z/OS UNIX software, then you should not need to make any further changes related to APAR OA42093. Exceptions to this would be:

- If you installed z/OS UNIX executable files and associated symbolic links without using SMP/E.
- If you installed any IBM or other vendor provided z/OS UNIX executable files and associated symbolic links outside the normal SMP/E install process.
- If you installed z/OS UNIX software using SMP/E from a user that is not running with UID 0 and is not permitted to BPX.SUPERUSER.

If any of these exceptions exist on your system, then you might have to change the installation of these files and links. To identify all z/OS executable files and associated symbolic links that need to change, you need to IPL with z/OS V2R2 installed. If any of these files or links are executed, you will then start seeing EC6-xxxxE04B abends along with message BPXP029I in the system log, which identifies the files or links that must be changed. You can then use the documentation for message BPXP029I to correct the files or links that are installed improperly. For more information about message BPXP029I, see *z/OS MVS System Messages, Vol 3 (ASB-BPX)*.

z/OS UNIX actions to perform after the first IPL of z/OS V2R2

If you see EC6-xxxxE04B abends occurring, look for message BPXP029I in the system log to determine the details of the z/OS UNIX files or links involved with the errors and how to correct the problem. This abend is indicative of an attempt to execute, call or load an improperly installed z/OS UNIX executable program file.

For more information about message BPXP029I, see *z/OS MVS System Messages, Vol 3 (ASB-BPX)*.

Reference information

For more information, see the following references:

- *z/OS UNIX System Services Programming: Assembler Callable Services Reference*
- *z/OS Using REXX and z/OS UNIX System Services*
- *z/OS MVS System Commands*
- *z/OS MVS System Messages, Vol 3 (ASB-BPX)*

z/OS UNIX actions to perform after the first IPL of z/OS V2R2

This topic describes z/OS UNIX migration actions that you can perform only after you have IPLed z/OS V2R2. You need a running z/OS V2R2 system to perform these actions.

None.

Determine whether certain files are involved with link-edited programs with AC=1 (Part 2)

Description

Starting in z/OS V2R2 and with the PTFs for APAR OA45793 installed, the invocation requirements for MVS load library programs invoked through the z/OS UNIX spawn, exec and attach_exec services have changed. These changes apply to the invocation of MVS programs link-edited AC=1 found in an

Migration actions from z/OS V1R13: z/OS UNIX

APF-authorized library and for MVS load library programs that are to run as a z/OS UNIX set-user-id or set-group-id program. The following list describes the changes:

- If the z/OS UNIX *pathname* that is supplied to spawn, exec or attach_exec represents an external link that resolves to an MVS program found in an APF-authorized library and link-edited with the AC=1 attribute, the external link must have an owning UID of 0 and not be found in a file system that is mounted as NOSECURITY to allow this type of invocation.
- If the z/OS UNIX *pathname* that is supplied to spawn, exec, or attach_exec represents a regular file with the sticky bit attribute that resolves to an MVS program found in an APF-authorized library and link-edited with the AC=1 attribute, the sticky bit file must have an owning UID of 0 or have the APF extended attribute turned on to allow this type of invocation. Additionally, the sticky bit file must not be found in a file system that is mounted as NOSECURITY to allow this type of invocation.
- If the z/OS UNIX *pathname* that supplied to spawn, exec or attach_exec represents a symbolic link to a regular file with the sticky bit attribute and the sticky bit file has the set-user-id attribute, the symbolic link must have an owning UID of 0 or an owning UID equal to that of the sticky bit file. If the sticky bit file has the set-group-id attribute, the symbolic link must have an owning UID of 0 or an owning GID equal to that of the sticky bit file. Additionally, the symbolic link must not be found in a file system that is mounted as NOSECURITY to allow this type of invocation.

Table 410 provides more details about this migration action. Use this information to plan your changes to the system.

Table 410. Information about this migration action

Element or feature:	z/OS UNIX.
When change was introduced:	z/OS V1R13 and z/OS V1R12, both with APAR OA41101.
Applies to migration from:	z/OS V1R13 without APAR OA41101 applied.
Timing:	After the first IPL of z/OS V2R2. (For steps to take before the first IPL, see "Determine whether certain files are involved with link-edited programs with AC=1 (Part 1)" on page 504).
Is the migration action required?	No, but recommended even though most, if not all, IBM and vendor products install their executable files into the z/OS UNIX file system with an owning UID of 0, so few, if any, executable files on your system should have a problem.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.
Related IBM Health Checker for z/OS check:	None.

Steps to take after the first IPL

If you see EC6-xxxxC04A abends occurring, look for message BPXP028I in the system log to determine the details of the z/OS UNIX files or links and MVS programs involved with the errors and how to correct the problem. This abend is indicative of an attempt to execute an improperly installed z/OS UNIX sticky bit file, symbolic link or external link that resolves to a MVS program.

For more information about message BPXP028I, see *z/OS MVS System Messages, Vol 3 (ASB-BPX)*.

For the steps to take before the first IPL, see "Determine whether certain files are involved with link-edited programs with AC=1 (Part 1)" on page 504.

Reference information

For more information, see *z/OS UNIX System Services Command Reference*.

Migration actions from z/OS V1R13: z/OS UNIX

Appendix. Accessibility

Accessible publications for this product are offered through IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SSLTBW/welcome).

If you experience difficulty with the accessibility of any z/OS information, send a detailed message to the Contact z/OS web page (www.ibm.com/systems/z/os/zos/webqs.html) or use the following mailing address.

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Building 707
2455 South Road
Poughkeepsie, NY 12601-5400
United States

Accessibility features

Accessibility features help users who have physical disabilities such as restricted mobility or limited vision use software products successfully. The accessibility features in z/OS can help users do the following tasks:

- Run assistive technology such as screen readers and screen magnifier software.
- Operate specific or equivalent features by using the keyboard.
- Customize display attributes such as color, contrast, and font size.

Consult assistive technologies

Assistive technology products such as screen readers function with the user interfaces found in z/OS. Consult the product information for the specific assistive technology product that is used to access z/OS interfaces.

Keyboard navigation of the user interface

You can access z/OS user interfaces with TSO/E or ISPF. The following information describes how to use TSO/E and ISPF, including the use of keyboard shortcuts and function keys (PF keys). Each guide includes the default settings for the PF keys.

- *z/OS TSO/E Primer*
- *z/OS TSO/E User's Guide*
- *z/OS V2R2 ISPF User's Guide Vol I*

Dotted decimal syntax diagrams

Syntax diagrams are provided in dotted decimal format for users who access IBM Knowledge Center with a screen reader. In dotted decimal format, each syntax element is written on a separate line. If two or more syntax elements are always present together (or always absent together), they can appear on the same line because they are considered a single compound syntax element.

Each line starts with a dotted decimal number; for example, 3 or 3.1 or 3.1.1. To hear these numbers correctly, make sure that the screen reader is set to read out punctuation. All the syntax elements that

have the same dotted decimal number (for example, all the syntax elements that have the number 3.1) are mutually exclusive alternatives. If you hear the lines 3.1 USERID and 3.1 SYSTEMID, your syntax can include either USERID or SYSTEMID, but not both.

The dotted decimal numbering level denotes the level of nesting. For example, if a syntax element with dotted decimal number 3 is followed by a series of syntax elements with dotted decimal number 3.1, all the syntax elements numbered 3.1 are subordinate to the syntax element numbered 3.

Certain words and symbols are used next to the dotted decimal numbers to add information about the syntax elements. Occasionally, these words and symbols might occur at the beginning of the element itself. For ease of identification, if the word or symbol is a part of the syntax element, it is preceded by the backslash (\) character. The * symbol is placed next to a dotted decimal number to indicate that the syntax element repeats. For example, syntax element *FILE with dotted decimal number 3 is given the format 3 * FILE. Format 3* FILE indicates that syntax element FILE repeats. Format 3* * FILE indicates that syntax element * FILE repeats.

Characters such as commas, which are used to separate a string of syntax elements, are shown in the syntax just before the items they separate. These characters can appear on the same line as each item, or on a separate line with the same dotted decimal number as the relevant items. The line can also show another symbol to provide information about the syntax elements. For example, the lines 5.1*, 5.1 LASTRUN, and 5.1 DELETE mean that if you use more than one of the LASTRUN and DELETE syntax elements, the elements must be separated by a comma. If no separator is given, assume that you use a blank to separate each syntax element.

If a syntax element is preceded by the % symbol, it indicates a reference that is defined elsewhere. The string that follows the % symbol is the name of a syntax fragment rather than a literal. For example, the line 2.1 %OP1 means that you must refer to separate syntax fragment OP1.

The following symbols are used next to the dotted decimal numbers.

? indicates an optional syntax element

The question mark (?) symbol indicates an optional syntax element. A dotted decimal number followed by the question mark symbol (?) indicates that all the syntax elements with a corresponding dotted decimal number, and any subordinate syntax elements, are optional. If there is only one syntax element with a dotted decimal number, the ? symbol is displayed on the same line as the syntax element, (for example 5? NOTIFY). If there is more than one syntax element with a dotted decimal number, the ? symbol is displayed on a line by itself, followed by the syntax elements that are optional. For example, if you hear the lines 5 ?, 5 NOTIFY, and 5 UPDATE, you know that the syntax elements NOTIFY and UPDATE are optional. That is, you can choose one or none of them. The ? symbol is equivalent to a bypass line in a railroad diagram.

! indicates a default syntax element

The exclamation mark (!) symbol indicates a default syntax element. A dotted decimal number followed by the ! symbol and a syntax element indicate that the syntax element is the default option for all syntax elements that share the same dotted decimal number. Only one of the syntax elements that share the dotted decimal number can specify the ! symbol. For example, if you hear the lines 2? FILE, 2.1! (KEEP), and 2.1 (DELETE), you know that (KEEP) is the default option for the FILE keyword. In the example, if you include the FILE keyword, but do not specify an option, the default option KEEP is applied. A default option also applies to the next higher dotted decimal number. In this example, if the FILE keyword is omitted, the default FILE(KEEP) is used. However, if you hear the lines 2? FILE, 2.1, 2.1.1! (KEEP), and 2.1.1 (DELETE), the default option KEEP applies only to the next higher dotted decimal number, 2.1 (which does not have an associated keyword), and does not apply to 2? FILE. Nothing is used if the keyword FILE is omitted.

*** indicates an optional syntax element that is repeatable**

The asterisk or glyph (*) symbol indicates a syntax element that can be repeated zero or more times. A dotted decimal number followed by the * symbol indicates that this syntax element can be used

zero or more times; that is, it is optional and can be repeated. For example, if you hear the line 5.1* data area, you know that you can include one data area, more than one data area, or no data area. If you hear the lines 3* , 3 HOST, 3 STATE, you know that you can include HOST, STATE, both together, or nothing.

Notes:

1. If a dotted decimal number has an asterisk (*) next to it and there is only one item with that dotted decimal number, you can repeat that same item more than once.
2. If a dotted decimal number has an asterisk next to it and several items have that dotted decimal number, you can use more than one item from the list, but you cannot use the items more than once each. In the previous example, you can write HOST STATE, but you cannot write HOST HOST.
3. The * symbol is equivalent to a loopback line in a railroad syntax diagram.

+ indicates a syntax element that must be included

The plus (+) symbol indicates a syntax element that must be included at least once. A dotted decimal number followed by the + symbol indicates that the syntax element must be included one or more times. That is, it must be included at least once and can be repeated. For example, if you hear the line 6.1+ data area, you must include at least one data area. If you hear the lines 2+, 2 HOST, and 2 STATE, you know that you must include HOST, STATE, or both. Similar to the * symbol, the + symbol can repeat a particular item if it is the only item with that dotted decimal number. The + symbol, like the * symbol, is equivalent to a loopback line in a railroad syntax diagram.

Notices

This information was developed for products and services offered in the U.S.A. or elsewhere.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

Site Counsel
IBM Corporation
2455 South Road
Poughkeepsie, NY 12601-5400
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of 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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

COPYRIGHT LICENSE:

This information might contain sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Policy for unsupported hardware

Various z/OS elements, such as DFSMS, HCD, JES2, JES3, and MVS, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Minimum supported hardware

The minimum supported hardware for z/OS releases identified in z/OS announcements can subsequently change when service for particular servers or devices is withdrawn. Likewise, the levels of other software products supported on a particular release of z/OS are subject to the service support lifecycle of those products. Therefore, z/OS and its product publications (for example, panels, samples, messages, and product documentation) can include references to hardware and software that is no longer supported.

- For information about software support lifecycle, see: IBM Lifecycle Support for z/OS (www.ibm.com/software/support/systemsz/lifecycle)
- For information about currently-supported IBM hardware, contact your IBM representative.

Trademarks

IBM, the IBM logo, and ibm.com[®] are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available at Copyright and Trademark information (www.ibm.com/legal/copytrade.shtml).

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Intel is a trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle, its affiliates, or both.

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.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names might be trademarks or service marks of others.

Index

Special characters

- `_BPXK_UNUSEDTASKS=KEEP`
 - specifying, to keep original threading behavior 187, 404
- `_CEE_DEBUG_FILENAME31`
 - recognized by Language Environment 214, 454
- `/etc` directory, migrating files in 16
- `/samples/ssh_smf.h`
 - migration actions 241, 493
- `/var` directory, migrating files in 16

Numerics

- 3270 PC File Transfer Program, no migration actions for 4
- 3800 Printing Subsystem, preparing to use 174, 375
- 3900 Printing Subsystem, preparing to use 174, 375
- 64-bit TMI copy buffer function 314

A

- ABEND messages
 - end of volume 367
- accessibility 511
 - contact IBM 511
 - features 511
- Accommodate new sslCipherSpecs
 - default
 - z/OS IBM Tivoli Directory Server 193, 411
- ACDS (active control data set), ensuring integrity of 168, 365
- actions to perform, meaning of
 - after first IPL x
 - before first IPL ix
 - before installing ix
- active control data set (ACDS), ensuring integrity of 168, 365
- after first IPL, migration actions
 - BCP 300
 - Communications Server 151, 340
 - Cryptographic Services 163, 360
 - DFSORT 397
 - Distributed File Service 187, 404
 - Integrated Security Services 441
 - JES2 211, 447
 - Language Environment 218, 460
 - RMF 224, 469
 - SDSF 474
 - Security Server 232, 481
 - XL C/C++ 234, 485
 - z/OS UNIX 495
- after the first IPL, migration actions
 - z/OS Font Collection 236, 488
- Alternate Library for REXX, no migration actions for 3
- AMBLIST utility 93, 251

- aophinvd, aoplogd, and aopsdbd daemons, discontinue use of 204, 435
- aopsetup, running 206, 437
- ARM couple data set 105, 276
- assembler mnemonic for a new machine instruction 189, 407
- assistive technologies 511
- AT-TLS access to CSFIQA and CSFRNG resources 324
- AT-TLS groups and FIPS140 mode, Communications Server 326
- AUTHCMD and AUTHPGM NAMES
 - section of your IKJTSOxx member 311
- authorization 179, 383
- Auto-reply for WTORs 100, 262
- automatic refresh UCB function
 - default 170, 369
- automatic start
 - IBM Health Checker for z/OS 266
- automation 328
 - D TCP/IP,tnproc,<Telnet>,CONN command 327
- AXRINIT and AXRRXTSS in the program
 - properties table 272, 273

B

- BBNBASE profile prefix
 - migration consideration 415
- BCP migration actions
 - after first IPL 300
 - before installing 264
 - z/OSMF Capacity Provisioning, CPCC 303
- BCP, assembler mnemonic for a new machine instruction 189, 407
- BCP, AXRINIT and AXRRXTSS in the program
 - properties table 272, 273
- BCPii
 - HWIREXX helper program
 - restriction 101, 264
- BCPii API calls 255
- BCPii ENF exits 255
- BDT File-to-File, no migration actions
 - for 3
- BDT SNA NJE, no migration actions
 - for 3
- BDT, no migration actions
 - for 3
- before first IPL, migration actions
 - Communications Server 328
 - Cryptographic Services 156, 348
 - DFSMS 173, 374
 - DFSORT 186, 396
 - Distributed File Service 401
 - general 13
 - JES2 210, 444
 - JES3 211, 447
 - Library Server 218, 220, 460, 462
 - RMF 464
 - SDSF 225, 471
 - Security Server 230, 231, 477, 478

- before first IPL, migration actions
 - (continued)
 - XL C/C++ 234, 485
 - z/OS UNIX 246, 502
- before installing, migration actions
 - BCP 264
 - BookManager BUILD 130, 306
 - DFSMS 168, 365
 - Distributed File Service 186, 399
 - general 5
 - HCD 188, 405
 - HLSAM 188, 407
 - IBM HTTP 191, 409
 - IBM Tivoli Directory Server 193, 411
 - ICKDSF (Device Support Facility) 199, 430
 - Infoprint Server 200, 431
 - JES2 208, 441
 - JES3 211, 447
 - Security Server 228, 475
 - sysplex 91, 249
 - TSO/E 482
 - XL C/C++ 233, 484
 - z/OS Font Collection 234, 485
 - z/OS UNIX 494
 - z/OSMF 195, 413
- before the first IPL, migration actions
 - z/OS Font Collection 235, 485
- BIND 9.2.0
 - before first IPL 316
- BIND 9.2.0 name server 316
- BIND jobs, OAM DB2 183, 391
- BookManager
 - BUILD 130, 306
 - BookManager BUILD, support for 130, 306
 - BookManager READ, no migration actions for 3
- bootstrap information 99, 261
- BPX.DEFAULT.USER profile replaced by BPX.UNIQUE.USER 495
- BPX.UNIQUE.USER profile 495
- BROADCAST parameter 445

C

- capacity evaluation with zSoftCap 7
- Capacity Provisioning 303
- Capacity Provisioning Control Center 303
- Capacity Provisioning Control Center (CPCC) xxx,yyy 303
- Capacity Provisioning Manager
 - CIM client for Java 2 97, 259
 - Java level 118, 291
 - WTOR suppression 98, 260
- CDT (class descriptor table) names,
 - RACF 230, 477
- CEEPRMxx parmlib 459
- CEERCOPT sample 457
- CEERDOPT sample 457

CELQRDOP sample 457
 CFCC (coupling facility control code)
 levels 89
 CFRM policy, updating 89
 changes
 z/OS V2R2 xvi
 checks, migration health 2
 CHOWN.UNRESTRICTED profile in the
 RACF UNIXPRIV class 480
 CICS system definition file for Language
 Environment, updating 216, 455
 CIM Client for Java Version 2
 Capacity Provisioning Manager 97,
 259
 class descriptor table (CDT) names,
 RACF 230, 477
 class name conflicts, RACF 230, 477
 coexistence
 definition of ix
 COMMDS (common communications
 data set), ensuring integrity of 168,
 365
 common communications data set
 (COMMDS), ensuring integrity of 168,
 365
 Common Information Model (CIM) 133,
 308
 Communications Server migration actions
 after first IPL 151, 340
 before first IPL 316, 328, 329
 before installing 309, 312, 313
 before the first IPL 327
 Communications Server Security Level 3,
 no migration actions for 3
 Communications Server, AT-TLS access to
 CSFIQA and CSFRNG resources 324
 Communications Server, AT-TLS groups
 and FIPS140 mode 326
 Communications Server, ICLI
 component 493
 Communications Server, IKE daemon and
 the NSS daemon access to the
 CSFIQF 323
 Communications Server, Netstat
 enhancements 141, 331
 communications storage manager
 (CSM) 150, 333
 console name modification 474
 contact
 z/OS 511
 control data sets, migrating SMS 168,
 365
 control units
 supported 85
 withdrawn 85
 conventions used in this document viii
 convertFromREtoSAF.rexx 413
 COPYVOLID 385
 core image of DFSMSdss Stand-Alone
 Services, building 180, 386
 coupling facility control code (CFCC)
 levels 89
 CPCC 303
 CPCC, Windows-based 303
 CPU
 maximum number supported 269
 CPU evaluation with zSoftCap 7

Cryptographic Services migration actions
 after first IPL 163, 360
 before first IPL 156, 348
 CSD (CICS system definition) file for
 Language Environment, updating 216,
 455
 CSFRNG resource 439
 CustomPac Installation Dialog 11, 12

D

DASD for z/OS root 8
 data integrity of SMS control data
 sets 168, 365
 data set
 dump allocation 92, 250
 data sets
 deleted 28
 new 36
 database templates, updating RACF 232,
 481
 DATASET keyword 177, 382
 DB2 BIND jobs, OAM 183, 391
 default amount for fixed storage
 buffers 150, 333
 default password 228, 475
 defaults DFSORT 397, 398
 Define the RACF definitions to enable the
 GPMSERVE Started Task for
 Authorization Code zero (AC=0) 466
 deleted data sets and paths 28
 description, meaning of x
 devices
 attaching new 88
 removing unsupported 87
 DFSMS migration actions
 before first IPL 173, 374
 before installing 168, 365
 DFSMS, removing SMA fields from the
 SMS storage group construct
 IGDSGD 368
 DFSMSdfp
 accommodate changes to LISTCAT
 LEVEL 375
 DFSMSdfp IEBCOPY
 examining and updating program
 calls to 377
 DFSMSdfp, IEBCOPYO 377
 DFSMSdss
 restore
 catalog data sets 395
 DFSMSdss, COPYVOLID 385
 DFSMSdss, EIREC14 182, 387
 DFSMSShsm
 applications that depend on the LIST
 DUMPCLASS command,
 updating 183, 388
 new default behavior for full-volume
 and track restore with VTOC 393
 DFSMSShsm, dump VTOC copies 389
 DFSMSrmm CIM provider 172, 371
 DFSORT EXPOLD=MAX and
 EXPRES=0 398
 DFSORT migration actions
 after first IPL 397
 before first IPL 186, 396
 DFSORT TUNE=OLD 397

DHGroups parameter default 137, 320
 DIAGxx
 FREEMAINEDFRAMES 110, 284
 discontinue use of Infoprint Server
 aophinvd, aoplogd, and aopsdbd
 daemons 204, 435
 discontinue use of Infoprint Server SNMP
 subagent 200, 431
 Distributed File Service migration actions
 after first IPL 187, 404
 before first IPL 401
 before installing 186, 399
 DISTRIBUTED mode 94, 252
 DLLs (dynamic link libraries) with
 Language Environment 173, 374
 document, this
 conventions and terminology in viii
 how organized vii
 how to use viii
 who should read vii
 dump
 stand-alone 92, 250
 dump allocation
 IPCS 92, 250
 DUMP parameter 448
 Dump VTOC copies, DFSMSShsm 389
 dump, reassembling stand-alone 101,
 263
 duplicate class names, RACF 230, 477
 dynamic link libraries with Language
 Environment 173, 374
 DYNCPADD keyword 268

E

EIREC14 182, 387
 environment variable 340
 OMPROUTE_OPTIONS 329
 EREP, no migration actions for 3
 ESCON Director Support, no migration
 actions for 4
 ESQA 275
 everyone, migration actions for
 before first IPL 13
 exec
 convertFromREtoSAF.rexx 413
 exit routines
 migrating 19
 SDSF 225, 471
 exploitation, definition of ix
 EXPOLD=OLD, DFSORT 398
 EXPRES=0 DFSORT 398

F

FACILITY class, RACF
 defining new profiles 22
 OCSF profiles 158, 349
 fallback
 definition of ix
 FFST, no migration actions for 4
 FIPS 140-2 mode 350
 first IPL, migration actions after
 BCP 300
 Communications Server 151, 340
 Cryptographic Services 163, 360

first IPL, migration actions after
(*continued*)

- DFSORT 397
- Distributed File Service 187, 404
- Integrated Security Services 441
- JES2 211, 447
- Language Environment 218, 460
- RMF 224, 469
- SDSF 474
- Security Server 232, 481
- XL C/C++ 234, 485
- z/OS UNIX 495

first IPL, migration actions before

- Communications Server 328
- Cryptographic Services 156, 348
- DFSMS 173, 374
- DFSORT 186, 396
- Distributed File Service 401
- general 13
- JES2 210, 444
- JES3 211, 447
- Library Server 218, 220, 460, 462
- RMF 464
- SDSF 225, 471
- Security Server 230, 477
- XL C/C++ 234, 485
- z/OS UNIX 246, 502

Fix Category 66, 77

FIXCAT 66, 77

Flash Express 275

Font Collection migration actions
before first IPL 235, 487

font type

- AFP 485
- compatibility 485
- IBM Infoprint fonts 485
- object 485
- WorldType 485

fonts

- collection 485
- using 485
- z/OS Font Collection 235, 485, 487

FREEMAINEDFRAMES 110, 284

G

GATEWAY statements replaced by
BEGINROUTES statements 135, 318

GDDM-PGF, no migration actions for 4

GDDM-REXX, no migration actions
for 4

GDDM, no migration actions for 4

GDGE format 213, 452

general migration actions
before first IPL 13

Generic Tracker 264

GetProfile request of the TCP/IP callable
network management interface
(NMI) 314

GLOBALCONFIG SMCR
PFID 140

GPMSEVERE and GPM4CIM options for
TCP/IP address regular
expressions 465

H

hardware

- supported 85
- withdrawn 85

hardware migration actions 43, 60

HCM, migrating security for 405

HCM, no migration actions for 4

HCR77A1, IBM Health Checker check

- ICFSMIG77A1_COPROCESSOR
_ACTIVE 152, 342

HCR77A1, IBM Health Checker check

- ICFSMIG77A1_TKDS_OBJECT 153,
343

health checks, migration 2

health checks, updating 25

HEWLKED linkage editor program 190,
408

HFS to zFS, migrating file system
from 241, 497

HLASM Toolkit, no migration actions
for 4

HOLDDATA 66, 77

how this document is organized vii

how to use this document viii

HWIREXX

- BCPii helper program restriction 101,
264

I

IARBRVEA 110, 284

IARBRVER 110, 284

IBM Configuration Assistant for z/OS
Communications Server 309

IBM Health Checker for z/OS
automatic start 266

IBM Health Checker related check,
meaning of x

IBM HTTP Server - Powered by Apache,
configuring 207, 438

IBM HTTP Server powered by Domino,
support for 191, 409

IBM z/OS Management Facility 195,
413, 426

- filtering tables 197, 428
- table filters 197, 428

ICHDEX01 exit routine 231, 478

ICKDSF (Device Support Facility)
migration actions 199, 430

ICLI component 493

ICSF installation options data set
deprecated parameters 156, 347

ICSF migration actions 152, 342

ICSF, hash services 154, 344, 346

IDCAMS ALLOCATE command 177,
382

IDCAMS DCOLLECT command 184,
392

IDCAMS DEFINE command 179, 383

IDCAMS REPRO utility 373

IEASYSxx

- LFAREA
INCLUDE1MAFC 109, 282

IEBCOPY utility 375, 377

IEBCOPYO, DFSMSdftp 377

IEXCEPTIONEXIT keyword 176, 380

IFAPRDxx product ID 40

IGD17054I 378

IKE daemon 148, 332

IKE daemon and the NSS daemon access
to the CSFIQF, Communications
Server 323

IKE daemon, Communications
server 325

IKJTSOxx

- AUTHCMD 311
- AUTHPGM 311

INCLUDE1MAFC 109, 282

Infoprint Server migration actions
after first IPL 206, 207, 437, 438

- before first IPL 205, 436
- before installing 200, 202, 204, 431,
433, 435

INIT

- default 199, 430

installation steps 1

installing, migration actions before
Infoprint Server 200, 431

Integrated Security Services migration
actions 439

- after first IPL 441

integrity of SMS control data sets 168,
365

Internet address

- for CFCC levels and processors 89
- for CFSizer tool 89
- for flashes 23, 25
- for ISVs 22
- for PSP buckets 5
- for zSoftCap 7

Internet Key Exchange (IKE) 148, 332

intranode management network 310

Intrusion Detection Services

- IP Fragment attack type 313

ioeagfmt (zFS batch utility) 403

IOEFSPRM configuration file
accept 399

IOSHMCTL

- start in TPC-R Basic Hyperswap
environment 102, 281

IOSSPOF macro 256

IP fragment
before installing 313

IP Services 310

IPCS

- setting up 13

IPL text
create 99, 261

IPL, migration actions after first
BCP 300, 303

- Communications Server 151, 340
- Cryptographic Services 163, 360
- DFSORT 397
- Distributed File Service 187, 404
- Integrated Security Services 441
- JES2 211, 447
- Language Environment 218, 460
- RMF 224, 469
- SDSF 474
- Security Server 232, 481
- XL C/C++ 234, 485
- z/OS UNIX 495

- IPL, migration actions before first
 - Communications Server 328
 - Cryptographic Services 156, 348
 - DFSMS 173, 374
 - DFSORT 186, 396
 - Distributed File Service 401
 - general 13
 - JES2 210, 444
 - JES3 211, 447
 - Library Server 218, 220, 460, 462
 - RMF 464
 - SDSF 225, 471
 - Security Server 230, 477
 - XL C/C++ 234, 485
 - z/OS UNIX 246, 502
- IPv6
 - before installing 312
- IPv6 support for policy-based
 - routing 315
- IRREXV01 exit 228, 475
- IRRMIN00 utility, RACF 232, 481
- ISFPARMS, SDSF
 - reassembling 226, 472
- ISV products, reconnecting 21
- IXCL1DSU utility 127, 301
- IZUANG1 started task
 - cataloged procedure 423, 424, 425
- IZUFPROC logon procedure
 - cataloged procedure 423, 424
 - permissions 423, 424
- IZUSVR user ID 425
 - permissions 423, 424
- IZUSVR1 started task
 - cataloged procedure 423, 424, 425

J

- Java Managed Provider Interface (JMPI) 132, 307
- Java support for IPP Server, upgrading 202, 433
- Java Version 2 97, 259
- JCLERR parameter 446
- JES2
 - z11 mode 208, 442
- JES2 exits 210, 444
- JES2 migration actions
 - after first IPL 211, 447
 - before first IPL 210, 444
 - before installing 208, 441
- JES3
 - data set integrity 211, 450
 - IATYLR macro 213, 452
- JES3 migration actions
 - before first IPL 211, 447
 - before installing 211, 447
- JES3 release level format 447
- JESJOBS access profiles 441
- Job Modify SSI 85
 - authority 441
- JOBDEF statement 446
- JVM applications 494

K

- keyboard
 - navigation 511
 - PF keys 511
 - shortcut keys 511

L

- Language Environment migration actions
 - after first IPL 218, 460
- Language Environment, options
 - report 458
- Library Server
 - notes file 219, 461
- Library Server information centers 463
- Library Server migration actions
 - before first IPL 218, 220, 460, 462
- link pack area (LPA)
 - Language Environment load modules
 - in 217, 456
 - relieving virtual storage constraint
 - with 88
- LIST DUMPCLASS command,
 - DFSMSshm 183, 388
- LOGR Couple Data Set 95, 257
- LPA (link pack area)
 - Language Environment load modules
 - in 217, 456
 - relieving virtual storage constraint
 - with 88

M

- maintenance, coexistence and fallback 6
- man page
 - clearing cache files and
 - directories 246, 502
- Management Facility, IBM z/OS 195, 413, 426
- Maximum Segment Size (MSS) 148, 331
- MAXUSER 41
- MEMLIMIT parameter
 - determining virtual storage with 24
- memory pool 275
- message automation 272
- messages, updating automation for
 - changed 19
- Metal C Runtime Library, no migration
 - actions for 4
- MICR/OCR, no migration actions for 4
- Migrate from IBM HTTP Server powered
 - by Domino
 - z/OS PKI Services 165, 361
 - by Apache
 - z/OS PKI Services 165, 361
- migration action, after IPLs
 - ICKDSF (Device Support Facility) 199, 430
 - TSO/E 484
 - z/OSMF 195, 426
- migration actions
 - after first IPL
 - BCP 300
 - Communications Server 151, 340
 - Cryptographic Services 163, 360

- migration actions (*continued*)
 - after first IPL (*continued*)
 - DFSORT 397
 - Distributed File Service 187, 404
 - Integrated Security Services 441
 - JES2 211, 447
 - Language Environment 218, 460
 - RMF 224, 469
 - SDSF 474
 - Security Server 232, 481
 - XL C/C++ 234, 485
 - z/OS UNIX 495
 - BCP 92, 250
 - before first IPL
 - Communications Server 328
 - Cryptographic Services 156, 348
 - DFSMS 173, 374
 - DFSORT 186, 396
 - Distributed File Service 401
 - general 13
 - JES2 210, 444
 - JES3 211, 447
 - Library Server 218, 220, 460, 462
 - RMF 464
 - SDSF 225, 471
 - Security Server 230, 231, 477, 478
 - XL C/C++ 234, 485
 - z/OS UNIX 246, 502
 - before installing
 - BCP 264
 - DFSMS 168, 365
 - Distributed File Service 186, 399
 - general 5
 - Infoprint Server 200, 431
 - JES2 208, 441
 - JES3 211, 447
 - Security Server 228, 475
 - sysplex 91, 249
 - XL C/C++ 233, 484
 - z/OS UNIX 494
 - C/C++ 233, 484
 - CIM 131, 132, 307, 308
 - Communications Server 133, 309
 - Cryptographic Services 152, 342
 - DFSMS 168, 365
 - DFSORT 185, 396
 - Distributed File Service 186, 399
 - for everyone 5
 - for OpenSSH 236, 488
 - general 5
 - hardware 43, 60
 - IBM HTTP Server 191, 409
 - IBM z/OS Management Facility 195, 413
 - Infoprint Server 200, 431
 - Integrated Security Services 439
 - JES3 211, 447
 - Language Environment 214, 453
 - Library Server 218, 460
 - none, elements and features with 3
 - OpenSSH 236, 488
 - RMF 221, 464
 - SDSF 225, 471
 - Security Server 228, 475
 - sysplex 91, 249
 - TSO/E 482
 - XL C/C++ 233, 484

- migration actions (*continued*)
 - z/OS UNIX 241, 493
- migration actions to perform, meaning of
 - after first IPL x
 - before first IPL ix
 - before installing ix
- migration actions, after first IPL
 - HCD 188, 406
 - HLASM 191, 409
- migration actions, before first IPL
 - HCD 188, 406
 - HLASM 190, 408
 - ICKDSF (Device Support Facility) 199, 430
 - TSO/E 483
 - z/OSMF 195, 421
- migration health checks 2
- migration steps 1
- migration, definition of ix
- modifications, user
 - examining 19
 - for Language Environment options 453
- Monitor III version, using correct 224, 469
- MVS
 - IEFUSI exit routine 107, 278

N

- navigation
 - keyboard 511
- Netstat enhancements 141, 331
- Network Job Entry 136, 319
- new data sets 36
- NFS, no migration actions for 4
- NMI applications 314
- notes files, Library Server 219, 461
- Notices 515
- nucleus size 274

O

- OAM DB2 BIND jobs 183, 391
- OCSF directory migration 156, 348
- OCSF migration actions 152, 342
- Offline device discovery 175, 379
- OMPROUTE 329
- OMROUTE
 - before first IPL 329
- one-stage JCL 101, 263
- one-step JCL 101, 263
- OpenSSH
 - migration actions 236, 488
- OPTIONS statement 448
- OSM interfaces 310
- other system (coexistence or fallback) requirements, meaning of x
- OUTDEF statement 445

P

- Parallel Sysplex migration actions
 - before installing 91, 249
- PARMDD keyword 106, 277

- parmlib
 - used by IPCS 13
 - using shipped members of 15
- PassTicket creation 422
- paths, deleted 28
- PDSE sharing restrictions 37
- PFA
 - check removal 256
 - frames and slots 256
- port settings for z/OSMF
 - checking 416
- post IPL migration actions
 - CIM 132, 308
- post-IPL migration actions
 - Communications Server 151, 340
 - Cryptographic Services 163, 360
 - DFSORT 397
 - Distributed File Service 187, 404
 - Integrated Security Services 441
 - JES2 211, 447
 - Language Environment 218, 460
 - RMF 224, 469
 - SDSF 474
 - Security Server 232, 481
 - XL C/C++ 234, 485
 - z/OS UNIX 495
- pre-IPL migration actions
 - Communications Server 328
 - Cryptographic Services 156, 348
 - DFSMS 173, 374
 - DFSORT 186, 396
 - Distributed File Service 401
 - general 13
 - JES2 210, 444
 - JES3 211, 447
 - Library Server 218, 220, 460, 462
 - RMF 464
 - SDSF 225, 471
 - Security Server 230, 477
 - z/OS UNIX 246, 502
- Predictive Failure Analysis
 - PFA_FRAMES_AND_SLOTS 256
- Predictive Failure Analysis (PFA)
 - check values 120, 293
 - configuration file 121, 294
 - Java level 122, 295
 - migration
 - HZSPRMxx 119, 292
 - time stamp 120, 293
- preinstallation migration actions
 - BCP 264
 - DFSMS 168, 365
 - Distributed File Service 186, 399
 - general 5
 - JES 208, 211, 441, 447
 - Security Server 228, 475
 - sysplex 91, 249
 - XL C/C++ 233, 484
 - z/OS UNIX 494
- Printer Inventory, migrating 205, 436
- procedures, updating operational 22
- processors
 - migrating to z114 60, 72
 - migrating to z196 60, 72
 - migrating to zEC12 60
- proclib, using shipped members of 15
- program files 245, 501

- PSP bucket
 - reviewing 5
 - upgrade IDs 5

Q

- QUEUEDRTT parameter
 - default value 147

R

- RACF
 - tape profile
 - processing 389
- RACF database templates, updating 232, 481
- RACF migration actions
 - after first IPL 232, 481
 - before first IPL 230, 231, 477, 478
 - before installing 228, 475
- RACROUTE AUTH check for SLIP command 253
- read this document, who should vii
- reference information, meaning of x
- REFORMAT
 - default 199, 430
- REFUCB function
 - default 170, 369
- REGIONX JCL keyword 23
- REGIONX keyword 106, 277
- removed data sets and paths 28
- removing check
 - PFA 256
- REPORTCOMPLETIONS option from the IEAOPTxx member, RMF action 254
- required action, meaning of x
 - resolver
 - resolver address space initialization 328
- Resource Measurement Facility (RMF)
 - update user written programs and applications that use ERBZFST3 or ERBZFAT3 223, 467
- restrictions, meaning of x
- RMF
 - determine whether RMF should monitor zFS file system activity by
 - default 222
 - ERB2XDGS 464
 - ERB3XDRS 464
 - SMF 74.9 data collection 470
 - RMF migration actions
 - after first IPL 224, 469
 - before first IPL 464
 - RMF Monitor II Sysplex Data Gathering services 464
 - RMF Monitor III Sysplex Data Retrieval services 464
 - RMF, RACF and GPMSEVER Started Task 466
 - RMF, REPORTCOMPLETIONS option from the IEAOPTxx member 254
 - root size, z/OS 8
 - router table, RACF 230, 477
 - Run-Time Library Extensions, no migration actions for 4

Runtime Diagnostics
Remove start or restart commands or
logic 116, 289

S

SADMP default 129, 305
SAF Authorization Mode
conversion to 413
SBLIM CIM Client for Java Version
2 133, 308
SCDS (source control data set), ensuring
integrity of 168, 365
scp command
migration actions 238, 490
SDI keyword 449
SDM TSO copy services commands 171,
370
SDSF migration actions
after first IPL 474
before first IPL 225, 471
SDSF, extended console name 474
Security Server migration actions
after first IPL 232, 481
before first IPL 230, 231, 477, 478
before installing 228, 475
before installing z/OS 228, 475
sending comments to IBM xiii
server
models in service 85
server, z114
software support features 60, 72
server, z13
software support features 43
server, z13s
software support features 43
server, z196
software support features 60, 72
server, zEC12
software support features 60
set-group-id attributes
z/OS UNIX program files 245, 501
set-user-id attributes
z/OS UNIX program files 245, 501
SETLOAD IEASYM 300
sftp
migration actions 238, 489
sftp command
migration actions 238, 490
SHARED mode, removal 94, 252
sharing restrictions, PDSE 37
shortcut keys 511
Simple Mail Transport Protocol 136, 319
SLIP command
MODE=HOME specification 115, 288
SMA fields from the SMS storage group
construct IGDSGD 368
SMF 74.9 data collection 470
SMF type 92 subtype 11 close
records 503
SMFLIMxx parmlib member 23
SMP/E REPORT MISSINGFIX
FIXCAT 66, 77
SMP/E, no migration actions for 4
SMS control data sets, migrating 168,
365
SMS volume selection 391

SNMP agent, discontinue use of 200,
431
Software Management task
migration consideration 421
source control data set (SCDS), ensuring
integrity of 168, 365
ssh command
migration actions 238, 490
ssh_config
migration actions 239, 490
ssh-keygen
migration actions 240, 491
ssh-keyscan
migration actions 240, 492
ssh-rand-helper
migration actions 237, 492
sshd command
migration actions 239, 491
sshd_config
migration actions 239, 491
SSI 54
JES3 release format 447
SSI 82
JES3 release format 447
SSI 83
JES3 release format 447
SSI 85
authority 441
stand-alone dump
IPCS 92, 250
stand-alone dump, reassembling 101,
263
Stand-Alone Services, building core
image of DFSMSdss 180, 386
steps for migration 1
steps to take, meaning of x
sticky attribute
z/OS UNIX program files 245, 501
sticky bit files 504, 507
storage
backing virtual 25
evaluation with zSoftCap 7
setting virtual limits 23
subsystems, reconnecting 22
summary of changes xv, xvi
Summary of changes xvi
SVC routines, migrating 19
SYNAD= sub-parameter 176, 380
SYS1.IMAGELIB 174, 375
SYS1.MACLIB(FOTSMF77)
migration actions 241, 493
SYS1.PARMLIB
used by IPCS 13
using shipped members of 15
SYS1.PROCLIB, using shipped members
of 15
syslogd 148, 332
sysplex
Coupling Facility 128, 303
CTRACE buffers 113, 287
sysplex migration actions
before installing 91, 249
sysplex root from HFS to zFS,
migrating 243, 499
SYSPRINT data set 93, 251
system impacts, meaning of x

System SSL application
configurations 158, 160, 355, 356
System SSL migration action 350, 352,
353
System SSL, ensuring all RACF user IDs
that start SSL applications in non-FIPS
mode can access the CSFRNG resource
of the CSFSERV class 353
System SSL, ensuring ICSF is available
when running System SSL in FIPS
mode 350
System SSL, modify automated scripts
running the gskkyman utility to interact
with new menus 352
system symbol underscore 103, 280

T

target system hardware requirements,
meaning of x
target system software requirements,
meaning of x
tasks
migration actions for
/samples/ssh_smf.h
steps for 241, 493
migration actions for sftp
steps for 238, 489
migration actions for ssh
steps for 238, 490
migration actions for ssh_config
steps for 239, 490
migration actions for ssh-keygen
steps for 240, 491
migration actions for ssh-keyscan
steps for 240, 492
migration actions for ssh-rand-helper
steps for 237, 492
migration actions for sshd
steps for 239, 491
migration actions for sshd_config
steps for 239, 491
migration actions for
SYS1.MACLIB(FOTSMF77)
steps for 241, 493
migration actions for users running
scp
steps for 240, 492
migration actions for users running
sftp
steps for 240, 492
migration actions for users running
ssh
steps for 240, 492
TCP related configuration
statements 330
TCP/IP
legacy device types 134, 138, 317, 321
TCP/IP profile
IPSEC statement
DVIPSEC parameter 312
TCPIP
before the first IPL 327
terminology used in this document viii
TFTP removal 139, 322
TIBUF poolsize value
T1BUF pool 150, 339

TIOC, no migration actions for 4
TLSv1.2 340
TRACEENTRY option and ICSF 163, 360
TRACKDIRLOAD 271
trademarks 517
TSO/E, EXECIO under REXX
EXECIO under REXX, TSO/E 482
TUNE=OLD, DFSORT 397

U

unsupported devices, removing 87
upgrade Java support for IPP
Server 202, 433
upgrade web browser for Infoprint
Central 202, 433
URL
for CFCC levels and processors 89
for CFSizer tool 89
for flashes 23, 25
for ISVs 22
for PSP buckets 5
for zSoftCap 7
use of ICSF when running FIPS 140-2
mode applications 350
use this document, how to viii
user exits
migrating 19
SDSF 225, 471
user interface
ISPF 511
TSO/E 511
user modifications
examining 19
for Language Environment
options 453
usermods
examining 19
for Language Environment
options 453
users running scp
migration actions 240, 492
users running sftp
migration actions 240, 492
users running ssh
migration actions 240, 492

V

V2R2 changes xvi
VERIFYOFFLINE
default 199, 430
virtual storage
backing 25
verifying limits 23
VTOC track, DFSMSHsm
default change for restore 393

W

web address
for CFCC levels and processors 89
for CFSizer tool 89
for flashes 23, 25
for ISVs 22

web address (*continued*)
for PSP buckets 5
for z/OSMF 427
for zSoftCap 7
web browser support for Infoprint
Central, upgrading 202, 433
when change was introduced, meaning
of x
who should read this document vii
WLM
IWM4HLTH service 123, 296
IWMSRDRS 124, 298
IWMSRSRG 124, 298
service definition 126, 299
service policy 126, 299

X

XCF group members 9
XCF groups 9
XL C/C++ migration actions
after first IPL 234, 485
before first IPL 234, 485
before installing 233, 484

Z

z/OS
release support 85
z/OS data set and file REST interface
cataloged procedure 423, 424
setting up 423, 424
z/OS elements
Font Collection 485
z/OS Font Collection
before IPL
migration action 485
using IBM fonts 235, 485, 487
z/OS Management Facility, IBM 195, 413, 426
z/OS PKI Services
migration action 165, 361
z/OS root size 8
z/OS Security Level 3, no migration
actions for 4
z/OS UNIX 245, 501
z/OS UNIX file 144, 336
z/OS UNIX migration actions
after first IPL 495
before first IPL 246, 502
before installing 494
z/OS UNIX set-group-ID privileged
programs 506
z/OS UNIX set-user-ID privileged
programs 506
z/OSMF 195, 413, 426
filtering tables 197, 428
IBM Configuration Assistant for z/OS
Communications Server 309
table filters 197, 428
z/OSMF bookmark link 427
z/OSMF server
cataloged procedures 423, 424, 425
setting up 423, 424, 425
started tasks 423, 424, 425

z11 mode
JES2 208, 442
z114 server
compatibility changes 60, 72
migrating to 60, 72
z13 server
compatibility changes 43
migrating to 43
z13s server
compatibility changes 43
migrating to 43
z196 server
compatibility changes 60, 72
migrating to 60, 72
zEC12 server
compatibility changes 60
migrating to 60
zEnterprise
migrating to 60, 72
zFS compatibility mode aggregates 402
zFS multi-file system aggregates 402
zFS, migrating from HFS to 241, 497
zlsf shell command
support added 496
ZOSMF**. generic profile
removing 196, 419
ZOSMFAD user ID
removing after migration 417, 418, 419
zSoftCap 7
zSoftware Migration Capacity Planning
Aid (zSoftCap) 7



Product Number: 5650-ZOS

Printed in USA

GA32-0889-08

