z/OS

Migration

Version 1 Release 7

"When behaviors aren't the same anymore,
Migration actions are called for."

z/OS

Migration

Version 1 Release 7

> **Note**
>
> Before using this information and the product it supports, be sure to read the general information under "Notices" on page 339.

Ninth Edition, January 2006

This is a major revision of GA22-7499-07.

This edition applies to version 1 release 7 of z/OS (5694-A01) and to all subsequent releases and modifications until otherwise indicated in new editions.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address below.

IBM welcomes your comments. A form for readers' comments may be provided at the back of this publication, or you may address your comments to the following address:
   IBM Corporation
   Department 55JA, Mail Station P384
   2455 South Road
   Poughkeepsie, NY 12601-5400
   United States of America

   FAX (United States and Canada): 1+845+432-9405
   FAX (Other Countries):
      Your International Access Code +1+845+432-9405

   IBMLink (United States customers only): IBMUSM10(MHVRCFS)
   Internet e-mail: mhvrcfs@us.ibm.com
   World Wide Web: http://www.ibm.com/servers/eserver/zseries/zos/webqs.html

If you would like a reply, be sure to include your name, address, telephone number, or FAX number.

Make sure to include the following in your comment or note:
*   Title and order number of this document
*   Page number or topic related to your comment

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

Contents

Tables

xiii

About this document

This document describes how to migrate *to* z/OS® Version 1 Release 7 (V1R7) *from* the following releases:
- z/OS V1R6
- z/OS V1R5
- z/OS V1R4

After a successful migration, the applications and resources on your new z/OS V1R7 system function the same way (or similar to the way) they did on your previous system. The only new functions enabled on the new system are those required on the new system.

This document does not explain how to make productive use of (exploit) new functions in z/OS. For that information, see the many publications that pertain to the z/OS base elements and optional features. Also, this document does not focus on z/OS.e, but most of the migration actions apply nonetheless.

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 V1R7.

How this document is organized

The first four chapters of this document are general in scope, that is, not devoted to a specific z/OS base element or optional feature. Chapter 1 is an introduction, Chapter 2 describes migration actions for everyone (that is, system-level actions), Chapter 3 describes hardware migration actions, and Chapter 4 summarizes sysplex migration actions.

The remaining chapters are devoted to the specific elements and features that have migration actions, with one element or feature per chapter. These chapters are in alphabetic order — from BCP (Chapter 5) to z/OS UNIX® (Chapter 29). Within each chapter, the following standard organization is used:

> Migration actions to perform *before installing* z/OS V1R7
>
> Migration actions to perform *before the first IPL* of z/OS V1R7
>
> Migration actions to perform *after the first IPL* of z/OS V1R7

How to use this document

z/OS migration documentation has undergone a transition from many documents that take a broad view of migration to one document (this one) that takes a narrower view of migration. By broad view is meant that any change you made for a new release was considered migration, whether the change was to exploit new functions or just to make the new system behave as the old one did. The narrower view sees migration as involving only those actions required to make the new system behave as the old one did. Exploitation of new functions is a separate task, following migration, and is described in element-specific and feature-specific documentation.

The transition has taken place as follows:

- In z/OS V1R4, this document was created. It consolidated migration information from the many element and feature migration documents into one place for the OS/390-V2R10-to-z/OS-V1R4 migration path. It used (and continues to use) the narrow definition of migration. All the element and feature migration documents continued to exist, covered all supported migration paths (not just one), and used the broad definition of migration.

- In z/OS V1R5, this document was expanded to cover all supported migration paths — z/OS V1R4 to z/OS V1R5, z/OS V1R3 to z/OS V1R5, and z/OS V1R2 to z/OS V1R5. It continued to use the narrow definition of migration. The element and feature migration documents continued to exist (except for Infoprint® Server and MVS™), continued to cover all supported migration paths, and continued to use the broad definition of migration.

  In z/OS V1R4, this document also contained an appendix that summarized interface changes and another appendix that summarized the release enhancements. As of z/OS V1R5, this information is in other documents. The interface changes are in *z/OS Summary of Message and Interface Changes*, and the enhancements are in *z/OS Introduction and Release Guide*.

- In z/OS V1R6, the element and feature documents devoted solely to migration were eliminated, except for the JES2 and JES3 migration documents, which were eliminated in z/OS V1R7, and *z/OS XL C/C++ Compiler and Run-Time Migration Guide for the Application Programmer*, which is directed to application programmers and is not planned for removal. The migration information in the other element and feature documents has been removed. This document is closer to being the sole z/OS migration document for system programmers. This document continues to use the narrow definition of migration. Exploitation of new functions is described in the many element and feature documents.

- In z/OS V1R7, the transition is complete. This document is the sole z/OS migration document for system programmers. (*z/OS XL C/C++ Compiler and Run-Time Migration Guide for the Application Programmer*, which is directed to application programmers, continues to exist and is not planned for removal.) This document continues to use the narrow definition of migration. Exploitation of new functions is described in the many element and feature documents.

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, "Introduction," on page 1. You can then proceed sequentially through the subsequent chapters or in whatever order you prefer based on element or feature interest. The chapters are in alphabetic order by name of element or feature, once you pass the chapter on migration actions for everyone, the chapter on hardware migration actions, and the chapter on sysplex migration actions. Another way to proceed is to concentrate first on preinstall migration actions within each chapter, then pre-IPL migration actions, and then post-IPL migration actions. These actions are clearly identified by major headings within each chapter.

Conventions and terminology used in this document

When this document refers to IBM® @server zSeries® servers without stating a specific server, it refers to all of the zSeries servers (z990, z890, z900, and z800).

Important terms you should understand are:

- *Migration.* Migration is the installation of a new version or release of a program to replace an earlier version or release. 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. Migration does not include exploitation of new functions except for new functions that are now required, such as workload manager (WLM) goal mode, which became a requirement in z/OS V1R3 when compatibility mode was no longer supported.

- *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.

- *Exploitation.* Exploitation is making productive use of new functions. Exploitation follows migration.

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

- *Actions to perform before installing z/OS V1R7.* 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 don't need the z/OS V1R7 level of code to make these changes, and the changes don't require the z/OS V1R7 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 V1R7.

- *Actions to perform before the first IPL of z/OS V1R7.* These are migration actions that you perform after you've installed z/OS V1R7 but before the first time you IPL. These actions require the z/OS V1R7 level of code to be installed but don't require it to be active. That is, you need the z/OS V1R7 programs, utilities, and samples in order to perform the migration actions, but the z/OS V1R7

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 V1R7 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 V1R7 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 V1R7.** These are migration actions that you can perform only after you've IPLed z/OS V1R7. You need a running z/OS V1R7 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 V1R7 to be active to perform the task. You might perform the task quite a while after the first IPL. In the case of activating z2 mode for JES2, it could be months after the first IPL.

Each migration action within the headings above 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.
- *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.

Related information

See *z/OS Introduction and Release Guide* for an introduction to z/OS and an overview of the new functions in each release of z/OS.

See *z/OS and z/OS.e Planning for Installation* for a summary of installation changes in each release of z/OS, driving system hardware and software requirements, target system hardware and software requirements, the coexistence-migration-fallback policy, required releases of IBM middleware products, and considerations for planning future installations. As an alternative to the document, use the Web-based, interactive z/OS and z/OS.e Installation Planning Wizard at http://www.ibm.com/eserver/zseries/zos/wizards/.

To view, search, and print z/OS publications, go to the z/OS Internet Library:

`http://www.ibm.com/eserver/zseries/zos/bkserv/`

Using LookAt to look up message explanations

LookAt is an online facility that lets you look up explanations for most of the IBM messages you encounter, as well as for some system abends and codes. Using LookAt to find information is faster than a conventional search because in most cases LookAt goes directly to the message explanation.

You can use LookAt from the following locations to find IBM message explanations for z/OS elements and features, z/VM®, VSE/ESA™, and Clusters for AIX® and Linux®:

- The Internet. You can access IBM message explanations directly from the LookAt Web site at http://www.ibm.com/eserver/zseries/zos/bkserv/lookat/.
- Your z/OS TSO/E host system. You can install code on your z/OS or z/OS.e systems to access IBM message explanations using LookAt from a TSO/E command line (for example: TSO/E prompt, ISPF, or z/OS UNIX System Services).
- Your Microsoft® Windows® workstation. You can install LookAt directly from the *z/OS Collection* (SK3T-4269) or the *z/OS and Software Products DVD Collection* (SK3T4271) and use it from the resulting Windows graphical user interface (GUI). The command prompt (also known as the DOS > command line) version can still be used from the directory in which you install the Windows version of LookAt.
- Your wireless handheld device. You can use the LookAt Mobile Edition from http://www.ibm.com/servers/eserver/zseries/zos/bkserv/lookat/lookatm.html with a

handheld device that has wireless access and an Internet browser (for example: Internet Explorer for Pocket PCs, Blazer or Eudora for Palm OS, or Opera for Linux handheld devices).

You can obtain code to install LookAt on your host system or Microsoft Windows workstation from:

- A CD-ROM in the *z/OS Collection* (SK3T-4269).
- The *z/OS and Software Products DVD Collection* (SK3T4271).
- The LookAt Web site (click **Download** and then select the platform, release, collection, and location that suit your needs). More information is available in the LOOKAT.ME files available during the download process.

Using IBM Health Checker for z/OS

IBM Health Checker for z/OS is a z/OS component that installations can use to gather information about their system environment and system parameters to help identify potential configuration problems before they impact availability or cause outages. Individual products, z/OS components, or ISV software can provide checks that take advantage of the IBM Health Checker for z/OS framework. This book may refer to checks or messages associated with this component.

For additional information about checks and about IBM Health Checker for z/OS, see *IBM Health Checker for z/OS: User's Guide*. z/OS V1R4, V1R5, and V1R6 users can obtain the IBM Health Checker for z/OS from the z/OS Downloads page at http://www.ibm.com/eserver/zseries/zos/downloads/.

SDSF also provides functions to simplify the management of checks. See *z/OS SDSF Operation and Customization* for additional information.

Summary of changes

This topic summarizes the changes made to this document.

Summary of Changes
for GA22-7499-08
z/OS Version 1 Release 7

This document contains information previously presented in GA22-7499-07, which supports z/OS V1R7.

New information:

- The Distributed File Service coexistence and fallback PTFs for APAR OA11573 are now known, so the APAR number in "Install coexistence and fallback PTFs" on page 4 was replaced with the PTF numbers: PTF UA20483 for z/OS V1R6, PTF UA20482 for z/OS V1R5, and PTF UA20485 for z/OS V1R4.
- The HCD coexistence and fallback PTFs for APAR OA07875 are now known, so the APAR number in "Install coexistence and fallback PTFs" on page 4 was replaced with the PTF numbers: PTFs UA90174 and UA90175 for z/OS V1R6, R5, and R4.
- The ISPF coexistence and fallback PTFs for APAR OA12382 are now known, so the APAR number in "Install coexistence and fallback PTFs" on page 4 was replaced with the PTF numbers: PTF UA19930 for z/OS V1R6, PTF UA19929 for z/OS V1R5, and PTF UA19928 for z/OS V1R4.
- The ISPF coexistence and fallback PTFs for APAR OA12436 are now known, so the APAR number in "Install coexistence and fallback PTFs" on page 4 was replaced with the PTF numbers:
  - For z/OS V1R6: PTF numbers UA19933, UA19942, UA19943, UA19944, UA19945
  - For z/OS V1R5: PTF numbers UA19932, UA19938, UA19939, UA19940, UA19941
  - For z/OS V1R4: PTF numbers UA19931, UA19934, UA19935, UA19936, UA19937
- JES2 coexistence and fallback PTFs for APAR OA12472 are new and were added to "Install coexistence and fallback PTFs" on page 4. The PTFs are UA20902 for z/OS V1R5-V1R6 JES2 and UA20901 for z/OS V1R4 JES2.
- In "Remove references to deleted data sets and paths" on page 40, notes were added that data sets SEQAAUTH, SEQAMOD, and SEQASAMP should not be removed because the Debug Tool product still uses these data sets.
- "Remove security-related parameters from IDCAMS ALTER" on page 192 is new.
- "Install the PTF for APAR OA13792 to avoid message GFSC729W" on page 271 is new.
- "Authorize the z/OS NFS server for component trace" on page 276 is new.
- "Add new component trace member CTINFS00 to parmlib" on page 275 is new.
- "Update the NFS client procedure" on page 275 is new.
- "Update the NFS server procedure" on page 276 is new.
- "Implement an exit routine if you want to allow sharing a console across address spaces" on page 289 is new.
- "Modify POSIT values that were documented incorrectly in an IMS redbook" on page 299 is new.

- "Use the changed cp and mv defaults for files with different source and target tags" on page 328 is new.

Changed information:
- The statement "removal of support for the HFS file system is planned for a future release" was removed from "Migrate from HFS file systems to zFS file systems" on page 334. Support for the HFS file system has been stabilized and you are encouraged to migrate to the zFS file system for better performance, but IBM has not announced removal of support for the HFS file system.

Moved information:
- "Rename sample fields" on page 304 was moved. It was in the Integrated Security Services chapter but belongs in the Security Server chapter.

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

**Summary of Changes
for GA22-7499-07
z/OS Version 1 Release 7**

This document contains information previously presented in GA22-7499-06, which supports z/OS V1R6.

New information:
- Approximately 50 migration actions are new, meaning they were not actions to perform when migrating to z/OS V1R6 but are actions to perform when migrating to z/OS V1R7. They are marked with "change bars".
- "z/OS V1R6 coexistence and fallback PTFs" on page 5 is new.
- All information about the IBM System z9 109 (z9-109) server is new.

Changed information:
- As of z/OS V1R7, the z/OS C/C++ compiler has been rebranded to z/OS XL C/C++.

Deleted information:
- Approximately 40 migration actions have been deleted. They were actions to perform when migrating from z/OS V1R3 (the earliest release supported for migration to z/OS V1R6) but are not actions to perform when migrating from z/OS V1R4 (the earliest release supported for migration to z/OS V1R7).

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

**Summary of Changes
for GA22-7499-06
z/OS Version 1 Release 6**

This document contains information previously presented in GA22-7499-05, which supports z/OS V1R6.

New information:

- Communications Server coexistence PTF UA11849 has been added to the z/OS V1R4 coexistence PTFs.
- By default in z/OS V1R5 and later, DFSMSdss™ obtains 64-bit backed I/O buffers when running in z/Architecture™ mode. If you want DFSMSdss to obtain 31-bit backed I/O buffers, you've been told to specify `EXEC PARM='ZBUFF64R=NO'` in the JCL or API invocation. Now a second method has been added, namely, change the installation's default by turning off the UFPZB64R bit in the ADRUFO block with the options installation exit routine, ADRUIXIT. See item 21 on page 68 for details (in the migration action Migrate to z/Architecture).
- "IP Services: Update /etc configuration files" on page 147 is new.
- The INETD daemon has been added to "Update /etc configuration files" on page 327.

Changed information:

- Previously, you were told that the system now uses the extended channel measurement block (ECMB) instead of the CMB, that you should convert user-written programs that use the CMB to use the ECMB, and that you should contact ISVs to obtain updates to ISV programs that use the CMB. Furthermore, you were told that if ISV support is not available, you could specify ECMB=NO in parmlib member IEAOPT*xx* as a circumvention until the ISV support is available.

  What's changed is that the circumvention now has a specific end date. z/OS V1R6 is planned to be the last release in which the circumvention is available.
- The date for removal of support for 1-byte console IDs has been changed from an unannounced future date to z/OS V1R7. See "Modify code that uses 1-byte console IDs" on page 93.
- The date for removal of the ability to customize the Communications Server sysObjectID value has been changed from an unannounced future date to z/OS V1R6. See "IP Services: Remove customization of SNMP sysObjectID MIB object in OSNMPD.DATA file" on page 134.
- The time to perform JES2 migration action "Migrate to z2 mode" on page 245 has been changed from after first IPL to before installing z/OS.
- The time to perform SMP/E migration actions has been clarified. Previously, the two categories were before installing SMP/E and after installing SMP/E. Now they are after installing SMP/E but before starting to use it, and after starting to use SMP/E. See Chapter 26, "SMP/E migration actions," on page 307.
- "Change NOAUTOMOVE to AUTOMOVE for sysplex-aware file systems" on page 329 has been clarified and corrected.

Summary of Changes
for GA22-7499-05
z/OS Version 1 Release 6

This document contains information previously presented in GA22-7499-04, which supports z/OS V1R5.

New information:

- Approximately 45 migration actions are new, meaning they were not actions to perform when migrating to z/OS V1R5 but are actions to perform when migrating to z/OS V1R6. They are marked with "change bars".
- "z/OS V1R5 coexistence and fallback PTFs" on page 8 is new.
- The "Steps to take" topic in "Migrate /etc and /var system control files" on page 32 has been enhanced.

Deleted information:

- Approximately 25 migration actions have been deleted. They were actions to perform when migrating from z/OS V1R2 (the earliest release supported for migration to z/OS V1R5) but are not actions to perform when migrating from z/OS V1R3 (the earliest release supported for migration to z/OS V1R6).
- "Appendix A. How we tested the migration tasks in this document" has been deleted. Migration test experiences are included in *zSeries Platform Test Report*, which is available from http://www.ibm.com/eserver/zseries/zos/integtst/.

This document contains terminology, maintenance, and editorial changes.

**Summary of Changes
for GA22-7499-04
z/OS Version 1 Release 5**

This document contains information previously presented in GA22-7499-03, which supports z/OS V1R5.

New information:

- All information about the IBM @server zSeries 890 (z890) server is new. The most significant updates are in "Migrate to a z990 or z890 server" on page 74.

Changed information:

- The tables of coexistence and fallback PTFs have been updated. They are in "Install coexistence and fallback PTFs" on page 4.

This document contains terminology, maintenance, and editorial changes.

**Summary of Changes
for GA22-7499-03
z/OS Version 1 Release 5**

This document contains information previously presented in GA22-7499-02, which supports z/OS V1R4.

New information:

- This document now supports all valid migration paths. (For z/OS V1R5, migrations are supported from z/OS V1R4, z/OS V1R3, and z/OS V1R2.) The previous document (for z/OS V1R4) supported only one migration path (from OS/390® V2R10).
- Approximately 50 migration actions are new, meaning they were not actions to perform when migrating to z/OS V1R4 but are actions to perform when migrating to z/OS V1R5. They are marked with "revision bars".

Moved information:

- "Appendix B. z/OS summary of interface changes" is moved to the new document *z/OS Summary of Message and Interface Changes*. But the scope of interface change information remains the same. That is, this *z/OS Migration* document continues to include interface changes within appropriate migration actions, and the new document describes *all* interface changes, regardless of whether the actions related to the changes are for migration or exploitation (or both).
- "Appendix C. New functions to consider for exploitation" is moved to *z/OS Introduction and Release Guide*.

Deleted information:

- Approximately 40 migration actions have been deleted. They were actions to perform when migrating from OS/390 V2R10 (the earliest release supported for migration to z/OS V1R4) but are not actions to perform when migrating from z/OS V1R2 (the earliest release supported for migration to z/OS V1R5).

This document contains terminology, maintenance, and editorial changes.

Summary of Changes
for GA22-7499-02 (April 2004)
z/OS Version 1 Release 4
with the enhancements that support the z890 server

This document contains information previously presented in the June 2003 edition of GA22-7499-02, which supports z/OS V1R4.

New information:

- All information about the IBM @server zSeries 890 (z890) server is new. The most significant updates are in "Migrate to a z990 or z890 server" on page 74.

Changed information:

- The table of coexistence and fallback PTFs has been updated.

This document contains terminology, maintenance, and editorial changes.

Summary of Changes
for GA22-7499-02 (June 2003)
z/OS Version 1 Release 4
with the enhancements that support the z990 server,
the z/OS V1R4 DFSMStvs feature,
and the z/OS V1R4 Consoles Enhancements feature

This document contains information previously presented in GA22-7499-01, which supports z/OS V1R4.

New information:

- The following topic has been added in support of the IBM @server zSeries 990 (z990) server: "Migrate to a z990 or z890 server" on page 74.
- The OSA/SF migration actions chapter is new.

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

Summary of Changes
for GA22-7499-01
z/OS Version 1 Release 4

This document contains information previously presented in GA22-7499-00, which supports z/OS V1R4.

New information:

- The following information is new in the migration chapters:
  - "Elements and features that don't have migration actions" on page 2 is new.

– A migration action for everyone to perform is new: "Review PSP buckets" on page 3.

– A Cryptographic Services migration action before installing is new: "ICSF: Add new services to the CICS wait list" on page 181.

- A summary of interface changes is new (but was subsequently moved to be its own document).

- An index is added.

Changed information:

- The topic "IPL with ILMMODE=NONE when on a z800 or z900 server" is retitled and changed. It is now "Remove customization for ILM" on page 27.

- The lists of deleted and new data sets are reformatted for better usability. The deleted data sets are now in a single table (Table 5 on page 41), are in alphabetic order by DDDEF name, and have an accompanying reason why each is deleted. The new data sets are now in lists by element or feature (they were by release); see "Add references to new data sets and paths" on page 53.

Moved information:

- The information in "Install coexistence and fallback PTFs" on page 4 used to be in an appendix but is now, more appropriately, in a regular migration chapter.

Deleted information:

- The topics "Secure your system resources" and "Ensure the data integrity of shared system resources" have been deleted from Chapter 2, "Migration actions for everyone." They shouldn't have been included because they don't apply specifically to an OS/390 V2R10 to z/OS V1R4 migration.

- The topic "Tivoli® NetView® and System Automation ordering and installation" is deleted from Chapter 2, "Migration actions for everyone." This topic is more appropriate to *z/OS and z/OS.e Planning for Installation*, where it already exists.

- The topic "Change PFK tables for MCS consoles because of the double underscore" is deleted from Chapter 5, "BCP migration actions." It shouldn't have been included in the first place.

- The topic "Convert to system-managed storage" is deleted from Chapter 8, "DFSMS migration actions." It shouldn't have been included because it doesn't apply specifically to an OS/390 V2R10 to z/OS V1R4 migration.

- The topic "Provide for virtual storage requirements of new product support" is deleted from Chapter 8, "DFSMS migration actions." It's covered in several other migration actions.

- The topic "Review informational APAR II11768 for last-minute information" is deleted from Chapter 18, "JES3 migration actions." The migration action is already covered in "Install coexistence and fallback PTFs" on page 4.

- The topic "RACF: Sysplex communication mode performance enhancements" is deleted from Chapter 25, "Security Server migration actions." It shouldn't have been included in the first place.

- The topic "Access Control Lists (ACL) preparation" is deleted from Chapter 29, "z/OS UNIX migration actions." It describes an exploitation action, not a migration action.

- The topic "Start the TCP/IP resolver address space" is deleted from Chapter 29, "z/OS UNIX migration actions." It shouldn't have been included in the first place.

- The topic "Keeping AUTOMOUNT policies consistent across the sysplex" is deleted from Chapter 29, "z/OS UNIX migration actions." It shouldn't have been

included in the first place because it doesn't apply specifically to an OS/390 V2R10 to z/OS V1R4 migration. It applies to a migration from a nonshared HFS environment to a shared one.

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

Chapter 1. Introduction

Migration is the process of installing a new version or release of a program to replace an earlier version or release. After a successful migration, the applications and resources on your new system function the same way (or similar to the way) they did on your old system. You are then in a position to use your new system to do whatever customizing and programming are necessary to take advantage of (exploit) the enhancements available on your new system.

This document describes what you must do to migrate from any of the three releases that are supported for direct migration to z/OS V1R7:
- z/OS V1R6
- z/OS V1R5
- z/OS V1R4

If you want to migrate to z/OS V1R7 from any other release, contact your IBM representative to find out what alternatives are available.

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 V1R7. Good sources of information are *z/OS Introduction and Release Guide*, *z/OS and z/OS.e Planning for Installation*, and http://www.ibm.com/eserver/zseries/zos/.

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 V1R7. In this document, the actions you can perform on your existing system are identified by headings that say **actions to perform before installing z/OS V1R7**. (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 V1R7.

3. Order and install coexistence and fallback service for any system that will share resources with a z/OS V1R7 system. (See "Install coexistence and fallback PTFs" on page 4.) Again, this service needs to be installed on, or cloned to, all existing systems. However, now all systems that will share resources with the z/OS V1R7 system, as well as all systems that will be migrated to z/OS V1R7, need this service.

4. Prepare the driving system. For driving system requirements, see *z/OS and z/OS.e Planning for Installation*.

5. Order and install z/OS V1R7. If you use a ServerPac, refer to *ServerPac: Installing Your Order*. If you use a CBPDO, refer to *z/OS Program Directory*.

6. Prepare target system hardware and software. During this step, use this document and perform the migration actions identified by headings that say **actions to perform before the first IPL of z/OS V1R7**. (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 V1R7 system with your updated customization and configuration files.

1

8. Perform any migration actions identified by headings that say **actions to perform after the first IPL of z/OS V1R7**. (Again, not all of the actions are required. Some depend on your environment, configuration, and workload, and are identified accordingly.)

9. Deploy z/OS V1R7 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 V1R6, z/OS V1R5, or z/OS V1R4, exploit the functions introduced in z/OS V1R7.

11. Deploy this exploitation on other systems (again within a sysplex, data center, and eventually enterprise).

Elements and features that don't have migration actions

The following z/OS V1R7 elements and features don't have migration actions and thus are not discussed in this document:

- BDT
- BDT File-to-File
- BDT SNA NJE
- BookManager® BUILD
- BookManager READ
- Common Information Model (CIM)
- Communications Server Security Level 3
- DCE Base Services
- EREP
- ESCON® Director Support
- FFST
- GDDM
- GDDM-PGF
- GDDM-REXX
- HCM
- HLASM Toolkit
- IBM HTTP Server
- MICR/OCR
- msys for Operations
- msys for Setup
- TIOC
- z/OS Security Level 3
- 3270 PC File Transfer Program

Chapter 2. Migration actions for everyone

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

Migration actions for everyone before installing z/OS V1R7

This section describes general migration actions that you can perform on your current (old) system. You don't need the z/OS V1R7 level of code to make these changes, and the changes don't require the z/OS V1R7 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).

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
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.

Steps to take:

1. Identify which PSP buckets to review by knowing their upgrade IDs (or "upgrades"). The most relevant upgrades are those related to z/OS V1R7 and its servers:
   - **ZOSV1R7** for z/OS V1R7
   - **2094DEVICE** for the z9-109 server
   - **2084DEVICE** for the z990 server
   - **2086DEVICE** for the z890 server
   - **2064DEVICE** for the z900 server
   - **2066DEVICE** for the z800 server
2. Obtain the PSP buckets from https://techsupport.services.ibm.com/server/390.psp390 or from IBMLink™.
3. Review the PSP buckets and take whatever actions are prescribed.

Reference information: For z/OS subsets, see *z/OS Program Directory*.

Install coexistence and fallback PTFs

Description: Coexistence and fallback PTFs installed on back-level systems allow those systems to coexist with z/OS V1R7 systems during your migration, and allow backout from z/OS V1R7 to the back-level systems if necessary. Coexistence and fallback are important because they allow you to migrate systems in a multisystem configuration to z/OS V1R7 using rolling IPLs (one system at a time), allowing for continuous application availability.

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
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: • "z/OS V1R6 coexistence and fallback PTFs" • "z/OS V1R5 coexistence and fallback PTFs" on page 8 • "z/OS V1R4 coexistence and fallback PTFs" on page 13
Restrictions:	None.
System impacts:	None.

Steps to take: Depending on the back-level releases with which your z/OS V1R7 system coexists, install the appropriate coexistence and fallback PTFs before introducing z/OS V1R7 into your environment:

- "z/OS V1R6 coexistence and fallback PTFs"
- "z/OS V1R5 coexistence and fallback PTFs" on page 8
- "z/OS V1R4 coexistence and fallback PTFs" on page 13

Reference information: For an explanation of the z/OS coexistence-migration-fallback policy, see *z/OS and z/OS.e Planning for Installation*.

z/OS V1R6 coexistence and fallback PTFs

Install, on z/OS V1R6, the coexistence and fallback PTFs listed in Table 1.

Table 1. Coexistence and fallback PTFs needed on z/OS V1R6 systems

Element or feature, and reason PTFs are needed	z/OS V1R6 PTFs
BCP: A z/OS V1R7 system cannot join a sysplex of lower-level systems, and a lower-level system cannot join a sysplex of z/OS V1R7 systems, without this PTF.	UA16036
BCP: z/OS V1R7 introduces the **logger** log stream DUPLEXMODE(DRXRC) specification. If DUPLEXMODE(DRXRC) is specified in a z/OS V1R7 system in a sysplex, and prior releases are running in the same sysplex, the PTF must be installed. If DUPLEXMODE(DRXRC) is not specified, installing the PTF is not required but is nevertheless recommended to avoid any complications if the configuration changes.	UA17179
BCP: Allows a pre-z/OS V1R7 system to use an **IODF** that was created using z/OS V1R7 HCD.	UA17028
BCP: Increased CPU utilization in the **console address space** might be reported on all systems in a sysplex after introducing a z/OS V1R4 system with the z/OS V1R4 Consoles Enhancements feature, or later-level system, into the sysplex. The coexistence PTF prevents heavy message traffic on the z/OS V1R7 system from impacting the other systems in the sysplex.	UA16510
BCP: Allows a z/OS V1R6 system to correctly handle blank **WTOs** issued to another system.	UA09962
BCP: Large format sequential data sets are only supported by z/OS V1R7. The coexistence PTF causes z/OS to detect the accidental specification of such a data set for stand-alone dump output and to reject its use, as has been done for data set organizations such as PDS.	UA19042

Element or feature, and reason PTFs are needed	z/OS V1R6 PTFs
BCP: Provides compatibility support for the corrected **global resource serialization** ISGLOCK structure rebuild processing in z/OS V1R7 APAR OA11147.	UA18542
DFSMSdfp: An enhancement in the z/OS V1R7 Object Access Method (OAM) component introduces a new valid value ("R") for the object location in the object directory to indicate that the object resides on DB2® disk in recalled status. This PTF enables pre-z/OS V1R7 OAMs to coexist in an **OAMplex** with OAMs at the z/OS V1R7 level.	UA16996
DFSMSdfp: As part of **VSAM extent constraint removal** in z/OS V1R7, these PTFs prevent pre-z/OS V1R7 systems from opening data sets that have more than 255 extents. Also, if a data set is open and a z/OS V1R7 job extends it past 255 extents, the close on the pre-z/OS V1R7 system fails. Finally, these PTFs prevent conversion of a data set having more than 255 extents from being converted by DFSMSdss to a non-SMS managed data set on pre-z/OS V1R7 releases.	UA14884, UA16225, UA16798
DFSMSdfp: z/OS V1R7 supports new QNAME and RNAME parameters for **VSAM RLS**. The coexistence PTFs prevent serialization problems from occurring when the new parameters are used in a global resource serialization complex that includes a pre-z/OS V1R7 system.	UA16635, UA16924, UA17236
DFSMSdfp: z/OS V1R7 supports **large format sequential data sets**. These PTFs cause pre-z/OS V1R7 systems to issue ABEND 213-14 or 213-16 if a program attempts to open data sets that cannot work on those systems.	UA15871, UA16552, UA18496
DFSMSdss: z/OS V1R7 supports **large format sequential data sets**. These PTFs cause pre-z/OS V1R7 systems to issue ABEND213-14 for any large format dump data sets that are provided as input to RESTORE or COPYDUMP, or output for DUMP and COPYDUMP. If DFSMSdss encounters any large format sequential data sets as input to logical data set COPY, logical and physical data set DUMP and RESTORE, data set print, or logical and physical data set RELEASE, the data set will fail with ADR878E rsn 17.	UA16798
DFSMShsm™: z/OS V1R7 supports **large format sequential data sets**. The PTFs cause pre-z/OS V1R7 systems that might potentially recall, recover, or ARECOVER a data set to first verify that the data set is not a large format data set. If it is, an error message is issued describing the reason for the failure.	UA16798, UA16953

Element or feature, and reason PTFs are needed	z/OS V1R6 PTFs
DFSMShsm: z/OS V1R7 supports **large format sequential data sets**. In an HSMplex with more than one DFSMShsm host, take care when migrating the journal to a large format sequential data set. All DFSMShsm hosts within an HSMplex must be at z/OS V1R7 before you can migrate the journal to a large format sequential data set. With the PTFs, when a pre-z/OS V1R7 DFSMShsm host attempts to open a journal, if the journal is a standard format data set, DFSMShsm initialization continues. If the journal is a large format data set, message MSGARC0509E with the "LARGE" text in the message is issued and DFSMShsm is stopped. If the journal is a striped data set, message MSGARC0509E with the "STRIPED" text in the message is issued and DFSMShsm is stopped. If the ARCBJRNL utility attempts to use a large format journal data set, it ends with return code RC40, which indicates an OPEN error.	UA15871, UA16552, UA16956, UA18496
DFSMShsm: z/OS V1R7 supports fast subsequent migration (**FSM**) of data sets. The PTFs cause DFSMShsm to set the appropriate flags during recall processing so that if the data set is later opened for output by either z/OS V1R7 systems or pre-z/OS V1R7 systems, the flags used for reconnection determination are set appropriately.	UA16851, UA16859, UA16862, UA16946
DFSMShsm: z/OS V1R7 increases the number of data set names supported in a tape table of contents (TTOC). If a system that has the coexistence PTF installed finds that the OCDS RECORDSIZE is 6144 bytes, which indicates that some instances of DFSMShsm in the HSMplex might be using the **extended TTOC**, then tape operations on that level of DFSMShsm are inhibited.	UA16949
Distributed File Service: Allows pre-z/OS V1R7 systems to tolerate new characters (@#$) allowed in z/OS V1R7 for zFS file systems and aggregates.	UA14530
Distributed File Service: Allows pre-z/OS V1R7 systems to tolerate the file system structure for z/OS V1R7 zFS file systems.	UA20483
HCD: Provides support for HCD users who share **IODF** data sets between pre-z/OS V1R7 systems and z/OS V1R7 systems.	UA90174 (base and English), UA90175 (Japanese)
ISPF: Allows pre-z/OS V1R7 systems to intelligently display the number of tracks in a large format sequential data set. If the number of tracks is greater than 64 KB, the string ">64K" and a larger explanatory message are written to the panel.	UA19930
ISPF: Provides an appropriate message when a user attempts to open a large format sequential data set from a pre-z/OS V1R7 release.	UA19933, UA19942 (Swiss German), UA19943 (Japanese), UA19944 (German), UA19945 (uppercase English)

Element or feature, and reason PTFs are needed	z/OS V1R6 PTFs
JES2: Allows a back-level JES2 to run with z/OS V1R7 JES2 in a multi-access spool (**MAS**). Install the PTFs that are appropriate to the JES2 level that you are using.	**z/OS V1R5–V1R6 JES2:** UA09501, UA18836, UA20902, UA90161; **z/OS V1R4 JES2:** UA03828, UA09500, UA18835, UA20901, UA90160
JES2: Fixes a problem on a receiving pre-z/OS V1R7 node that can occur in a rare situation with a large scheduler work block text unit (SWBTU). Data sets have a large SWBTU when MAILTO, MAILCC, and MAILBCC keywords are used in addition to other keywords on OUTPUT JCL statements. The problem is caused by APAR OA09152 (PTF UA16214 on z/OS V1R5–V1R6 JES2 or PTF UA16213 on z/OS V1R4 JES). This is a network-specific problem, not a MAS-specific problem.	**z/OS V1R5–V1R6 JES2:** UA16217; **z/OS V1R4 JES2:** UA16216
JES3: Allows a back-level JES3 to run with z/OS V1R7 JES3 in a **multisystem complex** and provides fallback support to the back-level JES3.	**z/OS V1R4 JES3:** UA04010, UA07715
NFS: Allows a pre-z/OS V1R7 NFS SMF report generator to process an SMF file that includes NFS V1R7 SMF records. Any records containing TCP/IP version 6 IP addresses will be ignored.	UA16683
NFS: Allows a pre-z/OS V1R7 NFS server to read a mount handle data set written by z/OS V1R7 NFS.	UA19507
SMP/E: Provides support for SMP/E users who share SMPCSI data sets between pre-z/OS V1R7 systems and z/OS V1R7 systems.	UO00116

z/OS V1R5 coexistence and fallback PTFs

Install, on z/OS V1R5, the coexistence and fallback PTFs listed in Table 2.

Table 2. Coexistence and fallback PTFs needed on z/OS V1R5 systems

Element or feature, and reason PTFs are needed	z/OS V1R5 PTFs
BCP: In z/OS V1R5, a **console enhancement** minimizes the possibility of outages because of exhaustion of system resources used for messaging. The PTFs allow back-level systems to tolerate the enhancement.	UA05643, UA06655
BCP: Prevents the depletion of private storage in the **console address space** on a receiving system when a large number of WTO/R messages are received on that system from other members of a sysplex.	UA07960, UA07963
BCP: Increased CPU utilization in the **console address space** might be reported on all systems in a sysplex after introducing a z/OS V1R4 system with the z/OS V1R4 Consoles Enhancements feature, or later-level system, into the sysplex. The coexistence PTF prevents heavy message traffic on the z/OS V1R7 system from impacting the other systems in the sysplex.	UA16512
BCP: Allows a z/OS V1R5 system to correctly handle blank **WTOs** issued to another system.	UA09964

Element or feature, and reason PTFs are needed	z/OS V1R5 PTFs
BCP: APARs OA05025 (PTF UA07361) and OA05391 together provide corrective service for **XCF** recovery from partial writes to couple data sets. APAR OA05391 introduces a new format for couple data set multi-subrecord check records (MSRCRs), which is required for recovery from partial writes to certain types of couple data set records. APAR OA05025 includes coexistence support that enables systems on which it is installed to interpret the new MSRCR format. Because both APARs have been incorporated into z/OS V1R6 and later, all other systems in the sysplex must be capable of interpreting the new MSRCR format before any V1R6 or later system can be IPLed into the sysplex. V1R5 systems include support for interpreting the new MSRCR format and do not require installation of additional maintenance to provide this capability. You must IPL all other systems in the sysplex with the appropriate PTF for APAR OA05025 (PTF UA07361 for V1R5) before IPLing any V1R6 or later system into the sysplex. Rolling IPLs are sufficient to install the PTFs for APARs OA05025 and OA05391. Note that the recovery provided by these two PTFs is not completely effective until all systems in the sysplex, including z/OS V1R5 systems, have been IPLed with both PTFs or with V1R6 or later.	UA07361
BCP: z/OS V1R6 has a new 64-bit **global resource serialization** ISGQUERY application programming interface (API). The PTF allows a z/OS V1R5 system to tolerate ISGQUERY requests from a z/OS V1R6 or later system.	UA09226
BCP: Provides compatibility support for the corrected **global resource serialization** ISGLOCK structure rebuild processing in z/OS V1R7 APAR OA11147.	UA18541
BCP: Allows a z/OS V1R5 system to tolerate new resource recovery services (**RRS**) restart function in z/OS V1R6 (and later).	UA09403, UA09425
BCP: Starting in z/OS V1R6, the sysplex couple data set (**CDS**) can be expanded to allow up to 2047 members in a cross-system coupling facility (XCF) group. This is an increase from the previous maximum of 1023 members per XCF group. Formatting a couple data set for more than 1023 members per group creates a Version 4 CDS. The PTF rolls back this function to z/OS V1R5. In terms of coexistence, it provides support for Version 4 sysplex CDSs on z/OS V1R5. This is important because all systems in a sysplex must support Version 4 sysplex CDSs to bring a Version 4 sysplex CDS into use, and once a sysplex is using a Version 4 sysplex CDS, a system that does not support Version 4 sysplex CDSs cannot join the sysplex.	UA09967
BCP: A z/OS V1R7 system cannot join a sysplex of lower-level systems, and a lower-level system cannot join a sysplex of z/OS V1R7 systems, without this PTF.	UA16038

Table 2. Coexistence and fallback PTFs needed on z/OS V1R5 systems (continued)

Element or feature, and reason PTFs are needed	z/OS V1R5 PTFs
BCP: z/OS V1R7 introduces the **logger** log stream DUPLEXMODE(DRXRC) specification. If DUPLEXMODE(DRXRC) is specified in a z/OS V1R7 system in a sysplex, and prior releases are running in the same sysplex, the PTF must be installed. If DUPLEXMODE(DRXRC) is not specified, installing the PTF is not required but is nevertheless recommended to avoid any complications if the configuration changes.	UA17178
BCP: Allows a pre-z/OS V1R7 system to use an **IODF** that was created using z/OS V1R7 HCD.	UA17027
BCP: Large format sequential data sets are only supported by z/OS V1R7. The coexistence PTF causes z/OS to detect the accidental specification of such a data set for stand-alone dump output and to reject its use, as has been done for data set organizations such as PDS.	UA19041
BCP, DFSMSdfp, DFSMSdss, DFSMShsm, DFSMSrmm™: In z/OS V1R6, a new function introduced by PTF UA90124 enables DFSMS software support for IBM TotalStorage® Enterprise Tape System **3592** and the media types MEDIA6, MEDIA7, and MEDIA8. Coexistence PTFs listed here allow a V1R5 system to coexist with a V1R6 or later system that uses this function.	UA90101, UA90113, UA90121, UA90127, UA90129
DFSMSdfp: z/OS V1R6 has a new PDSE address space, **SMSPDSE1**, which is restartable. The coexistence PTF allows a z/OS V1R5 system to coexist with a z/OS V1R6 or later system that is exploiting the new address space.	UA09833
DFSMSdfp: An enhancement in the z/OS V1R7 Object Access Method (OAM) component introduces a new valid value ("R") for the object location in the object directory to indicate that the object resides on DB2 disk in recalled status. This PTF enables pre-z/OS V1R7 OAMs to coexist in an **OAMplex** with OAMs at the z/OS V1R7 level.	UA16995
DFSMSdfp: As part of **VSAM extent constraint removal** in z/OS V1R7, these PTFs prevent pre-z/OS V1R7 systems from opening data sets that have more than 255 extents. Also, if a data set is open and a z/OS V1R7 job extends it past 255 extents, the close on the pre-z/OS V1R7 system fails. Finally, these PTFs prevent conversion of a data set having more than 255 extents from being converted by DFSMSdss to a non-SMS managed data set on pre-z/OS V1R7 releases.	UA14883, UA16224, UA16797
DFSMSdfp: z/OS V1R7 supports new QNAME and RNAME parameters for **VSAM RLS**. The coexistence PTFs prevent serialization problems from occurring when the new parameters are used in a global resource serialization complex that includes a pre-z/OS V1R7 system.	UA16634, UA16923, UA17235
DFSMSdfp: z/OS V1R7 supports **large format sequential data sets**. These PTFs cause pre-z/OS V1R7 systems to issue ABEND 213-14 or 213-16 if a program attempts to open data sets that cannot work on those systems.	UA15870, UA16551, UA18495

Element or feature, and reason PTFs are needed	z/OS V1R5 PTFs
DFSMSdss: z/OS V1R7 supports **large format sequential data sets**. These PTFs cause pre-z/OS V1R7 systems to issue ABEND213-14 for any large format dump data sets that are provided as input to RESTORE or COPYDUMP, or output for DUMP and COPYDUMP. If DFSMSdss encounters any large format sequential data sets as input to logical data set COPY, logical and physical data set DUMP and RESTORE, data set print, or logical and physical data set RELEASE, the data set will fail with ADR878E rsn 17.	UA16797
DFSMShsm: z/OS V1R7 supports **large format sequential data sets**. The PTFs cause pre-z/OS V1R7 systems that might potentially recall, recover, or ARECOVER a data set to first verify that the data set is not a large format data set. If it is, an error message is issued describing the reason for the failure.	UA16797, UA16952
DFSMShsm: z/OS V1R7 supports **large format sequential data sets**. In an HSMplex with more than one DFSMShsm host, take care when migrating the journal to a large format sequential data set. All DFSMShsm hosts within an HSMplex must be at z/OS V1R7 before you can migrate the journal to a large format sequential data set. With the PTFs, when a pre-z/OS V1R7 DFSMShsm host attempts to open a journal, if the journal is a standard format data set, DFSMShsm initialization continues. If the journal is a large format data set, message MSGARC0509E with the "LARGE" text in the message is issued and DFSMShsm is stopped. If the journal is a striped data set, message MSGARC0509E with the "STRIPED" text in the message is issued and DFSMShsm is stopped. If the ARCBJRNL utility attempts to use a large format journal data set, it ends with return code RC40, which indicates an OPEN error.	UA15870, UA16551, UA16955, UA18495
DFSMShsm: In z/OS V1R5, DFSMShsm is enhanced to use volume-level **fast replication** to create backup versions for sets of storage groups. A set of storage groups is defined through an SMS construct termed "copy pool". In support of fast replication, install the PTF on all z/OS V1R5 systems in a sysplex.	UA07443
DFSMShsm: z/OS V1R6 and later allow multiple secondary space management (SSM) tasks to run concurrently. The PTF allows a z/OS V1R5 system to tolerate this **SSM multitasking**.	UA09619
DFSMShsm: z/OS V1R7 supports fast subsequent migration (**FSM**) of data sets. The PTFs cause DFSMShsm to set the appropriate flags during recall processing so that if the data set is later opened for output by either z/OS V1R7 systems or pre-z/OS V1R7 systems, the flags used for reconnection determination are set appropriately.	UA16850, UA16858, UA16861, UA16945
DFSMShsm: z/OS V1R7 increases the number of data set names supported in a tape table of contents (TTOC). If a system that has the coexistence PTF installed finds that the OCDS RECORDSIZE is 6144 bytes, which indicates that some instances of DFSMShsm in the HSMplex might be using the **extended TTOC**, then tape operations on that level of DFSMShsm are inhibited.	UA16948
Distributed File Service: Allows pre-z/OS V1R7 systems to tolerate new characters (@#$) allowed in z/OS V1R7 for zFS file systems and aggregates.	UA14529

Table 2. Coexistence and fallback PTFs needed on z/OS V1R5 systems (continued)

Element or feature, and reason PTFs are needed	z/OS V1R5 PTFs
Distributed File Service: Allows pre-z/OS V1R7 systems to tolerate the file system structure for z/OS V1R7 zFS file systems.	UA20482
HCD: Provides support for HCD users who share **IODF** data sets between pre-z/OS V1R7 systems and z/OS V1R7 systems.	UA90174 (base and English), UA90175 (Japanese)
ISPF: Allows pre-z/OS V1R7 systems to intelligently display the number of tracks in a large format sequential data set. If the number of tracks is greater than 64 KB, the string ">64K" and a larger explanatory message are written to the panel.	UA19929
ISPF: Provides an appropriate message when a user attempts to open a large format sequential data set from a pre-z/OS V1R7 release.	UA19932, UA19938 (Swiss German), UA19939 (Japanese), UA19940 (German), UA19941 (uppercase English)
JES2: Allows a back-level JES2 to run with z/OS V1R7 JES2 in a multi-access spool (**MAS**). Install the PTFs that are appropriate to the JES2 level that you are using.	**z/OS V1R5–V1R6 JES2:** UA09501, UA18836, UA20902, UA90161; **z/OS V1R4 JES2:** UA03828, UA09500, UA18835, UA20901, UA90160
JES2: Fixes a problem on a receiving pre-z/OS V1R7 node that can occur in a rare situation with a large scheduler work block text unit (SWBTU). Data sets have a large SWBTU when MAILTO, MAILCC, and MAILBCC keywords are used in addition to other keywords on OUTPUT JCL statements. The problem is caused by APAR OA09152 (PTF UA16214 on z/OS V1R5–V1R6 JES2 or PTF UA16213 on z/OS V1R4 JES). This is a network-specific problem, not a MAS-specific problem.	**z/OS V1R5–V1R6 JES2:** UA16217; **z/OS V1R4 JES2:** UA16216
JES3: Allows a back-level JES3 to run with z/OS V1R7 JES3 in a **multisystem complex** and provides fallback support to the back-level JES3.	**z/OS V1R4 JES3:** UA04010, UA07715
Language Environment®: The **/etc/utmpx** file contains a user accounting database. In z/OS V1R6, the format of the records in the file was extended to support longer remote host names, 64-bit timestamp structures, and a version indicator. The coexistence PTF prevents the standard interfaces in pre-V1R6 releases from accessing /etc/utmpx databases that use the new format, avoiding confusion and possible data corruption. Attempts to access a /etc/utmpx database in the new format from an earlier release return a null pointer. Applications can use perror() to print the error message.	UQ85892
NFS: Allows a pre-z/OS V1R7 NFS SMF report generator to process an SMF file that includes NFS V1R7 SMF records. Any records containing TCP/IP version 6 IP addresses will be ignored.	UA16683
NFS: Allows a pre-z/OS V1R7 NFS server to read a mount handle data set written by z/OS V1R7 NFS.	UA19507
SMP/E: Allows back-level SMP/E to tolerate enhancements introduced in z/OS V1R6 SMP/E (which is equivalent to SMP/E V3R3).	UR54451, UR54454 (if Japanese)

Table 2. Coexistence and fallback PTFs needed on z/OS V1R5 systems (continued)

Element or feature, and reason PTFs are needed	z/OS V1R5 PTFs
SMP/E: Provides support for SMP/E users who share SMPCSI data sets between pre-z/OS V1R7 systems and z/OS V1R7 systems.	UO00115

z/OS V1R4 coexistence and fallback PTFs

Install, on z/OS V1R4, the coexistence and fallback PTFs listed in Table 3.

Table 3. Coexistence and fallback PTFs needed on z/OS V1R4 systems

Element or feature, and reason PTFs are needed	z/OS V1R4 PTFs
BCP, Communications Server, RMF™: Allows a z/OS V1R4 system to coexist with a z/OS V1R5 or later system that runs on a **z9-109, z990, or z890 server**. For non-PTF requirements, see item 6 on page 80.	UA01785, UA02025, UA02173, UA02178, UA90002 (if Japanese), UA90003, UQ74992
BCP, SDSF: In z/OS V1R5, a **console enhancement** minimizes the possibility of outages because of exhaustion of system resources used for messaging. The PTFs allow back-level systems to tolerate the enhancement.	BCP PTFs UA05642 and UA06654, SDSF PTF UQ79592
BCP: Prevents the depletion of private storage in the **console address space** on a receiving system when a large number of WTO/R messages are received on that system from other members of a sysplex.	UA07959, UA07962 (if the Consoles Enhancements feature is installed)
BCP: Increased CPU utilization in the **console address space** might be reported on all systems in a sysplex after introducing a z/OS V1R4 system with the z/OS V1R4 Consoles Enhancements feature, or later-level system, into the sysplex. The coexistence PTFs prevent heavy message traffic on the z/OS V1R7 system from impacting the other systems in the sysplex.	UA16509, UA16511 (if the Consoles Enhancements feature is installed)
BCP: A lower-level system in a sysplex can receive messages from a z/OS V1R6 or later system with a **console ID** of 0 and an area ID specified. The coexistence PTFs allow the lower-level receiving system to handle the messages correctly.	UA09332, UA09334 (if the Consoles Enhancements feature is installed)
BCP: Allows a z/OS V1R4 system with the Consoles Enhancement feature installed to correctly handle blank **WTOs** issued to another system.	UA09963
BCP: Produces an informative message when the z/OS V1R4 or earlier version of the **program management binder** is used to try to rebind incompatible program objects created in z/OS V1R5 or later. The PTF detects when the program object level of the V1R5 object is incompatible with back-level capabilities and produces an error message. Without the PTF, there might be a misleading error message or abend.	UA02566

Table 3. Coexistence and fallback PTFs needed on z/OS V1R4 systems (continued)

Element or feature, and reason PTFs are needed	z/OS V1R4 PTFs
BCP: APARs OA05025 (PTF UA07360) and OA05391 together provide corrective service for **XCF** recovery from partial writes to couple data sets. APAR OA05391 introduces a new format for couple data set multi-subrecord check records (MSRCRs), which is required for recovery from partial writes to certain types of couple data set records. APAR OA05025 includes coexistence support that enables systems on which it is installed to interpret the new MSRCR format. Because both APARs have been incorporated into z/OS V1R6 and later, all other systems in the sysplex must be capable of interpreting the new MSRCR format before any V1R6 or later system can be IPLed into the sysplex. V1R5 systems include support for interpreting the new MSRCR format and do not require installation of additional maintenance to provide this capability. You must IPL all other systems in the sysplex with the appropriate PTF for APAR OA05025 (PTF UA07360 for V1R4) before IPLing any V1R6 or later system into the sysplex. Rolling IPLs are sufficient to install the PTFs for APARs OA05025 and OA05391. Note that the recovery provided by these two PTFs is not completely effective until all systems in the sysplex, including z/OS V1R5 systems, have been IPLed with both PTFs or with V1R6 or later.	UA07360 and, if Japanese, UW95504
BCP: z/OS V1R6 has a new 64-bit **global resource serialization** ISGQUERY application programming interface (API). The PTF allows a z/OS V1R4 system to tolerate ISGQUERY requests from a z/OS V1R6 or later system.	UA09225
BCP: Provides compatibility support for the corrected **global resource serialization** ISGLOCK structure rebuild processing in z/OS V1R7 APAR OA11147.	UA18540
BCP: Allows a z/OS V1R4 system to tolerate new resource recovery services (**RRS**) restart function in z/OS V1R6 (and later).	UA09402, UA09424
BCP: Starting in z/OS V1R6, the sysplex couple data set (**CDS**) can be expanded to allow up to 2047 members in a cross-system coupling facility (XCF) group. This is an increase from the previous maximum of 1023 members per XCF group. Formatting a couple data set for more than 1023 members per group creates a Version 4 CDS. The PTF rolls back this function to z/OS V1R4. In terms of coexistence, it provides support for Version 4 sysplex CDSs on z/OS V1R4. This is important because all systems in a sysplex must support Version 4 sysplex CDSs to bring a Version 4 sysplex CDS into use, and once a sysplex is using a Version 4 sysplex CDS, a system that does not support Version 4 sysplex CDSs cannot join the sysplex.	UA09966
BCP: A z/OS V1R7 system cannot join a sysplex of lower-level systems, and a lower-level system cannot join a sysplex of z/OS V1R7 systems, without this PTF.	UA16035, UA16037 (if the Consoles Enhancements feature is installed)

Element or feature, and reason PTFs are needed	z/OS V1R4 PTFs
BCP: z/OS V1R7 introduces the **logger** log stream DUPLEXMODE(DRXRC) specification. If DUPLEXMODE(DRXRC) is specified in a z/OS V1R7 system in a sysplex, and prior releases are running in the same sysplex, the PTF must be installed. If DUPLEXMODE(DRXRC) is not specified, installing the PTF is not required but is nevertheless recommended to avoid any complications if the configuration changes.	UA17177
BCP: Allows a pre-z/OS V1R7 system to use an **IODF** that was created using z/OS V1R7 HCD.	UA17026
BCP: Large format sequential data sets are only supported by z/OS V1R7. The coexistence PTFs cause z/OS to detect the accidental specification of such a data set for stand-alone dump output and to reject its use, as has been done for data set organizations such as PDS.	UA19040, UA19043 (if the z/OS V1R4 z990 Exploitation Support feature is installed)
Communications Server: Allows a z/OS V1R4 system to coexist with a V1R7 system.	UA11849
BCP, DFSMSdfp, DFSMSdss, DFSMShsm, DFSMSrmm: In z/OS V1R6, a new function introduced by PTF UA90124 enables DFSMS software support for IBM TotalStorage Enterprise Tape System **3592** and the media types MEDIA6, MEDIA7, and MEDIA8. Coexistence PTFs listed here allow a V1R4 system to coexist with a V1R6 or later system that uses this function.	UA90083, UA90089, UA90093, UA90098, UA90099
DFSMSdfp: Before z/OS V1R5, a striped, extended-format sequential data set could be allocated with a maximum of 16 stripes, which limited the maximum data set size to 16 volumes. Beginning with z/OS V1R5, an extended-format sequential data set can have a maximum of 59 stripes and, thus, a maximum of 59 volumes. This PTF allows a back-level system to read or write to an extended-format sequential data set with **more than 16 stripes**. However, the back-level system cannot allocate a data set with more than 16 stripes.	UW87192
DFSMSdfp: Allows users on z/OS V1R4 systems to read and write non-VSAM extended format data sets with **more than 16 stripes**. Although such data sets can only be allocated with more than 16 stripes on z/OS V1R5 or later, they can be accessed for read and write on back-level systems.	UA09049
DFSMSdfp: Object Access Method (OAM) now expires object tape volumes and expires tape and optical volumes that belong to object backup storage groups. This function significantly reduces the amount of private storage that the OAM address space uses at larger installations. This PTF enables back-level OAMs to coexist in an **OAMplex** with OAMs at the z/OS V1R5 level.	UW94336
DFSMSdfp: Allows DFSMSdfp to tolerate the support in ICKDSF R17 and DFSMS for reindexing online volumes.	UA03391
DFSMSdfp: z/OS V1R6 has a new PDSE address space, **SMSPDSE1**, which is restartable. The coexistence PTFs allow a z/OS V1R4 system to coexist with a z/OS V1R6 or later system that is exploiting the new address space.	UA09832, UA10775

Table 3. Coexistence and fallback PTFs needed on z/OS V1R4 systems (continued)

Element or feature, and reason PTFs are needed	z/OS V1R4 PTFs
DFSMSdfp: ICKDSF R17 (equivalent to the level in the z/OS V1R4 z990 Compatibility Support feature) removed the requirement to have volumes varied offline to all other OS/390 or z/OS systems sharing the volumes when building indexes or refreshing, extending, or building new VTOCs. However, before implementing this function, you must install these coexistence PTFs on all sharing z/OS V1R4 systems.	UA01753, UA03391, UW95817
DFSMSdfp: Allows a z/OS V1R4 system to tolerate the **64-bit POSIX time support** in z/OS V1R6 and later by converting values to the 32-bit format.	UW85576
DFSMSdfp: An enhancement in the z/OS V1R7 Object Access Method (OAM) component introduces a new valid value ("R") for the object location in the object directory to indicate that the object resides on DB2 disk in recalled status. This PTF enables pre-z/OS V1R7 OAMs to coexist in an **OAMplex** with OAMs at the z/OS V1R7 level.	UA16993
DFSMSdfp: As part of **VSAM extent constraint removal** in z/OS V1R7, these PTFs prevent pre-z/OS V1R7 systems from opening data sets that have more than 255 extents. Also, if a data set is open and a z/OS V1R7 job extends it past 255 extents, the close on the pre-z/OS V1R7 system fails. Finally, these PTFs prevent conversion of a data set having more than 255 extents from being converted by DFSMSdss to a non-SMS managed data set on pre-z/OS V1R7 releases.	UA14882, UA16223, UA16796
DFSMSdfp: z/OS V1R7 supports new QNAME and RNAME parameters for **VSAM RLS**. The coexistence PTFs prevent serialization problems from occurring when the new parameters are used in a global resource serialization complex that includes a pre-z/OS V1R7 system.	UA16633, UA16922, UA17234
DFSMSdfp, DFSMShsm, DFSMSrmm: In z/OS V1R5, the maximum value of the file sequence number for a data set on a tape volume increased from 9999 to 65 535 for IBM standard label (SL) tapes, unlabeled (NL) tapes, and bypass label processing (BLP). This PTF causes a message and abend if a tape data set with **file sequence number greater than 9999** is attempted to be opened on a back-level system.	UW88886
DFSMSdfp, DFSMShsm: In z/OS V1R5, DFSMShsm was enhanced to use volume-level **fast replication** to create backup versions for sets of storage groups. A set of storage groups is defined through an SMS construct termed "copy pool". The coexistence PTFs prevent back-level versions of DFSMShsm from processing target volumes in the copy pool backup storage group. The DFSMShsm recovery of fast replication backups is not available on systems before V1R5. If you must back out of V1R5 to an earlier release, you can use the DFSMSdss COPY command to recover individual volumes.	UA07442, UW95453
DFSMSdfp: z/OS V1R7 supports **large format sequential data sets**. These PTFs cause pre-z/OS V1R7 systems to issue ABEND 213-14 or 213-16 if a program attempts to open data sets that cannot work on those systems.	UA15869, UA16550, UA18494

Element or feature, and reason PTFs are needed	z/OS V1R4 PTFs
DFSMSdss: z/OS V1R7 supports **large format sequential data sets**. These PTFs cause pre-z/OS V1R7 systems to issue ABEND213-14 for any large format dump data sets that are provided as input to RESTORE or COPYDUMP, or output for DUMP and COPYDUMP. If DFSMSdss encounters any large format sequential data sets as input to logical data set COPY, logical and physical data set DUMP and RESTORE, data set print, or logical and physical data set RELEASE, the data set will fail with ADR878E rsn 17.	UA16796
DFSMShsm: z/OS V1R7 supports **large format sequential data sets**. The PTFs cause pre-z/OS V1R7 systems that might potentially recall, recover, or ARECOVER a data set to first verify that the data set is not a large format data set. If it is, an error message is issued describing the reason for the failure.	UA16796, UA16951
DFSMShsm: z/OS V1R7 supports **large format sequential data sets**. In an HSMplex with more than one DFSMShsm host, take care when migrating the journal to a large format sequential data set. All DFSMShsm hosts within an HSMplex must be at z/OS V1R7 before you can migrate the journal to a large format sequential data set. With the PTFs, when a pre-z/OS V1R7 DFSMShsm host attempts to open a journal, if the journal is a standard format data set, DFSMShsm initialization continues. If the journal is a large format data set, message MSGARC0509E with the "LARGE" text in the message is issued and DFSMShsm is stopped. If the journal is a striped data set, message MSGARC0509E with the "STRIPED" text in the message is issued and DFSMShsm is stopped. If the ARCBJRNL utility attempts to use a large format journal data set, it ends with return code RC40, which indicates an OPEN error.	UA15869, UA16550, UA16954, UA18494
DFSMShsm: z/OS V1R6 and later allow multiple secondary space management (SSM) tasks to run concurrently. The PTF allows a z/OS V1R4 system to tolerate this **SSM multitasking**.	UA09618
DFSMShsm: z/OS V1R7 supports fast subsequent migration (**FSM**) of data sets. The PTFs cause DFSMShsm to set the appropriate flags during recall processing so that if the data set is later opened for output by either z/OS V1R7 systems or pre-z/OS V1R7 systems, the flags used for reconnection determination are set appropriately.	UA16849, UA16857, UA16860, UA16944
DFSMShsm: z/OS V1R7 increases the number of data set names supported in a tape table of contents (TTOC). If a system that has the coexistence PTF installed finds that the OCDS RECORDSIZE is 6144 bytes, which indicates that some instances of DFSMShsm in the HSMplex might be using the **extended TTOC**, then tape operations on that level of DFSMShsm are inhibited.	UA16947
DFSMSrmm: Backup at anytime is an enhancement in z/OS V1R5. Coexistence service prevents the failure of inventory management when a backup that uses this enhancement starts on a lower-level system.	UA03299, UA90010, UA90011, UA90012 (if Japanese), UW92622, UW92623 (if Japanese), UW94636, UW95741
Distributed File Service: Allows pre-z/OS V1R7 systems to tolerate new characters (@#$) allowed in z/OS V1R7 for zFS file systems and aggregates.	UA14531

Table 3. Coexistence and fallback PTFs needed on z/OS V1R4 systems (continued)

Element or feature, and reason PTFs are needed	z/OS V1R4 PTFs
Distributed File Service: Allows pre-z/OS V1R7 systems to tolerate the file system structure for z/OS V1R7 zFS file systems.	UA20485
HCD: Provides support for HCD users who share **IODF** data sets between pre-z/OS V1R7 systems and z/OS V1R7 systems.	UA90174 (base and English), UA90175 (Japanese)
ISPF: Allows pre-z/OS V1R7 systems to intelligently display the number of tracks in a large format sequential data set. If the number of tracks is greater than 64 KB, the string ">64K" and a larger explanatory message are written to the panel.	UA19928
ISPF: Provides an appropriate message when a user attempts to open a large format sequential data set from a pre-z/OS V1R7 release.	UA19931, UA19934 (Swiss German), UA19935 (Japanese), UA19936 (German), UA19937 (uppercase English)
JES2: Allows z/OS V1R4 JES2 to run with z/OS V1R7 JES2 in a multi-access spool (**MAS**).	UA03828, UA09500, UA18835, UA20901, UA90160
JES2: Fixes a problem on a receiving z/OS V1R4 node that can occur in a rare situation with a large scheduler work block text unit (SWBTU). Data sets have a large SWBTU when MAILTO, MAILCC, and MAILBCC keywords are used in addition to other keywords on OUTPUT JCL statements. The problem is caused by APAR OA09152 (PTF UA16213 on z/OS V1R4 JES). This is a network-specific problem, not a MAS-specific problem.	UA16216
JES3: Allows z/OS V1R4 JES3 to run with z/OS V1R7 JES3 in a **multisystem complex** and provides fallback support to the back-level JES3.	UA04010, UA07715
Language Environment: Detects attempts to use a **new suboption** on back-level releases that do not support it. This coexistence service is necessary to support downward compatibility for Language Environment.	UQ78072
Language Environment: The `/etc/utmpx` file contains a user accounting database. In z/OS V1R6, the format of the records in the file was extended to support longer remote host names, 64-bit timestamp structures, and a version indicator. The coexistence PTF prevents the standard interfaces in pre-V1R6 releases from accessing `/etc/utmpx` databases that use the new format, avoiding confusion and possible data corruption. Attempts to access a `/etc/utmpx` database in the new format from an earlier release return a null pointer. Applications can use perror() to print the error message.	UQ85891
NFS: Allows a pre-z/OS V1R7 NFS SMF report generator to process an SMF file that includes NFS V1R7 SMF records. Any records containing TCP/IP version 6 IP addresses will be ignored.	UA16682
NFS: Allows a pre-z/OS V1R7 NFS server to read a mount handle data set written by z/OS V1R7 NFS.	UA19506
SMP/E: Allows back-level SMP/E to tolerate enhancements introduced in z/OS V1R5 SMP/E (which is equivalent to SMP/E V3R2).	UR53977, UR54450, UR54453 (if Japanese)

Element or feature, and reason PTFs are needed	z/OS V1R4 PTFs
SMP/E: Provides support for SMP/E users who share SMPCSI data sets between pre-z/OS V1R7 systems and z/OS V1R7 systems.	UO00114

Use SoftCap to identify the effect of capacity changes

Description: The Software Migration Capacity Planning Aid (SoftCap) is a PC-based tool that evaluates the effects of software release migrations. It also helps evaluate the migration from ESA/390 (31-bit) architecture to z/Architecture (64-bit).

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	No, but recommended to help in assessing processor capacity and available resources when migrating to new software levels.
Target system hardware requirements:	This tool runs on your workstation. Requirements are: • A Pentium® III class or faster processor. • An SVGA display 1024 x 768 or better. • Approximately 5 MB of hard disk space for the SoftCap application and user's guide, plus 40 MB for the IBM Java™ 1.4.1 run-time environment.
Target system software requirements:	This tool runs on your workstation. Requirements are: • Windows 2000 or Windows XP. • IBM Java 1.4.1 or later run-time environment. This environment is now available with the tool.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Steps to take:

• Download SoftCap from one of the following Web sites:
  – Customers:
    http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS268
  – Business partners: http://www.ibm.com/partnerworld/sales/systems
• Run SoftCap to determine your expected increase in CPU utilization (if any) and to identify your storage requirements, such as how much storage is needed to IPL.

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

Upgrade Windows 95, 98, and NT clients

Description: z/OS does not support service for client operating systems whose service is withdrawn by the operating system manufacturer. As a result, IBM no longer supports service for clients running Windows 95, Windows 98, or Windows NT® Workstation 4.xx.

Element or feature:	Multiple.
When change was introduced:	13 August 2002 in the z/OS V1R4 availability announcement.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you have clients running Windows 95, Windows 98, or Windows NT Workstation 4.xx.
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: Use a supported follow-on to Windows 95, Windows 98, or Windows NT Workstation 4.xx.

Reference information: For client software supported with z/OS, see *z/OS and z/OS.e Planning for Installation*.

Verify that you have enough XCF groups in your CDS and enough XCF members in your XCF groups

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.

Element or feature:	Multiple.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you have an inadequate number of XCF groups and members formatted in your sysplex couple data sets, and functions that you are using need additional XCF groups or members.
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:

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. In z/OS V1R7, one additional XCF group is used. Its name is IOEZFS and it is used by base element Distributed File Service to provide zFS support. If you do not have enough groups formatted to support this additional XCF group, reformat your sysplex data sets with a larger number of groups.

3. 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 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*.

Migrate from discontinued service delivery options

Description: SMP/E Internet Service Retrieval and ShopzSeries now offer extensive options for service acquisition and delivery. To reduce the number of ordering interfaces and help assure timely delivery of new functions, some older options for service delivery are being simplified or discontinued:

- Effective March 2006, new ESO and CBPDO (5751-CS8 and 5775-MVS) physical delivery subscriptions will not be accepted.

- Effective June 2006, CBPDO product orders will include service only for the products included in the order. Formerly, CBPDO product orders included service for other products licensed under the same customer number within the same SREL. To get service for other products, you can use SMP/E Internet Service Retrieval, ShopzSeries, or a fee service offering.

- Effective June 2006, Service-Only CBPDO (5751-CS3) orders will no longer be accepted. An improved option for ordering service by SREL, or for all licensed products under the same customer number, will continue to be supported in ShopzSeries. You can also get service based on what you have installed using SMP/E Internet Service Retrieval, ShopzSeries, or selected fee offerings. Note that CBPDO product orders are not affected by this change.

- Effective September 2006, existing ESO and CBPDO physical delivery subscriptions will be discontinued. You can use a job scheduling system and SMP/E Internet Service Retrieval to get service at any interval you find convenient, or use the Internet delivery subscription option available in

ShopzSeries. IBM recommends that you begin to use SMP/E Internet Service Retrieval, ShopzSeries, or one of the following worldwide fee offerings prior to the above changes taking effect:

– SoftwareXcel, Resolve (United States)
– Enhanced Technical Support (Europe, Middle East, Africa)
– SupportLine (Asia Pacific, Latin America, Canada)

Element or feature:	All.
When change was introduced:	Discontinuance was announced in the z/OS V1R7 general availability announcement.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	If you use any of the service delivery options in "Description" above, the migration action is either recommended or required, as follows:
	• Before the date that the option is discontinued, the migration action is recommended because it will become a requirement in the future.
	• As of the date of discontinuance, the migration action is required.
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: Follow the recommendations in "Description" above.

Reference information:

• For information about SMP/E Internet Service Retrieval, see *SMP/E User's Guide*.
• For information about ShopzSeries, see http://www.ibm.com/software/shopzseries.

Use SMP/E Internet Service Retrieval or ShopzSeries instead of SUF

Description: The S/390® Service Update Facility (SUF), the Internet-based software service tool for ordering and receiving z/OS, z/OS.e, z/VM, and VSE/ESA software service, is discontinued effective 15 January 2006. Instead, use one of the following:

• *SMP/E Internet Service Retrieval*. This function is new in z/OS V1R7 (and in the SMP/E V3R4 product). It allows you to automate ordering and delivery of PTFs and HOLDDATA, and can help eliminate manual tasks required for ordering and delivery of PTFs using prior methods.
• *ShopzSeries*. This application allows you to order System z9 and zSeries software products and service over the Internet.

Existing electronic worldwide fee services offerings that deliver z/OS software service will continue to provide electronic delivery using:

- SoftwareXcel, Resolve (United States)
- Enhanced Technical Support (Europe, Middle East, Africa)
- SupportLine (Asia Pacific, Latin America, Canada)

Element or feature:	All.
When change was introduced:	Stabilization of SUF was announced on 10 August 2004 in the z/OS V1R6 availability and z/OS V1R7 preview announcement. Discontinuance of SUF was announced on 15 February 2005 in the z/OS V1R7 preview announcement.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	If you use SUF, the migration action is either recommended or required, as follows: • Before 15 January 2006, the migration action is recommended because it will become a requirement on 15 January 2006. • As of 15 January 2006, the migration action is required.
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: Instead of using SUF, use SMP/E Internet Service Retrieval or ShopzSeries. You might prefer SMP/E Internet Service Retrieval because it frees you from the manual steps required by ShopzSeries to create and manage software inventory files (bitmaps), and because you can use existing batch job scheduling services to create a totally automated PTF service delivery process.

Reference information:
- For information about SMP/E Internet Service Retrieval, see *SMP/E User's Guide*.
- For information about ShopzSeries, see http://www.ibm.com/software/shopzseries.

Find alternatives to removed elements and features

Description: A number of base elements and optional features have been, or are planned to be, removed from z/OS. See "When change was introduced" below for their names and releases.

If you are using any of the base elements or optional features that have already been removed, you need to find alternatives. If you are using any of those planned for removal, now might be a good time to start preparing for their removal.

Notes:

1. This topic deals with the removal of entire elements and features. Removal of part of an element or feature (that is, a particular function within an element or feature) is covered in the chapter of the element or feature that supplied the function.

2. Statements about future removals represent IBM's current intentions. IBM development plans are subject to change or withdrawal without further notice.

Element or feature:	Multiple.
When change was introduced:	Future removals (after z/OS V1R7): • msys for Operations (base element) • msys for Setup (base element) Removals made in z/OS V1R6: • DCE Application Support (base element) • Encina® Toolkit Executive (base element) • Text Search (base element) Removals made in z/OS V1R5: • ILM (base element) • C/C++ IBM Open Class® Library (base element) • C/C++ with Debug Tool (optional feature)
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	• For msys for Setup and msys for Operations: No, but recommended if you use these base elements because they are planned to be removed in the future. • For the other base elements and optional features: Yes, if you use any of them because they have already been removed.
Target system hardware requirements:	Dependent upon your replacement usage of the removed elements and features. See "Steps to take" below.
Target system software requirements:	Dependent upon your replacement usage of the removed elements and features. See "Steps to take" below.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Steps to take for msys for Operations: z/OS V1R7 is planned to be the last release to support the msys for Operations base element. IBM intends to remove the msys for Operations base element from the release following z/OS V1R7. IBM plans to transition many of the current msys for Operations functions to a new user interface and infrastructure in a future release of z/OS.

Steps to take for msys for Setup: Support for the following plug-ins for msys for Setup is planned to be removed in the release following z/OS V1R7: TCP/IP Services, z/OS UNIX, Language Environment, Parallel Sysplex, ISPF, and RMF. When this support is withdrawn, you will not be able to use msys for Setup for function enablement, setup, or configuration of these areas of z/OS. The only

remaining plug-in, the DB2 V8 plug-in, is unaffected and remains available for enablement, setup, and configuration of DB2. The TCP/IP plug-in will continue to be available for download from the Web and will no longer require msys for Setup. IBM intends to continue to deliver improvements to help with z/OS setup and configuration in the future.

Steps to take for DCE Application Support: DCE Application Support facilitated the interaction between DCE clients and CICS® or IMS™ regions. With the continued evolution of technology and accompanying changes in the marketplace, there is no need for this support. If similar function is required, IBM recommends that you use IBM WebSphere®. Note that the DCE Base Services element, which provides services for developing and running client/server applications, is planned to continue to ship with z/OS.

Steps to take for Encina Toolkit Executive: Encina Toolkit Executive provided a set of tools for developing client components of distributed transactional applications. Over time, the marketplace has moved to other technologies. This element was an enabler for DCE Application Support. There will be no replacement.

Steps to take for Text Search: Text Search has been removed from the z/OS product but is available as a Web download because the Text Search function is still required by the DB2 UDB Text Extender feature of the following two products: DB2 Universal Database™ for z/OS V8 (5625-DB2), and DB2 Universal Database Server for OS/390 and z/OS V7 (5675-DB2). Therefore, before you use this DB2 feature on z/OS V1R7, download and install the Text Search Web deliverable from the DB2 UDB Text Extender Web site: http://www.ibm.com/software/data/db2/extenders/text/te390/. (This is a different Web site than the one previously used. The previous one was the z/OS downloads Web site.)

Steps to take for ILM: IBM License Manager (ILM), planned for introduction in z/OS V1R1, was intended to be a combination of license management tools that you would use to manage licenses and check compliance with software terms and conditions. However, on 26 November 2002, IBM announced the decision not to deliver ILM. IBM will continue to deliver sub-capacity software pricing benefits using the Sub-Capacity Reporting Tool (SCRT) until a strategic software license management solution is available. For additional information, see the 26 November 2002 announcement through the ILM Web site at http://www.ibm.com/eserver/zseries/zos/ilm/. Also see "Remove customization for ILM" on page 27.

Steps to take for C/C++ IBM Open Class Library: See "Remove your dependency on the C/C++ IBM Open Class Library" on page 320.

Steps to take for C/C++ with Debug Tool: Instead of using this feature, use the following:
- For debugging, use the z/OS optional feature C/C++ without Debug Tool, along with the product Debug Tool for z/OS V4 (5655-L23).
- For all other functions, use the z/OS optional feature C/C++ without Debug Tool. This feature is the same as the C/C++ with Debug Tool feature except that it doesn't have a Debug Tool.

General steps to take: You should stop referencing the data sets that were associated with deleted elements and features. See "Remove references to deleted data sets and paths" on page 40 for migration actions associated with deleted data sets.

Reference information: See the "Steps to take" topics above.

Update the CustomPac Installation Dialog

Description: If this is the first time you will install a ServerPac using the level of the CustomPac Installation Dialog supplied with z/OS V1R6 or later, you must update the dialog before receiving your ServerPac order.

Element or feature:	All.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you use ServerPac to install z/OS and have not yet performed this migration action.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	If you are installing an older order and want to run UPDATE or EUPDATE, use the CPPCINV sample job to convert some of the older order's data sets to VSAM before finishing its installation.
System impacts:	None.

Steps to take: Determine whether you need to update the CustomPac Installation Dialog by starting the dialog and looking at the bottom of the first panel that is displayed (CPPPPOLI) for the text "This dialog supports electronic delivery". Then:

- If the panel contains the text, no migration action is required.
- If the panel does not contain the text, follow the instructions for getting and running the UPDATE or EUPDATE job in *ServerPac: Using the Installation Dialog*.

Reference information: *ServerPac: Using the Installation Dialog*.

Update local panels, CLISTs, and execs that invoke the CustomPac Installation Dialog

Description: If this is the first time you will install a ServerPac using the level of the CustomPac Installation Dialog supplied with z/OS V1R6 or later, you might need to update local panels, CLISTs, and execs used to start it.

Element or feature:	All.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before installing z/OS V1R7.

Is the migration action required?	Yes, if you use ServerPac to install z/OS; use local CLISTs, execs, or panels to invoke the CustomPac Installation Dialog; and have not yet performed this migration action.
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: Determine whether you need to update the CustomPac Installation Dialog by starting the dialog and looking at the bottom of the first panel that is displayed (CPPPPOLI) for the text "This dialog supports electronic delivery". Then:

- If the panel contains the text, no migration action is required.
- If the panel does not contain the text, remove the ISPF4X parameter from the CPPCISPF command in local CLISTs, execs, and panels. For example, change:

```
PROC  1 CPPMHLQ ISPF4X(N)
CONTROL NOMSG NOFLUSH              /* LIST SYMLIST CONLIST
SET COMMAND  = CPPCISPF           /* COMMAND NAME, DO NOT DELETE */
```

to:

```
PROC  1 CPPMHLQ
CONTROL NOMSG NOFLUSH              /* LIST SYMLIST CONLIST
SET COMMAND  = CPPCISPF           /* COMMAND NAME, DO NOT DELETE */
```

Also, if you have added recovery code to a local CLIST or exec to restore a user's PROFILE PREFIX in case of abnormal dialog termination, remove it. The CustomPac Installation Dialog no longer runs with NOPREFIX set.

Reference information: *ServerPac: Using the Installation Dialog*.

Remove customization for ILM

Description: IBM License Manager (ILM) will not be delivered. Accordingly, you should remove any customization that you performed for this base element.

Element or feature:	ILM.
When change was introduced:	ILM was originally intended to be in z/OS V1R1; nondelivery was announced 26 November 2002.
Applies to migration from:	z/OS V1R4.
Timing:	Before installing z/OS V1R7.
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.

Steps to take:

- Install the PTF for APAR OW56271 on your current system. (The PTF is UW94755 for z/OS V1R4.) The PTF makes ILMMODE=NONE the default, and allows you to remove the ILMMODE specification from your IEASYS*xx* parmlib member.
- Update parameters as follows:
  - Remove the ILMLIB parameter from IEASYS*xx* members.
  - Remove the ILMMODE parameter from IEASYS*xx* members.
  - Remove the MOUNT parameters for the ILM unprocessed certificates HFS and the ILM PDM HFS data sets from BPXPRM*xx* parmlib members.
  - Remove the START command for ILMTSRVR from COMMND*xx* parmlib members.
  - Remove reserved port definitions for the license server from the PROFILE member of the TCPPARMS data set.
- Delete the following data sets and files:
  - Delete the ILMLIB data set.
  - Unmount and delete the ILM PDM HFS.
  - Unmount and delete the ILM unprocessed certificates HFS.
  - Delete the Application Agent configuration file, which is /etc/licmgmt/conf/ilmaapp.cfg.
  - Delete the Application Agent environment variable file, which is /etc/licmgmt/conf/ilmaapp.env.
  - Delete the License Server configuration file, which is /etc/licmgmt/conf/ilmasvr.cfg.
  - Delete the License Server environment variable file, which is /etc/licmgmt/conf/ilmasvr.env.
  - Delete the Management Agent configuration file, which is /etc/licmgmt/conf/ilmamgma.cfg and possibly /u/*userid*/ilmamgma.cfg.
  - Delete (RMDIR) the ILM directories for the configuration files.
- Delete the ILM general event and audit trail log stream models.
- Update security system definitions as follows:
  - Delete the ILMADMIN profile from the STARTED class.
  - Delete the user IDs for the Application Agent, License Server, and Management Agent.
  - Delete any groups created for ILM administration (such as LICADM).
  - Delete all profiles in the ILMADMIN class.
  - Deactivate the ILMADMIN class and remove it from the list of RACLISTed classes.
  - Remove the profile for ILMINIT2 in the PROGRAM class.
  - Remove the profile for ILMINICD in the PROGRAM class.
  - Delete the profiles for ILM log streams in the LOGSTRM class.
  - Delete any profiles in the DATASET class created specifically for the ILMLIB data set.
  - Delete any profiles in the DATASET class created specifically for the ILM unprocessed certificates HFS data set.
  - Delete any profiles in the DATASET class created specifically for the ILM PDM HFS data set.

– Delete any other profiles in the DATASET class created specifically for ILM data sets.

Reference information: See the software pricing Web site at http://www.ibm.com/eserver/zseries/wlc_lm/.

Migration actions for everyone before the first IPL of z/OS V1R7

This section describes general migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't 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.

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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:	Ensure that the current IPCS data sets are accessible from a back-level system for debugging a dump. You can ensure this by putting the IPCS data sets on a volume that is shared between your current system and your back-level system.
	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 back-level 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, which are uniquely referenced.
	When using unique aliases, remember that you may have to update the security definition for the unique high-level qualifier used in the catalog.
Restrictions:	None.
System impacts:	None.

Steps to take: Set up an IPCS environment. For guidance, use the documents listed in the "Reference information" below. During setup, ensure that your logon procedure points to the target system's level of IPCS data sets, which are shown in Table 4.

Note: Starting with z/OS V1R7, a new data set, SYS1.SIEAMIGE, has been added. It is a PDSE data set that complements SYS1.MIGLIB. This data set needs to be used along with SYS1.MIGLIB, when necessary, for IPCS.

Table 4. 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. If you use JES3, ensure that this data set corresponds to the level of JES3 that you are running with z/OS V1R7.
IPCSPARM **Note:** This DD name is needed if one of the following is true: • 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 V1R7 parmlib IPCS members. If the copies of BLSCECT and all the other IPCS members are not at z/OS V1R7 level, then IPCS might fail when you attempt to use it.
	SYS1.SHASPARM, if applicable	This is a JES2 data set. If you use JES2, ensure that this data set corresponds to the level of JES2 that you are running with z/OS V1R7.
	SYS1.SIATPARM, if applicable	This is a JES3 data set. If you use JES3, ensure that this data set corresponds to the level of JES3 that you are running with z/OS V1R7.
ISPMLIB	SYS1.SBLSMSG0	
	SYS1.SIATMSG0, if applicable	This is a JES3 data set. If you use JES3, ensure that this data set corresponds to the level of JES3 that you are running with z/OS V1R7.
ISPPLIB	SYS1.SBLSPNL0	
	SYS1.SHASPNL0, if applicable	This is a JES2 data set. If you use JES2, ensure that this data set corresponds to the level of JES2 that you are running with z/OS V1R7.
	SYS1.SIATPNL0, if applicable	This is a JES3 data set. If you use JES3, ensure that this data set corresponds to the level of JES3 that you are running with z/OS V1R7.
ISPSLIB	SYS1.SBLSKEL0	
ISPTLIB	SYS1.SBLSTBL0	

Table 4. IPCS data set requirements for a logon procedure or DD name allocation (continued)

DD name	Data set name	Notes
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	
	SYS1.SIEAMIGE	
	SYS1.SHASMIG, if applicable	This is a JES2 data set. If you use JES2, ensure that this data set corresponds to the level of JES2 that you are running with z/OS V1R7.
	SYS1.SIATMIG, if applicable	This is a JES3 data set. If you use JES3, ensure that this data set corresponds to the level of JES3 that you are running with z/OS V1R7.
SYSEXEC	SYS1.SIATCLI0, if applicable	This is a JES3 data set. If you use JES3, ensure that this data set corresponds to the level of JES3 that you are running with z/OS V1R7.
SYSPROC	SYS1.SBLSCLI0	

Reference information:

- For more information about IPCS, see *z/OS MVS IPCS Customization*.
- For more information about the correct logon procedure updates, see the *z/OS Program Directory*.
- 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*.
- *z/OS Communications Server: IP Diagnosis 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 V1R7 are updated in your parmlib and proclib concatenations.

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

Steps to take:

- For parmlib, add the data set pointed to by the z/OS V1R7 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 don't 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 won't 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* have been placed in the necessary procedure library concatenations and are available to the system.

Reference information: For lists of parmlib and proclib members that are shipped, see *z/OS Program Directory*.

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`:

- Communications Server (IP Services component). See "IP Services: Update /etc configuration files" on page 147.
- Cryptographic Services (PKI Services and System SSL components).
- DCE Base Services.
- Distributed File Service. The SMB server uses `/etc/dfs`.
- IBM HTTP Server.
- Infoprint Server. See "Export the Printer Inventory and copy other files that were customized" on page 226.
- Integrated Security Services (Firewall Technologies, LDAP Server, and Network Authentication Service components).
- Library Server. See "Library Server actions to perform before the first IPL of z/OS V1R7" on page 269.
- Network File System. See "Convert NFS lock data sets from HFS files to VSAM data sets" on page 273.
- z/OS UNIX. See "Update /etc configuration files" on page 327.

The following elements and features use `/var`:

- Cryptographic Services (OCSF component). See "OCSF: Migrate the directory structure" on page 183.
- Infoprint Server. See "Export the Printer Inventory and copy other files that were customized" on page 226.
- 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 or SystemPac®, some files are loaded into `/etc` and `/var` because of the customization performed in ServerPac and SystemPac. 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 V1R7 `/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 V1R7 requirements.

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

Steps to take: Copy files from your old system to the z/OS V1R7 `/etc` and `/var` subdirectories, and then modify the files as necessary to reflect z/OS V1R7 requirements. If you have other files under your existing `/var` directory, then you will have to merge the old and new files under `/var`. The easiest way to do this is to create a clone of your current `/var` HFS 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.
- **pax**: The **-rw** option works like a copy (instead of making or extracting from a single file archive) for directories, symlinks, and files. Consider the **-pe** option for saving the attributes when doing the copy. The **-k** option prevents overwriting of existing files.

To determine what you need to migrate, first compare the ServerPac's `/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 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.

Once you know the directories, symlinks, and files you are missing from your
existing system, there are 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 -rvwk -pe * /Service/ImageX/etc
  ```

  Another example:

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

  The **pax** command is a good choice because it copies all files, directories, and
  symlinks 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
  symlinks 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've 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: None.

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 appropriately.

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

Steps to take: Review the lists of changed and deleted messages at Summary of message changes 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 for greater detail about certain message changes:

- "IP Services: Update automation for SNTP daemon activation" on page 157
- "IP Services: Accommodate Telnet display format for IPv6 and IPCONFIG FORMAT LONG" on page 161
- "SNA Services: Make changes to PPO, SPO, or CLISTs" on page 164
- "SNA Services: Exclude new session failure RSCV messages" on page 166
- "SNA Services: Eliminate messages caused by improved APPN search diagnostics" on page 168
- "SNA Services: Adjust automation for changed RTP PU display responses" on page 168
- "SNA Services: End automation on message EZZ4313I using Enterprise Extender" on page 169
- "SNA Services: Adjust automation for additional SNA session setup messages" on page 174
- "Update automation that handles message ICE000I" on page 208
- "Migrate from IP PrintWay basic mode to extended mode" on page 231
- "LDAP Server: Update automation for return code and reason code changes in z/OS V1R6" on page 240
- "Review automation that handles message $HASP621" on page 247

Reference information: *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
- 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 NUCLST*xx* parmlib member
- Updates to defaults modules to set site defaults differently than the IBM-supplied defaults, such as for the following element and features:

- C/C++ without Debug Tool.
  - DFSORT™.
  - HLASM.
  - Language Environment. Consider using the CEEROPT module, which can be used to specify run-time options for CICS, IMS LRR, and other LRR users. Also consider using the CEEPRM*xx* parmlib member, introduced in z/OS V1R7, to eliminate the assembler language run-time option modules. See "Determine the impact of changes to default run-time options" on page 265 for more information about CEEPRM*xx*.

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

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you've 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.

Steps to take: Use the z/OS SMP/E Planning 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 desired modifications to the z/OS release you are installing.

Reference information:
- For information about XL C/C++ customization, see *z/OS XL C/C++ Compiler and Run-Time Migration Guide for the Application Programmer*.
- 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 Language Environment customization, see *z/OS Language Environment Customization*.

Reconnect non-IBM products

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

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use any ISV products and need to reconnect them after performing a ServerPac or SystemPac installation.
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: 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 or SystemPac.

For those using SystemPac, if the ISV products are selectable in the SystemPac shopping list, configure them such that they are placed on a separate volume and in their own SMP/E zones. You can either (1) place all the selectable ISV products in one SMP/E zone, separate from IBM products, or (2) separate ISV products even further by placing products from different vendors in their own unique zone. Use the Local Order Entry tool during order placement to perform the separation. For details about the tool, refer to:

http://www.ibm.com/ca/custompac/

Reference information:
- For a list of independent software vendors (ISVs) that support z/OS, as well as announcements, testimonials, and other information, see http://www.ibm.com/eserver/zseries/solutions/s390da/.
- 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.

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you will 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.

Steps to take: Ensure that any required coexistence PTFs are installed before using the subsystem with the new z/OS system, as well as any required SVCs, system modifications, parmlib setup, and proclib setup. Follow the instructions for the subsystem that you need to reconnect.

Reference information: Subsystem program directories.

Update operational and other procedures

Description: Depending on which method you used to install (ServerPac, CBPDO, or other 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.

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

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 53.
- 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: For the RACF FACILITY class profiles that were added for z/OS UNIX, see *z/OS UNIX System Services Planning*.

Verify that virtual storage limits are set properly

Description: Virtual storage requirements usually grow from release to release. You should review the virtual storage limits 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.

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

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 zero if it is not specified. However, the system-wide default MEMLIMIT can be overridden by specifying REGION=0 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 the topic about 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:

- For MEMLIMIT, you must specify a nonzero MEMLIMIT in an active SMFPRM*xx* member of parmlib to establish a system default other than zero for available virtual storage above 2 GB. (The default MEMLIMIT is zero.)
- You can specify MEMLIMIT explicitly in JCL to override the system default that was set (or allowed to default) in SMFPRM*xx*.

- You can specify REGION=0 on the job statement in JCL to implicitly set MEMLIMIT to NOLIMIT, which also overrides the system default (from SMFPRM*xx*).
- 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 SMFPRM*xx*.

Reference information: Information about how to evaluate the central storage configuration can be found in the Washington Systems Center white paper *z/OS Performance: Managing Processor Storage in a 64-bit Environment - V1* at http://www.ibm.com/support/techdocs. (Search for "WP100269".)

Back virtual storage with 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.

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

Steps to take: Review real storage concentration indicators by using an RMF report to evaluate if additional real or auxiliary storage is needed:

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

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

Remove references to deleted data sets and paths

Description: Data sets and paths are routinely removed from z/OS because of consolidation of data sets, removal of elements and features, and other reasons. You must determine whether these changes affect your environment.

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

Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

Steps to take: Using Table 5 as a guide, remove references to data sets and paths that no longer exist. Remove the references from the following places:

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

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

*Table 5. Data sets and paths **deleted** from z/OS V1R7, z/OS V1R6, and z/OS V1R5 (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 (and sample deletion job if any)
None	/usr/lib/nls/msg/ En_US/IBM	Target	z/OS UNIX – Application Services	z/OS V1R6	Obsolete
None	/usr/lpp/encina/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/bin/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/etc/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/etc/ IBM/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/ example/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/ example/ecnims/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS

*Table 5. Data sets and paths **deleted** from z/OS V1R7, z/OS V1R6, and z/OS V1R5 (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 (and sample deletion job if any)
None	/usr/lpp/encina/ example/ecnims/ asimso/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/ example/ecnims/ imstran/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/ example/IBM/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/ example/ telshop/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/IBM/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/include/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/include/ admin/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/include/ dceutils/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/include/ ecnims/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/include/ encina	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/include/ IBM/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/include/ sec/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/include/ tc/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/include/ tc/client/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/include/ tc/rpc/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS

Table 5. Data sets and paths **deleted** *from z/OS V1R7, z/OS V1R6, and z/OS V1R5 (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 (and sample deletion job if any)
None	/usr/lpp/encina/include/ threadTid/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/include/ tran/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/include/ trdce/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/include/ trpc/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/include/ tx/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/include/ utils/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/include/ uuid/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/lib/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/lib/IBM/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/lib/nls/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/lib/nls/ msg/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/lib/nls/ msg/En_US.IBM-1047/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/msg/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/msg/C/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/msg/ IBM/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS

*Table 5. Data sets and paths **deleted** from z/OS V1R7, z/OS V1R6, and z/OS V1R5 (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 (and sample deletion job if any)
None	/usr/lpp/encina/msg/Ja_JP/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/msg/Ja_JP/IBM/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/src/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/encina/src/IBM/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
None	/usr/lpp/gskssl/java	Target	Cryptographic Services – System SSL	z/OS V1R6	Obsolete
None	/usr/lpp/gskssl/java/docs	Target	Cryptographic Services – System SSL	z/OS V1R6	Obsolete
None	/usr/lpp/gskssl/java/docs/com	Target	Cryptographic Services – System SSL	z/OS V1R6	Obsolete
None	/usr/lpp/gskssl/java/docs/com/ibm/	Target	Cryptographic Services – System SSL	z/OS V1R6	Obsolete
None	/usr/lpp/gskssl/java/docs/com/ibm/gskssl	Target	Cryptographic Services – System SSL	z/OS V1R6	Obsolete
None	/usr/lpp/gskssl/java/docs/com/ibm/gskssl/class-use	Target	Cryptographic Services – System SSL	z/OS V1R6	Obsolete
None	/usr/lpp/ldap/doc	Target	Integrated Security Services – LDAP Server	z/OS V1R6	Obsolete
None	/usr/lpp/ldap/doc/jndi	Target	Integrated Security Services – LDAP Server	z/OS V1R6	Obsolete
None	/usr/lpp/ldap/doc/jndi/images	Target	Integrated Security Services – LDAP Server	z/OS V1R6	Obsolete
None	/usr/lpp/ldap/examples/jndi	Target	Integrated Security Services – LDAP Server	z/OS V1R6	Obsolete
None	/usr/lpp/TextTools/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/bin/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/data/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/data/locales/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS

*Table 5. Data sets and paths **deleted** from z/OS V1R7, z/OS V1R6, and z/OS V1R5 (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 (and sample deletion job if any)
None	/usr/lpp/TextTools/ dict/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/ include/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/ install/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/lib/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/ NetQ/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/ NetQ/isinq/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/ NetQ/samples/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/nls/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/nls/ C/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/nls/ en_US/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/nls/ En_US/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/ TextSearch/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/ TextSearch/IBM/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/ TextSearch/ivp/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/ TextSearch/ivp/docs/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/ TextSearch/samples/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/lpp/TextTools/ TextSearch/samples/ comwrap/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
None	/usr/man/C/cat8	Target	z/OS UNIX – Application Services	z/OS V1R6	Obsolete
None	/usr/man/C/cat8/IBM	Target	z/OS UNIX – Application Services	z/OS V1R6	Obsolete
AASUACF	ASU.AASUACF	DLIB	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS

*Table 5. Data sets and paths **deleted** from z/OS V1R7, z/OS V1R6, and z/OS V1R5 (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 (and sample deletion job if any)
AASUCIDL	ASU.AASUCIDL	DLIB	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
AASUEXEC	ASU.AASUEXEC	DLIB	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
AASUHDR	ASU.AASUHDR	DLIB	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
AASUHHDR	ASU.AASUHHDR	DLIB	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
AASUHLIB	ASU.AASUHLIB	DLIB	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
AASUHSAM	ASU.AASUHSAM	DLIB	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
AASUIDL	ASU.AASUIDL	DLIB	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
AASULINK	ASU.AASULINK	DLIB	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
AASUMENU	ASU.AASUMENU	DLIB	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
AASUMJPN	ASU.AASUMJPN	DLIB	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
AASUPENU	ASU.AASUPENU	DLIB	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
AASUPJPN	ASU.AASUPJPN	DLIB	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
AASUSAMP	ASU.AASUSAMP	DLIB	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
AASUSTUB	ASU.AASUSTUB	DLIB	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
AASUTLI	ASU.AASUTLI	DLIB	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS

*Table 5. Data sets and paths **deleted** from z/OS V1R7, z/OS V1R6, and z/OS V1R5 (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 (and sample deletion job if any)
ACBCCMP	CBC.ACBCCMP	DLIB	C/C++ without Debug Tool	z/OS V1R7	OS/390 V2R10 C/C++ compiler removed from z/OS
ACBCSR1	CBC.ACBCSR1	DLIB	C/C++ without Debug Tool	z/OS V1R7	OS/390 V2R10 C/C++ compiler removed from z/OS
ACLBOBJ2	CBC.ACLBOBJ2	DLIB	Run-Time Library Extensions	z/OS V1R5	Obsolete
ACLBSR2	CBC.ACLBSR2	DLIB	Run-Time Library Extensions	z/OS V1R5	Obsolete
ACLBSR3	CBC.ACLBSR3	DLIB	Run-Time Library Extensions	z/OS V1R5	Obsolete
ACLBSR4	CBC.ACLBSR4	DLIB	Run-Time Library Extensions	z/OS V1R5	Obsolete
ACLDHFS1	CBC.ACLDHFS1	DLIB	C/C++ IBM Open Class Library	z/OS V1R5	Obsolete
ACLDSR1	CBC.ACLDSR1	DLIB	C/C++ IBM Open Class Library	z/OS V1R5	Obsolete
ACUNREXX	SYS1.ACUNREXX	DLIB	BCP – Unicode	z/OS V1R7	Obsolete
AECNEXP	ECN.AECNEXP	DLIB	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
AECNHETC	ECN.AECNHETC	DLIB	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
AECNHEXP	ECN.AECNHEXP	DLIB	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
AECNHINC	ECN.AECNHINC	DLIB	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
AECNHJPN	ECN.AECNHJPN	DLIB	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
AECNHLBR	ECN.AECNHLBR	DLIB	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
AECNLINK	ECN.AECNLINK	DLIB	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
AEQAMOD2	EQAW.AEQAMOD2	DLIB	C/C++ with Debug Tool	z/OS V1R5	C/C++ with Debug Tool removed from z/OS
AEQASRC2	EQAW.AEQASRC2	DLIB	C/C++ with Debug Tool	z/OS V1R5	C/C++ with Debug Tool removed from z/OS

*Table 5. Data sets and paths **deleted** from z/OS V1R7, z/OS V1R6, and z/OS V1R5 (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 (and sample deletion job if any)
AEUVFEXP	EUVF.AEUVFEXP	DLIB	Integrated Security Services – Network Authentication Service	z/OS V1R6	Data set SYS1.AIEASID is now used for all z/OS side decks
AEUVFHDR	EUVF.AEUVFHDR	DLIB	Integrated Security Services – Network Authentication Service	z/OS V1R6	Data set SYS1.AIEASID is now used for all z/OS side decks
AEUVFLNK	EUVF.AEUVFLNK	DLIB	Integrated Security Services – Network Authentication Service	z/OS V1R6	Shared PDSE SYS1.AIEALNKE is now used
AGLDLNK	GLD.AGLDLNK	DLIB	Integrated Security Services – LDAP Server	z/OS V1R6	Shared PDSE SYS1.AIEALNKE is now used
AGSKLINK	GSK.AGSKLINK	DLIB	Cryptographic Services – System SSL	z/OS V1R6	Shared PDSE SYS1.AIEALNKE is now used
AILMHFS1	ILM.AILMHFS1	DLIB	ILM	z/OS V1R5	ILM removed from z/OS
AILMMODS	ILM.AILMMODS	DLIB	ILM	z/OS V1R5	ILM removed from z/OS
AILMSAMP	ILM.AILMSAMP	DLIB	ILM	z/OS V1R5	ILM removed from z/OS
AIMOHFS1	IMO.AIMOHFS1	DLIB	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
AIMOJCL1	IMO.AIMOJCL1	DLIB	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
AIMOMOD1	IMO.AIMOMOD1	DLIB	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
ANFSLIB	SYS1.ANFSLIB	DLIB	NFS	z/OS V1R7	Replaced by SYS1.ANFSLIBE (GFSDELET deletes data set, GFSDLDDF deletes DDDEF)
AOSD8	SYS1.AOSD8	DLIB	DFSMSdfp	z/OS V1R7	Native ISAM support removed from z/OS
ISAMLPA	SYS1.ISAMLPA	Target	DFSMSdfp	z/OS V1R7	Native ISAM support removed from z/OS
NFSLIB	SYS1.NFSLIB	Target	NFS	z/OS V1R7	Replaced by SYS1.NFSLIBE (GFSDELET deletes data set, GFSDLDDF deletes DDDEF)
SASUACF	ASU.SASUACF	Target	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS

*Table 5. Data sets and paths **deleted** from z/OS V1R7, z/OS V1R6, and z/OS V1R5 (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 (and sample deletion job if any)
SASUCIDL	ASU.SASUCIDL	Target	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
SASUEXEC	ASU.SASUEXEC	Target	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
SASUHDR	ASU.SASUHDR	Target	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
SASUIDL	ASU.SASUIDL	Target	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
SASUMENU	ASU.SASUMENU	Target	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
SASUMJPN	ASU.SASUMJPN	Target	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
SASUPENU	ASU.SASUPENU	Target	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
SASUPJPN	ASU.SASUPJPN	Target	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
SASUSAMP	ASU.SASUSAMP	Target	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
SASUSTUB	ASU.SASUSTUB	Target	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
SASUTLIB	ASU.SASUTLIB	Target	DCE Application Support	z/OS V1R6	DCE Application Support removed from z/OS
SCBCCMP	CBC.SCBCCMP	Target	C/C++ without Debug Tool	z/OS V1R7	OS/390 V2R10 C/C++ compiler removed from z/OS
SCBCIMG	CBC.SCBCIMG	Target	C/C++ without Debug Tool	z/OS V1R7	OS/390 V2R10 C/C++ compiler removed from z/OS
SCBCPNL	CBC.SCBCPNL	Target	C/C++ without Debug Tool	z/OS V1R7	OS/390 V2R10 C/C++ compiler removed from z/OS
SCBCPRC	CBC.SCBCPRC	Target	C/C++ without Debug Tool	z/OS V1R7	OS/390 V2R10 C/C++ compiler removed from z/OS

*Table 5. Data sets and paths **deleted** from z/OS V1R7, z/OS V1R6, and z/OS V1R5 (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 (and sample deletion job if any)
SCBCSKL	CBC.SCBCSKL	Target	C/C++ without Debug Tool	z/OS V1R7	OS/390 V2R10 C/C++ compiler removed from z/OS
SCBCUTL	CBC.SCBCUTL	Target	C/C++ without Debug Tool	z/OS V1R7	OS/390 V2R10 C/C++ compiler removed from z/OS
SCBCDOC	CBC.SCBCDOC	Target	C/C++ without Debug Tool	z/OS V1R7	OS/390 V2R10 C/C++ compiler removed from z/OS
SCBCJCL	CBC.SCBCJCL	Target	C/C++ without Debug Tool	z/OS V1R7	OS/390 V2R10 C/C++ compiler removed from z/OS
SCBCSAM	CBC.SCBCSAM	Target	C/C++ without Debug Tool	z/OS V1R7	OS/390 V2R10 C/C++ compiler removed from z/OS
SCCNIMG	CBC.SCCNIMG	Target	C/C++ without Debug Tool	z/OS V1R6	C/C++ ISPF panels removed from z/OS
SCCNPNL	CBC.SCCNPNL	Target	C/C++ without Debug Tool	z/OS V1R6	C/C++ ISPF panels removed from z/OS
SCCNSKL	CBC.SCCNSKL	Target	C/C++ without Debug Tool	z/OS V1R6	C/C++ ISPF panels removed from z/OS
SCEERTLS	CEE.SCEERTLS	Target	Language Environment	z/OS V1R6	Language Environment no longer uses RTLS
SCLBCPP2	CBC.SCLBCPP2	Target	Run-Time Library Extensions	z/OS V1R5	Obsolete
SCLBHC	CBC.SCLBH.C	Target	Run-Time Library Extensions	z/OS V1R5	Obsolete
SCLBHFS	/usr/lpp/ioclib/include/ IBM	Target	Run-Time Library Extensions	z/OS V1R5	Obsolete
SCLBHI	CBC.SCLBH.INL	Target	Run-Time Library Extensions	z/OS V1R5	Obsolete
SCLBHPP	CBC.SCLBH.HPP	Target	Run-Time Library Extensions	z/OS V1R5	Obsolete
SCLBSHFS	/usr/lpp/ioclib/sample/ IBM	Target	Run-Time Library Extensions	z/OS V1R5	Obsolete
SCLDHFS	/usr/lpp/ioclib/source/ IBM/	Target	C/C++ IBM Open Class Library	z/OS V1R5	C/C++ IBM Open Class Library removed from z/OS
SCLDJCL	CBC.SCLDJCL	Target	C/C++ IBM Open Class Library	z/OS V1R5	C/C++ IBM Open Class Library removed from z/OS
SCUNREXX	SYS1.SCUNREXX	Target	BCP – Unicode	z/OS V1R7	Obsolete
SECNEXP	ECN.SECNEXP	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS

Table 5. Data sets and paths **deleted** *from z/OS V1R7, z/OS V1R6, and z/OS V1R5 (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 (and sample deletion job if any)
SECNHBIN	/usr/lpp/encina/bin/ IBM/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
SECNHETC	/usr/lpp/encina/etc/ IBM/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
SECNHEXP	/usr/lpp/encina/ example/IBM/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
SECNHINC	/usr/lpp/encina/include/ IBM/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
SECNHJPN	/usr/lpp/encina/msg/ Ja_JP/IBM/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
SECNHLBR	/usr/lpp/encina/lib/ IBM/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
SECNHSCR	/usr/lpp/encina/src/ IBM/	Target	Encina Toolkit Executive	z/OS V1R6	Encina Toolkit Executive removed from z/OS
SEQAAUTH	EQAW.SEQAAUTH	Target	C/C++ with Debug Tool	z/OS V1R5	C/C++ with Debug Tool removed from z/OS **Note:** The Debug Tool product still uses this data set.
SEQADUM	EQAW.SEQADUM	Target	C/C++ with Debug Tool	z/OS V1R5	C/C++ with Debug Tool removed from z/OS
SEQAMOD	EQAW.SEQAMOD	Target	C/C++ with Debug Tool	z/OS V1R5	C/C++ with Debug Tool removed from z/OS **Note:** The Debug Tool product still uses this data set.
SEQASAMP	EQAW.SEQASAMP	Target	C/C++ with Debug Tool	z/OS V1R5	C/C++ with Debug Tool removed from z/OS **Note:** The Debug Tool product still uses this data set.
SEUVFEXP	EUVF.SEUVFEXP	Target	Integrated Security Services – Network Authentication Service	z/OS V1R6	Data set SYS1.SIEASID is now used for all z/OS side decks
SEUVFHDR	EUVF.SEUVFHDR	Target	Integrated Security Services – Network Authentication Service	z/OS V1R6	Data set SYS1.SIEASID is now used for all z/OS side decks

*Table 5. Data sets and paths **deleted** from z/OS V1R7, z/OS V1R6, and z/OS V1R5 (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 (and sample deletion job if any)
SEUVFLNK	EUVF.SEUVFLNK	Target	Integrated Security Services – Network Authentication Service	z/OS V1R6	Shared PDSE SYS1.SIEALNKE is now used
SEUVFLPA	EUVF.SEUVFLPA	Target	Integrated Security Services – Network Authentication Service	z/OS V1R6	Shared PDSE SYS1.SIEALNKE is now used
SEZADEFS	TCPIP.SEZADEFS	Target	Communications Server	z/OS V1R5	Obsolete (EZADSCLN deletes data set, EZADDCLN deletes DDDEF)
SGLDLNK	GLD.SGLDLNK	Target	Integrated Security Services – LDAP Server	z/OS V1R6	Shared PDSE SYS1.SIEALNKE is now used
SGSKLOAD	GSK.SGSKLOAD	Target	Cryptographic Services – System SSL	z/OS V1R6	Shared PDSE SYS1.SIEALNKE is now used
SHASLINK	SYS1.SHASLINK	Target	JES2	z/OS V1R7	Replaced by SYS1.SHASLNKE
SILMDSD	ILM.SILMDSD	Target	ILM	z/OS V1R5	ILM removed from z/OS
SILMJPN1	/usr/lpp/licmgmt/man/C/cat1/jpn/IBM	Target	ILM	z/OS V1R5	ILM removed from z/OS
SILMP001	/usr/lpp/licmgmt/bin/IBM	Target	ILM	z/OS V1R5	ILM removed from z/OS
SILMP002	/usr/lpp/licmgmt/conf/IBM	Target	ILM	z/OS V1R5	ILM removed from z/OS
SILMP003	/usr/lpp/licmgmt/lib/IBM	Target	ILM	z/OS V1R5	ILM removed from z/OS
SILMP004	/usr/lpp/licmgmt/lib/nls/msg/C/enu/IBM	Target	ILM	z/OS V1R5	ILM removed from z/OS
SILMP005	/usr/lpp/licmgmt/man/C/cat1/enu/IBM	Target	ILM	z/OS V1R5	ILM removed from z/OS
SILMP006	/usr/lpp/licmgmt/mgmtgui/IBM	Target	ILM	z/OS V1R5	ILM removed from z/OS
SILMP007	/usr/lpp/licmgmt/samples/ivp/IBM	Target	ILM	z/OS V1R5	ILM removed from z/OS
SILMPJPN	/usr/lpp/licmgmt/lib/nls/msg/C/jpn/IBM	Target	ILM	z/OS V1R5	ILM removed from z/OS
SILMSAMP	ILM.SILMSAMP	Target	ILM	z/OS V1R5	ILM removed from z/OS
SIMOHFS1	/usr/lpp/TextTools/TextSearch/IBM/	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS
SIMOJCL1	IMO.SIMOJCL1	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS

Table 5. Data sets and paths **deleted** *from z/OS V1R7, z/OS V1R6, and z/OS V1R5 (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 (and sample deletion job if any)
SIMOMOD1	IMO.SIMOMOD1	Target	Text Search	z/OS V1R6 (see note)	Text Search removed from z/OS

Note: Text Search has been removed from the z/OS product but is available as a Web download because the Text Search function is still required by the DB2 UDB Text Extender feature of the following two products: DB2 Universal Database for z/OS V8 (5625-DB2), and DB2 Universal Database Server for OS/390 and z/OS V7 (5675-DB2). Therefore, before you use this DB2 feature on z/OS V1R7, download and install the Text Search Web deliverable from the DB2 UDB Text Extender Web site: http://www.ibm.com/software/data/db2/extenders/text/te390/.

Reference information: None.

Add references to new data sets and paths

Description: New data sets and paths are routinely added to z/OS, as the result of new elements and features being added to the system as well as other reasons. You must determine whether these additions affect your environment.

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

Steps to take: Using Table 6 on page 54 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
- Any backup and recovery procedures.

Be sure that you don't overlook the following data sets, which are critical to the successful execution of the z/OS components that use them:
- *SYS1.SIEALNKE.* This is a PDSE introduced in z/OS V1R6 for use by multiple elements and features. It provides a common location to store program objects that are eligible for the link list. You should add SYS1.SIEALNKE to the link list.

When SYS1.SIEALNKE is added to the link list, by default it is APF authorized and does not need to be specified on a STEPLIB DD statement.

- *SYS1.SHASLNKE.* This is a PDSE introduced in z/OS V1R7 and used by JES2. It replaces the data set SYS1.SHASLINK. When SYS1.SHASLNKE is added to the link list, by default it is APF authorized and does not need to be specified on a STEPLIB DD statement.
- *SYS1.NFSLIBE.* This is a PDSE introduced in z/OS V1R7 and used by NFS. It replaces the data set SYS1.NFSLIB. Be sure to update your APF list in parmlib with the new name.

Rules: Some of the data sets shipped with z/OS are PDSEs and are most likely in your link list. If one or more are in your link list 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.

*Table 6. Data sets and paths **added** to z/OS V1R7, z/OS V1R6, and z/OS V1R5 (in alphabetic order by DDDEF name)*

DDDEF	Data set name or path (high-level qualifiers are defaults)	DLIB or target	To element or feature	When added	Why added
ABPXXMLS	SYS1.ABPXXMLS	DLIB	BCP	z/OS V1R6	To support XML schema data
ACFZHFS	CFZ.ACFZHFS	DLIB	Common Information Model	z/OS V1R7	For binary code and shell scripts
ACUNIMG	SYS1.ACUNIMG	DLIB	BCP	z/OS V1R6 but rolled back to prior releases by APAR OA04069	Unicode support for DB2 V8
AEDGHFS	SYS1.AEDGHFS	DLIB	DFSMSrmm	z/OS V1R7	To contain any elements that must reside in the UNIX file system, such as Java classes and EAR files
AGIMBIN	GIM.AGIMBIN	DLIB	SMP/E	z/OS V1R7	To contain elements supplied by SMP/E that reside in the UNIX file system
AIEAHDRV	SYS1.AIEAHDRV	DLIB	BCP	z/OS V1R6	For use by multiple elements and features for header files
AIEALNKE	SYS1.AIEALNKE	DLIB	BCP	z/OS V1R6	For use by multiple elements and features that require a PDSE data set in the link list

*Table 6. Data sets and paths **added** to z/OS V1R7, z/OS V1R6, and z/OS V1R5 (in alphabetic order by DDDEF name) (continued)*

DDDEF	Data set name or path (high-level qualifiers are defaults)	DLIB or target	To element or feature	When added	Why added
AIEAMIGE	SYS1.AIEAMIGE	DLIB	BCP	z/OS V1R7	For use by mutliple elements and features that require a PDSE data set in the link list for migration purposes (similar to SYS1.AMIGLIB)
AIEASID	SYS1.AIEASID	DLIB	BCP	z/OS V1R6	For use by multiple elements and features for side decks
AINGJMSG	ING.AINGJMSG	DLIB	msys for Operations	z/OS V1R6	For System Automation Japanese messages
AINGJPNL	ING.AINGJPNL	DLIB	msys for Operations	z/OS V1R6	For System Automation Japanse command, message, and panel help
ANFSLIBE	SYS1.ANFSLIBE	DLIB	NFS	z/OS V1R7	Replaces SYS1.ANFSLIB
NFSLIBE	SYS1.NFSLIBE	Target	NFS	z/OS V1R7	Replaces SYS1.NFSLIB
SAOPICHE	/usr/lpp/Printsrv/ InfoprintCentral/help/ En_US/IBM/	Target	Infoprint Server	z/OS V1R5	For the Infoprint Central component of Infoprint Server
SAOPICHJ	/usr/lpp/Printsrv/ InfoprintCentral/help/ Ja_JP/IBM/	Target	Infoprint Server	z/OS V1R5	For the Infoprint Central component of Infoprint Server
SAOPICIM	/usr/lpp/Printsrv/ InfoprintCentral/ Images/IBM/	Target	Infoprint Server	z/OS V1R5	For the Infoprint Central component of Infoprint Server
SAOPICSC	/usr/lpp/Printsrv/ InfoprintCentral/ Scripts/IBM/	Target	Infoprint Server	z/OS V1R5	For the Infoprint Central component of Infoprint Server
SAOPICTE	/usr/lpp/Printsrv/ InfoprintCentral/html/ En_US/IBM/	Target	Infoprint Server	z/OS V1R5	For the Infoprint Central component of Infoprint Server
SAOPICTJ	/usr/lpp/Printsrv/ InfoprintCentral/html/ Ja_JP/IBM/	Target	Infoprint Server	z/OS V1R5	For the Infoprint Central component of Infoprint Server
SAOPICXC	/usr/lpp/Printsrv/ InfoprintCentral/xsl/ Controls/IBM/	Target	Infoprint Server	z/OS V1R5	For the Infoprint Central component of Infoprint Server
SAOPICXE	/usr/lpp/Printsrv/ InfoprintCentral/xml/ En_US/IBM/	Target	Infoprint Server	z/OS V1R5	For the Infoprint Central component of Infoprint Server
SAOPICXJ	/usr/lpp/Printsrv/ InfoprintCentral/xml/ Ja_JP/IBM/	Target	Infoprint Server	z/OS V1R5	For the Infoprint Central component of Infoprint Server

*Table 6. Data sets and paths **added** to z/OS V1R7, z/OS V1R6, and z/OS V1R5 (in alphabetic order by DDDEF name) (continued)*

DDDEF	Data set name or path (high-level qualifiers are defaults)	DLIB or target	To element or feature	When added	Why added
SAOPICXM	/usr/lpp/Printsrv/ InfoprintCentral/xml/ IBM/	Target	Infoprint Server	z/OS V1R5	For the Infoprint Central component of Infoprint Server
SAOPICXP	/usr/lpp/Printsrv/ InfoprintCentral/xsl/ Page/IBM/	Target	Infoprint Server	z/OS V1R5	For the Infoprint Central component of Infoprint Server
SAOPICXS	/usr/lpp/Printsrv/ InfoprintCentral/xsl/ IBM/	Target	Infoprint Server	z/OS V1R5	For the Infoprint Central component of Infoprint Server
SBPXXMLS	/usr/lib/xml_schema/ IBM	Target	z/OS UNIX	z/OS V1R6	To support XML schema data
SCCNOBJ	CBC.SCCNOBJ	Target	C/C++ without Debug Tool	z/OS V1R5	To support profile-directed feedback (PDF)
SCFZHFS	/usr/lpp/wbem/IBM/	Target	Common Information Model	z/OS V1R7	For binary code and shell scripts
SCLBHFS1	/usr/lpp/cbclib/IBM/	Target	Run-Time Library Extensions	z/OS V1R5	To support Run-Time Library Extensions in an HFS
SCUNIMG	SYS1.SCUNIMG	Target	BCP	z/OS V1R6 but rolled back to prior releases by APAR OA04069	Unicode support for DB2 V8
SGIMDIR	/usr/lpp/smp/IBM	Target	SMP/E	z/OS V1R7	To contain Java application classes that reside in the UNIX file system
SEDGHFS	/usr/lpp/dfsms/ rmm/IBM/	Target	DFSMSrmm	z/OS V1R7	To contain any elements that must reside in the UNIX file system, such as Java classes and EAR files
SEPHCASE	/usr/lpp/booksrv/ cases/IBM/	Target	Library Server	z/OS V1R5	To hold samples for extended shelf support
SEPHSHLF	/usr/lpp/booksrv/ shelves/IBM/	Target	Library Server	z/OS V1R5	To hold samples for extended shelf support
SEPHSRVR	/usr/lpp/booksrv/public/ bookmgr/libraryserver/ IBM/	Target	Library Server	z/OS V1R5	To support library center creation
SEPHTPLT	/usr/lpp/booksrv/public/ bookmgr/templates/ IBM/	Target	Library Server	z/OS V1R5	To support library center creation
SFOMJ64R	/usr/lib/java_runtime64/ IBM	Target	z/OS UNIX	z/OS V1R6	Java 64-bit run-time support

*Table 6. Data sets and paths **added** to z/OS V1R7, z/OS V1R6, and z/OS V1R5 (in alphabetic order by DDDEF name) (continued)*

DDDEF	Data set name or path (high-level qualifiers are defaults)	DLIB or target	To element or feature	When added	Why added
SFOMJVCL	/usr/include/ java_classes/IBM/	Target	z/OS UNIX	z/OS V1R5	Future Java support
SFOMJVRT	/usr/lib/java_runtime/ IBM/	Target	z/OS UNIX	z/OS V1R5	Future Java support
SHASLNKE	SYS1.SHASLNKE	Target	JES2	z/OS V1R7	Replaces SYS1.SHASLINK
SIEAHDRV	SYS1.SIEAHDRV.H	Target	BCP	z/OS V1R6	For use by multiple elements for header files
SIEALNKE	SYS1.SIEALNKE	Target	BCP	z/OS V1R6	For use by multiple elements and features that require a PDSE data set in the link list
SIEAMIGE	SYS1.SIEAMIGE	Target	BCP	z/OS V1R7	For use by mutliple elements and features that require a PDSE data set in the link list for migration purposes (similar to SYS1.MIGLIB)
SIEASID	SYS1.SIEASID	Target	BCP	z/OS V1R6	For use by multiple elements and features for side decks
SINGJMSG	ING.SINGJMSG	Target	msys for Operations	z/OS V1R6	For System Automation Japanese messages
SINGJPNL	ING.SINGJPNL	Target	msys for Operations	z/OS V1R6	For System Automation Japanse command, message, and panel help

Reference information: None.

Don't try to order z/OS source code

Description: Before z/OS V1R7, source code was available for the following base elements and optional features: BCP (both English and Japanese), BDT base, BDT SNA NJE, BDT File-to-File, DFSMS, MICR/OCR, and Security Server (RACF). The source code was available as optional media features at no additional charge.

As of z/OS V1R7, source code is not offered for any z/OS base element or optional feature.

Element or feature:	Multiple.
When change was introduced:	10 August 2004 in the z/OS V1R6 availability and z/OS V1R7 preview announcement.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.

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.

Steps to take: Don't try to order z/OS source code.

Reference information: None.

Accommodate new address spaces

Description: The following address spaces are new:

- *DEVMAN:* This DFSMSdfp address space is new in z/OS V1R7. z/OS uses this device manager address space to provide various kinds of device support. In z/OS V1R7, this support includes component trace information for DADSM creation and CVAF events. These new component trace records are formatted when viewed by IPCS using CTRACE COMP(SYSDMO). Component tracing for DADSM creation and CVAF events are activated and deactivated by DEVMAN modify commands.

  The CVAF trace events to GTF formerly provided by the CVAFTR procedure have been removed. The debug/trap options of CVAFTR, however, are still available.

- *HZSPROC:* This address space, new in z/OS V1R7, is for the IBM Health Checker for z/OS. The IBM Health Checker for z/OS can help you identify potential problems before they impact your system availability or cause outages. It checks the current active z/OS and sysplex settings and definitions for a system and compares the values to those suggested by IBM or defined by you. The open architecture of the framework supports checks written by IBM, ISVs, and users.

- *JES2 NJE over TCP/IP:* As of z/OS V1R7 JES2, NJE over TCP/IP runs in a new address space. The address space is responsible for sending data to, and receiving data from, TCP/IP. This move of processing from the JES2 main task to the user environment is designed to improve reliability, availability, and serviceability by isolating the moved function from processing in the JES2 main task, and to improve performance by taking advantage of multiple CPUs to do the work (so that not all work is done under the single JES2 main task).

  One address space is created for each active JES2 NETSERV. The format of the name of the address space is *jjjj*S*nnn*, where *jjjj* is the owning JES2 subsystem name and *nnn* is the subscript of the owning NETSERV. For example, for NETSERV(1) owned by subsystem JES2, the name would be JES2S001.

- *SMSPDSE1:* This DFSMSdfp address space was new in z/OS V1R6. It is a restartable PDSE address space that allows you to recover from a PDSE problem (hang, deadlock, or out-of-storage condition) without having to re-IPL the system or sysplex, and to determine which systems require a re-IPL or repair to eliminate PDSE hangs and failures.

  SMSPDSE1 is related to SMSPDSE. SMSPDSE is a nonrestartable address space for PDSEs that are in the link list concatenation. SMSPDSE was introduced in z/OS V1R4 through the service stream (and rolled back to prior releases) to relieve extended common service area (ECSA) usage. SMSPDSE

cannot be restarted because global connections cannot handle the interruption and reconnection that are part of an address space restart. SMSPDSE is the only PDSE address space for z/OS systems when the following conditions exist:

– The IGDSMS*xx* initialization parameter, PDSESHARING, is set to NORMAL.
– The IGDSMS*xx* initialization parameters in a sysplex coupled systems environment are set as follows:
  - PDSESHARING(EXTENDED)
  - PDSE_RESTARTABLE_AS(NO)

If these conditions do not apply, the z/OS system has both the SMSPDSE and SMSPDSE1 address spaces. The SMSPDSE1 address space provides connections to, and processes requests for, PDSE data sets that are not part of the link list concatenation.

• *TN3270E Telnet server:* This Communications Server address space was new in z/OS V1R6. It allows the TN3270E server to run in a separate address space from the TCP/IP stack address space. For details, see "IP Services: Run the TN3270E Telnet server as a separate address space" on page 176.

Element or feature:	• BCP (for HZSPROC) • Communications Server (for TN3270E Telnet server) • DFSMSdfp (for DEVMAN and SMSPDSE1) • JES2 (for JES2 NJE over TCP/IP)
When change was introduced:	• z/OS V1R7 (for DEVMAN, HZSPROC, and JES2 NJE over TCP/IP) • z/OS V1R6 (for SMSPDSE1 and TN3270E Telnet server) Note that HZSPROC was also rolled back to z/OS V1R6, z/OS V1R5, and z/OS V1R4 in the IBM Health Checker for z/OS Web deliverable.
Applies to migration from:	• z/OS V1R6 (for DEVMAN, HZSPROC, and JES2 NJE over TCP/IP) • z/OS V1R5 (for DEVMAN, HZSPROC, JES2 NJE over TCP/IP, SMSPDSE1, and TN3270E Telnet server) • z/OS V1R4 (for DEVMAN, HZSPROC, JES2 NJE over TCP/IP, SMSPDSE1, and TN3270E Telnet server)
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use the CVAFTR procedure. If you don't use it, the migration action is not required but is recommended so that you take advantage of the benefits afforded by the new address spaces.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	SMSPDSE1 requires coexistence PTFs. See "Install coexistence and fallback PTFs" on page 4.
Restrictions:	None.
System impacts:	None.

Steps to take:

- *For DEVMAN:* Instead of using the CVAFTR procedure to collect CVAF trace events, use component tracing techniques provided in DEVMAN. CVAF trace events to GTF by device (CVGTF01 responses for Sxxx, Pxxx) are no longer supported.

  The DEVMAN address space is started by default. However, on address space errors, it terminates and is not restarted automatically. You can use the DEVMAN procedure to restart the address space in this case.

- *HZSPROC:* If you plan to use the IBM Health Checker for z/OS, you must complete its setup, which is started but not completed as part of installation with ServerPac. For example, if you plan to use a coupling facility log stream or want to provide user-supplied overrides in the HZSPRM*xx* parmlib member, there are tasks for you to perform. See "Migrate to, or start using, the IBM Health Checker for z/OS" on page 103.

  The default ServerPac configuration provides the setup and starts the HZSPROC address space. If you do not want to start this address space, update the ServerPac-generated jobs and supplied samples accordingly.

- *For JES2 NJE over TCP/IP:* This address space is started and stopped using the $S NETSERV and $P NETSERV JES2 commands. No special definitions are required. However, if desired, the characteristics of the TCP/IP connection associated with the address space can be altered in the TCP/IP profile data set.

- *For SMSPDSE1:* Create this restartable PDSE address space if you are concerned with system outages that are caused by PDSE problems. By enabling the SMSPDSE1 address space, you can perform an operator-initiated SMSPDSE1 address space restart if there is a PDSE problem where all other means of recovery are not successful. (Until the introduction of SMSPDSE1, a PDSE hang or other PDSE problem would result in an unscheduled system outage caused by an IPL.)

  By default, the new SMSPDSE1 address space is not created during the IPL process. SMSPDSE1 is created during IPL in a sysplex coupled systems environment when the IGDSMS*xx* initialization parameters are set as follows:
  - PDSESHARING(EXTENDED)
  - PDSE_RESTARTABLE_AS(YES)

- *For TN3270E Telnet server:* This address space is not started by default. For instructions on setting it up, see "IP Services: Run the TN3270E Telnet server as a separate address space" on page 176.

Reference information:

- For details about DEVMAN modify commands, traced events, and their formats, see *z/OS DFSMSdfp Diagnosis*.

- To understand the jobs and procedures that need to be completed for the IBM Health Checker for z/OS, see *ServerPac: Installing Your Order*. For information about completing the setup tasks, see *IBM Health Checker for z/OS: User's Guide*.

- For details about the NJE over TCP/IP address space, see *z/OS JES2 Initialization and Tuning Guide*.

- For details about the SMSPDSE1 address space, see *z/OS DFSMSdfp Diagnosis*, *z/OS DFSMS Implementing System-Managed Storage*, and *z/OS DFSMSdfp Storage Administration Reference*.

Accommodate new SCOPE=COMMON data spaces

Description: The MAXCAD parameter specifies the maximum number of SCOPE=COMMON data spaces to be allowed during an IPL. Since z/OS V1R4, several new SCOPE=COMMON data spaces have been added. They are:

- Added in z/OS V1R7:
  - One data space for JES2, named *xxxx*WTO, where *xxxx* is the JES2 name. For example: JES2WTO.
  - One or more data spaces for XES connections to serialized structures. For details, see "Check the maximum number of XES connectors per address space" on page 114.
- Added in z/OS V1R4 by the Consoles Enhancements feature: three data spaces for this feature
- Added in z/OS V1R4 by the z/OS V1R4 z990 Exploitation Support feature: one data space for z990 support

Your MAXCAD setting must be adequate to accommodate these new data spaces.

Element or feature:	BCP and JES2.
When change was introduced:	z/OS V1R7, z/OS V1R4 with the Consoles Enhancements feature, and z/OS V1R4 with the z/OS V1R4 z990 Exploitation Support feature
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use the MAXCAD parameter of parmlib member IEASYS*xx* and the value specified is inadequate for your z/OS V1R7 system.
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: Increase the limit for the number of SCOPE=COMMON data spaces defined on the MAXCAD parameter if your specification is not adequate to cover the new data spaces that have been added. Note that in z/OS V1R6, the MAXCAD default was increased from 25 to 50. If this default is acceptable for your environment, you might want to remove your MAXCAD specification and allow it to default.

Tip: The IBM Health Checker for z/OS can help you determine what to specify for the MAXCAD value. Use the check IBMRSM,RSM_MAXCADS. This check is available in z/OS V1R7 and also in APAR OA09366 back to z/OS V1R4. By running this check, you can find out:

- The MAXCAD value you specified during IPL
- The number of SCOPE=COMMON data spaces currently in use
- The high water mark, which is the highest usage of SCOPE=COMMON data spaces used during this IPL

| Use this information to help you set your MAXCAD specification in IEASYS*xx*.

| **Reference information:**
| • For details about coding parmlib parameters, including MAXCAD, see *z/OS MVS*
| *Initialization and Tuning Reference*.
| • For more information about the additional data spaces required for serialized
| coupling facility structures, see "Check the maximum number of XES connectors
| per address space" on page 114.

Migrate to z/Architecture

Description: z/Architecture is the 64-bit architecture provided by the IBM System
z9 109 (z9-109) server and the IBM @server zSeries servers (z990, z890, z900,
| and z800). With z/OS IPLed in z/Architecture mode on a z9-109 or zSeries server,
you can take advantage of functions such as 64-bit real and virtual storage support,
Intelligent Resource Director (IRD), and HiperSockets™.

If you are migrating from an IBM S/390 Parallel Enterprise Server™ – Generation 5
(G5) or Generation 6 (G6), or from an IBM S/390 Multiprise® 3000 Enterprise
| Server, to the z9-109 server or one of the zSeries servers, you need to migrate to
| z/Architecture. z/OS V1R7 on a z9-109 or zSeries server does not support ESA/390
architecture. (See Table 7.)

Table 7. Architecture modes supported by z/OS releases and servers

	Architecture mode supported by G5, G6, and Multiprise 3000 servers	Architecture mode supported by z9-109 and zSeries servers
z/OS V1R4	ESA/390	z/Architecture and ESA/390 (but ESA/390 mode is only for six months and requires the z/OS V1R2/3/4 Bimodal Migration Accommodation installed)
z/OS V1R5	ESA/390	z/Architecture
z/OS V1R6 and z/OS V1R7	z/OS V1R6 and z/OS V1R7 do not run on the G5, G6, and Multiprise 3000 servers.	z/Architecture

Element or feature:	Multiple.
When change was introduced:	OS/390 V2R10 introduced z/Architecture support (initially on the z900 server and later on the other zSeries servers and the z9-109 server). z/OS V1R6 introduced an architectural level set, whereby z/Architecture became required.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have not yet migrated to z/Architecture.
Target system hardware requirements:	A z9-109 or zSeries server.
Target system software requirements:	z/OS V1R7.
Other system (coexistence or fallback) requirements:	Install the PTFs in "Install coexistence and fallback PTFs" on page 4 if they are not already installed.

Restrictions:	See the "Steps to take" below.
System impacts:	See the "Steps to take" below.

Steps to take: *First (of three), decide whether to migrate software first or hardware first:*

- *If migrating from z/OS V1R5* on a G5, G6, or Multiprise 3000 server to z/OS V1R7 on a z9-109 or zSeries server:
  - You must migrate your hardware first (to z9-109 or zSeries), then your software (z/OS V1R5 to z/OS V1R7). The hardware change must be done first because z/OS V1R7 does not IPL on a G5, G6, or Multiprise 3000 server. You cannot avoid the concurrent change of hardware and architecture (from ESA/390 to z/Architecture) because the z/OS V1R2/3/4 Bimodal Migration Accommodation is not available on z/OS V1R5. Thus, you will have two concurrent changes to verify: the hardware upgrade and the change from ESA/390 mode to z/Architecture mode.

- *If migrating from z/OS V1R4* on a G5, G6, or Multiprise 3000 server to z/OS V1R7 on a z9-109 or zSeries server, you should migrate your hardware first, then your software:
  1. Download and install the z/OS V1R2/3/4 Bimodal Migration Accommodation (explained below) on your old system. Your old system will still run in ESA/390 (31-bit) mode.
  2. Make sure that you have the correct support for the z9-109 or zSeries server installed. Minimally, you need the z/OS V1R4 z990 Compatibility Support feature for running on a z9-109, z990, or z890 server. Make sure that you have any necessary PTFs installed by referring to the appropriate PSP bucket for your server.
  3. Upgrade to a z9-109 or zSeries server. When you IPL your old system (z/OS V1R4) on the new server, your system will still run in ESA/390 mode if you specify ARCHLVL 1 in parmlib member LOAD*xx*.
  4. Migrate to z/Architecture mode, first by specifying ARCHLVL 2, then by removing ARCHLVL and allowing it to default.
  5. Install z/OS V1R7 using ServerPac, CBPDO, or SystemPac. When you IPL z/OS V1R7, your system will come up in z/Architecture (64-bit) mode.

Second (of three), if migrating from z/OS V1R4, understand the z/OS V1R2/3/4 Bimodal Migration Accommodation. The accommodation is software that can assist you in the transition from ESA/390 architecture to z/Architecture by providing a fallback capability. For example, if you encounter problems after migrating to z/Architecture with z/OS on a z9-109 or zSeries server, you can fall back to z/OS in ESA/390 mode on the z9-109 or zSeries server (while you are within the terms of the accommodation). Without the accommodation, z/Architecture mode is the only mode possible when running z/OS on a z9-109 or zSeries server.

The z/OS V1R2/3/4 Bimodal Migration Accommodation software is available for six months for each z/OS license starting from the registration of a z/OS license to a z/Architecture-capable server. It runs on z/OS V1R4. There is no additional charge for it. You can get the accommodation only from the z/OS downloads Web page:

`http://www.ibm.com/eserver/zseries/zos/downloads/`

When you use the z/OS V1R2/3/4 Bimodal Migration Accommodation to run z/OS in ESA/390 mode on a z/Architecture (z9-109 or zSeries) server, functions that require z/Architecture are not supported, such as:

- Intelligent Resource Director (IRD)
- HiperSockets
- 64-bit real storage
- 64-bit virtual storage
- IPv6

Entry Workload License Charges is not available for z890 and z800 servers when running z/OS in ESA/390 mode.

To use the z/OS V1R2/3/4 Bimodal Migration Accommodation after you download and install it, specify a value of 1 on the ARCHLVL parameter of parmlib member LOAD*xx* before you re-IPL. This will bring up z/OS in ESA/390 mode on your z9-109 or zSeries server. For example:

```
IODF     01 SYS0   TEST01
ARCHLVL  1
NUCLEUS  1
NUCLST   00
SYSCAT   MCATDS123SYS1..MCAT                              RES01
IEASYM   (01,L)
INITSQA  0064K
SYSPARM  01
```

Third (of three), use the following checklist as a guide to the changes you have to make to migrate to z/Architecture:

__ 1. Decide how many servers and LPARs you need. Support for 64-bit real storage might allow you to consolidate your current systems into fewer LPARs or to a single native image.

__ 2. Determine whether any locally-developed code is affected by z/Architecture. For information about 64-bit virtual addressing support, see:
   - *z/OS MVS Programming: Assembler Services Reference ABE-HSP*
   - *z/OS MVS Programming: Assembler Services Reference IAR-XCT*
   - *z/OS MVS Programming: Authorized Assembler Services Reference ALE-DYN*
   - *z/OS MVS Programming: Authorized Assembler Services Reference ENF-IXG*
   - *z/OS MVS Programming: Authorized Assembler Services Reference LLA-SDU*
   - *z/OS MVS Programming: Authorized Assembler Services Reference SET-WTO*

__ 3. Check with your ISVs to ensure that they support z/Architecture. See http://www.ibm.com/eserver/zseries/zos/software/isv14.html.

__ 4. Check the server PSP buckets for any service needed for 64-bit addressing (or other hardware-related functions):
   - For the z9-109, the upgrade is 2094DEVICE and the subset is 2094/ZOS.
   - For the z990, the upgrade is 2084DEVICE and the subset is 2084/ZOS.
   - For the z890, the upgrade is 2086DEVICE and the subset is 2086/ZOS.
   - For the z900, the upgrade is 2064DEVICE and the subset is 2064/ZOS.
   - For the z800, the upgrade is 2066DEVICE and the subset is 2066/ZOS.

__ 5. Install real storage manager (RSM) service: PTFs for APARs OW55209, OW55255 (and companion OW56071), OW54938, and OW55729 (and companion OW55902).

   Note: It is important to read the APAR cover letters and apply circumventions as appropriate. For example, the circumvention for

OW55729 and OW55902, which is documented in OW55729, recommends that you set the IEAOPT*xx* MCCAFCTH thresholds based on the amount of central storage on your system. Once you have the fixes for OW55729 and OW55902 installed, it is recommended that you use the default MCCAFCTH thresholds (and remove the circumvention), and remove the MCCAFCTH statement from IEAOPT*xx* altogether.

__ 6. Plan for additional resources for stand-alone dump. In z/Architecture, all of central storage is dumped rather than just the 2 GB of central storage in an ESA/390 system. In order to support this much larger requirement, review the use of multivolume stand-alone dump data set support, which was provided in z/OS V1R2. Refer to *z/OS MVS Diagnosis: Tools and Service Aids.* Also review Washington Systems Center flash 10143 at http://www.ibm.com/support/techdocs. (Search for "flash10143".)

__ 7. When you're ready to switch to z/Architecture, reconfigure the LPAR to use only real storage (formerly called central storage) rather than central and expanded storage by shutting down the system, deactivating and then activating the LPAR to pick up the new storage allocation, and then IPLing the system. (LPARs in basic mode require a power-on reset.) If you run in z/Architecture mode and still have expanded storage defined, the expanded storage is not used and the system issues these messages:

- `IAR016I THE SYSTEM WAS IPLED IN ESAME MODE WITH EXPANDED STORAGE DEFINED. THIS STORAGE WILL NOT BE USED BY THE SYSTEM.`

- `IEE038E AMOUNT OF EXPANDED STORAGE EXCEEDS 0G MAXIMUM.  EXPANDED STORAGE IN EXCESS OF MAXIMUM IS IGNORED.  RECONFIGURATION FUNCTIONS ARE NOT AVAILABLE.` This is followed by the WTOR `IEE039A REPLY TO ACKNOWLEDGE MESSAGE IEE038E.`

Any expanded storage you have defined for z/Architecture mode is allocated to the partition and, even though it isn't used, is unavailable to other partitions.

Fallback note: ESA/390 mode can still be IPLed successfully in an LPAR defined with greater than 2 GB real storage. However, only the first 2 GB of real storage is used, the system issues the following two messages, and the storage is unavailable to other partitions:

- `IAR015I THE SYSTEM WAS IPLED IN ESA/390 MODE WITH MORE THAN 2 GIGABYTES OF CENTRAL STORAGE`

- `IEE020E AMOUNT OF CENTRAL STORAGE EXCEEDS 2G MAXIMUM.  CENTRAL STORAGE IN EXCESS OF MAXIMUM IS IGNORED.` This is followed by the WTOR `IEE021A REPLY TO ACKNOWLEDGE MESSAGE IEE020E.`

The preferred fallback method is to reconfigure the LPAR to use central and expanded storage as desired, shut down the system, deactivate and then activate the LPAR to pick up the new storage allocation, and then IPL the system.

System services that used expanded storage in ESA/390 mode (such as hiperspaces) have been changed to use real storage in z/Architecture mode. Programs that use these system services should not require any changes.

The amount of central storage you should need is the sum of your current central and expanded storage. No additional processor storage is required by z/Architecture itself. You should need more storage only if your workloads grow.

Slightly more real storage might be required to IPL in 64-bit mode. Use the SoftCap tool to help you determine how much. See "Use SoftCap to identify the effect of capacity changes" on page 19.

___ 8. Understand how to evaluate an all central storage environment. See Washington Systems Center white paper WP100269 at http://www.ibm.com/support/techdocs.

___ 9. Understand Load Real Address (LRA) instruction considerations: LRA issued by a program running in AMODE 24 or AMODE 31 cannot return an address larger than 2 GB and it can be used if the virtual address is known to be backed below 2 GB.

Some additional information: When z/OS is running in z/Architecture mode, authorized applications that issue the LRA instruction against unfixed storage might receive an abend 0D3, reason code 13. The results of an LRA instruction against unfixed storage has always been unpredictable. In z/Architecture mode, the LRA instruction might require a 64-bit result when only a 32–bit result can be returned; in this case, the hardware causes a program interrupt. If the program is using the LRA instruction to validate that the virtual address is backed by real storage, then use the TPROT instruction instead. If a valid real address is required, the storage must be properly fixed in real storage below 2 GB before issuing the LRA instruction. The STRAG or LRAG instruction can be used to obtain a 64-bit real address if the storage can be backed anywhere. You should review your usage before migrating to z/Architecture, and make any required changes.

___ 10. Understand that z/Architecture provides a different format for architected parts of the first page of storage (the PSA). The ESA/390 format is mapped by macro IHAPSA. The z/Architecture format is mapped by macro IHAPSAE. In particular, the "old PSW", "new PSW" and "interruption parameter" fields have moved. Programs should not use any of these fields. But, if they do, they will not work correctly when running in z/Architecture (64-bit) mode. Note that none of the programming interface fields in the PSA have changed. For information about IHAPSA and IHAPSAE, look under the name PSA in *z/OS MVS Data Areas, Vol 3 (IVT-RCWK)*.

___ 11. Possibly increase the size of the extended system queue area (ESQA). Before z/Architecture, the system determined the size of the ESQA automatically during IPL/NIP to allow for the storage required to manage expanded storage. A portion of this ESQA storage was typically available for system use. However, when running in z/Architecture mode, the system does not set aside as much ESQA because none is needed to manage expanded storage, and thus there is also less ESQA available for other system uses. The effects of this reduction in ESQA will vary from system to system, ranging from:
- No negative impact at all, if the previous total ESQA size was large enough
- Increased conversion of ECSA/CSA to ESQA/SQA
- An inability to IPL
- Outages after IPL with abend X'878', abend X'80A', or a wait state

To avoid the more serious impacts, such as inability to IPL and outages, you might need to increase either:
- The ESQA value in the SQA= parameter of the IEASYSxx parmlib member, or
- The INITSQA value in the LOADxx parmlib member.

If you do specify additional ESQA on one of the two parmlib parameters, keep in mind that the reduction in ESQA available after migrating to z/Architecture mode will be about 8 MB less for every 1 GB of expanded

storage before the migration. However, because most of this storage was actually used for expanded storage management, you might need to specify only a fraction of this amount of additional ESQA. The amount of additional ESQA required will vary on each system.

__ 12. Determine if you want to control (by using the API64R start option) whether Communications Server - IP Services application programs should be passed 64-bit backed storage. TCP/IP 64-bit real addressing support is automatically enabled. TCP/IP exploits real storage in excess of 2 GB by allowing z/OS to back most fixed communications storage manager (CSM) data space pages above the 2 GB real storage bar. For information about API64R, see *z/OS Communications Server: SNA Resource Definition Reference*.

__ 13. Understand the capacity impacts of migrating to 64-bit mode. Washington Systems Center flash 10086 outlines the capacity planning methodology. (Search for "flash10086" at http://www.ibm.com/support/techdocs.) Use the SoftCap tool, available through the same Web address, to evaluate the effect on z/Architecture and processor capacity when migrating to newer levels of software.

__ 14. Evaluate and plan your paging environment. Review Chapter 2 of Washington Systems Center white paper *z/OS Performance: Managing Processor Storage in a 64-bit Environment - V1R1* at http://www.ibm.com/support/techdocs. (Search for "WP100269".)

__ 15. Understand enhancements in RMF. All metrics related to expanded storage are obsolete.

__ 16. Understand 64-bit virtual storage restrictions:
- Data spaces greater than 2 GB are not supported.
- Hiperspaces greater than 2 GB are not supported.
- Subspace capability is not extended to virtual storage above 2 GB.
- DIV is not extended to virtual storage above 2 GB.
- Sharing virtual storage above 2 GB is not supported.
- Copy-on-Write is not supported for virtual storage above 2 GB.
- DAT tables for virtual storage above 2 GB are not pageable.

__ 17. Review the IEFUSI exit routine for 64-bit virtual considerations. In the past you could limit program storage below 16 MB in virtual storage by using IEALIMIT. IEALIMIT can still be used to limit program storage in the nonextended region; however, IEFUSI is the preferred exit routine. For details on the advantages over IEALIMIT, see *z/OS MVS Installation Exits*.

__ 18. Use the MEMLIMIT parameter of parmlib member SMFPRM*xx*. This new parameter establishes a system default other than zero for available virtual storage above 2 GB. It is used for jobs that do not explicitly specify MEMLIMIT (or REGION=0) in their JCL. You must set up the system MEMLIMIT default according to individual system environment requirements. You need to take into account the overall central storage and paging space requirements in assessing an individual system's suitable MEMLIMIT default value. See Washington Systems Center flash 10165 at http://www.ibm.com/support/techdocs. (Search for "flash10165".)

We recommend that you use the IEFUSI exit routine to establish a MEMLIMIT value to protect the system from runaway tasks using too much storage above the 2 GB bar, thus exhausting central and auxiliary storage. Refer to item 13 and item 17.

__ 19. Review APAR OW54022, which describes changes to the thresholds at which SRM detects a common storage shortage below the 16 MB line.

__ 20. Specifying ARCHLVL 1 is not supported when running z/OS V1R7, so remove the ARCHLVL parameter from parmlib member LOAD*xx* once your migration to z/Architecture is complete, letting ARCHLVL default to 2.

__ 21. Determine if you want to control whether DFSMSdss obtains I/O buffers backed by 64-bit real storage. By default in z/OS V1R5 and later, DFSMSdss obtains 64-bit backed I/O buffers when running in z/Architecture mode. If you want DFSMSdss to obtain 31-bit backed I/O buffers, specify `EXEC PARM='ZBUFF64R=NO'` in the JCL or API invocation, or change the installation's default by turning off the UFPZB64R bit in the ADRUFO block with the options installation exit routine, ADRUIXIT. For example, when running DFSMSdss operations against storage devices that do not support 64-bit real addressing, you must tell DFSMSdss not to use I/O buffers that can be backed above the 2 GB bar. The DFSMSdss ZBUFF64R parameter is new in z/OS V1R5.

Reference information: See the checklist above.

Migration actions for everyone after the first IPL of z/OS V1R7

None.

Chapter 3. Hardware migration actions

This chapter describes hardware migration actions. The information in this chapter is not specifically related to migrating to z/OS V1R7; it only applies if you are changing hardware. Therefore, this chapter does not categorize the actions in terms of when they should be performed (before installing, before the first IPL, or after the first IPL).

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.

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
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.

Steps to take:

1. Determine whether the devices you use are supported. A list of supported I/O devices is in *z/OS and z/OS.e Planning for Installation*. Devices for which support was recently removed are listed below. 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).

Support was recently removed for the following devices:

- *Sysplex Timer® Model 1, 9037-001.* This device is a critical component of any multi-CEC sysplex or Parallel Sysplex. Service support for the Model 1 ended on 31 December 2003. Use the Model 2 instead, which is a full replacement for the Model 1. (You cannot upgrade a Model 1 to a Model 2.) An International Technical Support Organization (ITSO) redpaper, *Migration Planning for the 9037 Model 2 Sysplex Timer*, REDP3666, is available through http://www.ibm.com/redbooks.
- *Filenet 9246 optical libraries, 9247 optical drives, and 12-inch optical media.* As of z/OS V1R5, IBM has removed object access method (OAM) support for these devices. If you need to store objects on optical devices, you can replace these Filenet devices and media with IBM 3995 optical devices and media. If you do not require optical devices, you can transition the data to any z/OS-supported tape media or to DB2 tables on DASD.

Reference information:
- For a list of I/O devices that are supported, see *z/OS and z/OS.e Planning for Installation*.
- For information about deleting device definitions from the IODF, see *z/OS HCD Planning*.

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 65 536 devices, each with up to eight access paths.

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Anytime.
Is the migration action required?	Yes, if you are going to use new devices with z/OS V1R7.
Target system hardware requirements:	Dependent upon the new devices used.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	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). (For information about upgrading to the most current IODF level, see "Upgrade the IODF to V5" on page 216.) 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 a summary of the most commonly-used I/O devices supported by z/OS that are also directly supported by DFSMS functions, see *z/OS and z/OS.e 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*.

Determine appropriate coupling facility structure sizes

Description: Changing to a new coupling facility code (CFCC) level might require additional migration actions, such as increasing coupling facility structure sizes. For instance, if you are upgrading your z990 server to CFCC Level 14 to take advantage of the new functions it provides, then you might be required to increase coupling facility structure size definitions as a result of that migration.

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
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/eserver/ zseries/pso/cftable.html.
Target system software requirements:	None.

Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Steps to take: If you are migrating to a new CFCC level, 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 http://www.ibm.com/eserver/zseries/cfsizer/.

Reference information: For a detailed description of coupling facility code levels and the processors that support those levels, see http://www.ibm.com/eserver/zseries/pso/cftable.html.

Do not use ZOSE*xxxx* for a z/OS LPAR name on a z890 or z800 server

Description: In order for z/OS to run on a z890 or z800 server, the LPAR in which it runs (whether natively or as a VM guest) **cannot** be named ZOSE*xxxx*. If an LPAR on a z890 or z800 server is named ZOSE*xxxx*, you cannot run z/OS in that LPAR.

Element or feature:	Multiple.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Anytime.
Is the migration action required?	Yes, if you are installing a new z890 or z800 server and plan to run z/OS in an LPAR (either natively or as a VM guest).
Target system hardware requirements:	z890 or z800 server.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Steps to take: If you are installing a new z890 or z800 server and plan to run any release of z/OS in an LPAR, including as a VM guest, make sure that the LPAR name is not ZOSE*xxxx*.

Tip: The ability to add meaningful LPAR names to the configuration without a power-on reset was introduced on the z890 and z990 (driver 55) servers and z/OS V1R7. This support is called dynamic add/delete of an LPAR name. Before this support, extra LPARs were defined by adding reserved names in the input/output configuration data set (IOCDS). However, predicting meaningful LPAR names was often difficult.

Dynamic add/delete of an LPAR name allows reserved LPAR "slots" to be created in an IOCDS in the form of extra LCSS, Multiple Image Facility (MIF) image ID

pairs. These extra LCSS MIF image ID pairs (CSSID/MIFID) can be later assigned an LPAR name for use (or later removed) by dynamic I/O commands using HCD. The IOCDS still must have the extra I/O slots defined in advance because many structures are built based upon these major I/O control blocks in the hardware system area (HSA). This support on z/OS is exclusive to z/OS V1R6 (and later) on a z9-109, z990, or z890 server.

Reference information: *z/OS and z/OS.e Planning for Installation*.

Prepare for hardware changes described in IBM statements of direction

Description: The following statements of direction were announced in Hardware Announcement 203-266, dated 7 October 2003:

- **Token Ring on Hardware Management Console, SE, TKE workstation, IBM 2074:** The z990 and z890 will be the last zSeries servers to offer Token Ring adapter features on the Hardware Management Consoles, Support Elements (SEs), and Trusted Key Entry (TKE) workstations. The IBM 2074 Model 3 Console Support Controller will be the last controller to offer Token Ring adapter features. IBM is making these statements to allow enterprises sufficient opportunity to prepare for a migration to an Ethernet environment.

- **Hardware Management Consoles:** Beginning with the next server after the z990 and z890, all new Hardware Management Consoles on all currently marketed zSeries servers are intended to become closed platforms. They will only support the Hardware Management Console application and not the installation of other applications such as the IBM ESCON Director and the IBM Sysplex Timer console applications. When available, the next-generation Hardware Management Console is expected to communicate only with G5 servers and above (Multiprise 3000, G5, G6, and zSeries servers). TCP/IP is intended to be the only communications protocol supported.

- **OSA-Express Layer 2 support:** IBM intends to extend its network virtualization capabilities with updates to OSA-Express, Virtual Switch, and guest LANs. When updated, these facilities will be designed to operate in Layer 2 mode (referring to Layer 2 of the Open Systems Interface [OSI] reference model). This is planned to allow destination and target nodes to be referenced by their Media Access Control (MAC) addresses instead of by Internet Protocol (IP) addresses, which is intended to enable protocol-independent network connectivity. Layer 2 support applies to an OSA-Express feature when configured in QDIO mode (CHPID type OSD). Layer 2 support is expected to be applicable, initially, to the z/VM and Linux on zSeries environments.

- **ISC-3s in compatibility mode:** IBM intends z990 and z890 to be the last family of zSeries servers to support:
  - Attachment of ISC-3 links to HiPerLinks (ISC-2) on G5/G6 servers
  - Compatibility mode definitions for ISC-3 links (CHPID types CFS and CFR)

All statements regarding IBM's plans, directions, and intent are subject to change or withdrawal without notice.

Element or feature:	Multiple.
When change was introduced:	Announced in Hardware Announcement 203-266, dated 7 October 2003.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Anytime.

Is the migration action required?	No, but recommended if you use any of the hardware in "Description" above because it will become a requirement in the future.
Target system hardware requirements:	See "Description" above.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Steps to take: Take into account the statements in "Description" above as you make your plans for the future.

Reference information: None.

Migrate to a z9-109 server

Description: The IBM System z9 109 (z9-109) server is the follow-on to the zSeries servers. The z9-109 server provides more processing power, memory, and I/O capacity than the zSeries servers (z990, z890, z900, and z800). By migrating to z/OS V1R7 on a z9-109 server, you can take advantage of these improvements.

To read about the software actions necessary to migrate your z/OS system from your current server to a z9-109 server, see *z/OS Migration to the IBM System z9*. You can obtain this document by going to the Migration and Installation section of the z/OS Web site: http://www.ibm.com/servers/eserver/zseries/zos/installation/.

Migrate to a z990 or z890 server

Description: The IBM @server zSeries 990 (z990) and zSeries 890 (z890) represent the second generation of zSeries servers. The z990 and z890 servers provide more processing power, memory, and I/O capacity than the first generation of zSeries servers (z900 and z800). By migrating to z/OS V1R7 on a z990 or z890 server, you can take advantage of these improvements.

Element or feature:	Multiple.
When change was introduced:	June 2003 and later through the following enhancements: • The *z/OS V1R4 z990 Compatibility Support* feature • The *z/OS V1R4 z990 Exploitation Support* feature • The *z990 Cryptographic Support* Web deliverable • The *z990 and z890 Enhancements to Cryptographic Support* Web deliverable • The *z/OS.e V1R4 z990 Coexistence* feature • The *z/OS.e V1R4 z990 Coexistence Update* feature
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Anytime.
Is the migration action required?	Yes, if you want to run z/OS V1R7 on a z990 or z890 server. Also, be aware that if any non-z990, non-z890 systems coexist with z990 or z890 systems, coexistence requirements affect the non-z990, non-z890 systems.

Target system hardware requirements:	A z990 or z890 server and, for cryptography, the following hardware features: PCI X Cryptographic Coprocessor (PCIXCC), CP Assist for Cryptographic Functions (CPACF) DES/TDES, and PCI Cryptographic Accelerator (PCICA).
Target system software requirements:	If you use Tivoli System Automation for OS/390 V2 (5645-006), R2 or later is required.
Other system (coexistence or fallback) requirements:	For sysplex and shared DASD requirements, see item 6 on page 80. For CFCC coexistence requirements, see item 7 on page 81.
Restrictions:	• Only LPAR mode (not basic mode) is supported on a z990 or z890 server. • Also, see the note on page 78.
System impacts:	A power-on reset is required when adding or removing an LCSS, changing the maximum number of devices for an LCSS, adding or deleting LPARs, changing the name of an LPAR, and adding or changing a resource in an LCSS other than LCSS 0.

Steps to take: Follow the requirements and recommendations below. Included is information about required HMC levels, configuring a z990 or z890 server, installing software for images that run on a z990 or z890 server, installing software and microcode for coexistence with a z990 or z890 server, cryptographic considerations, and operational considerations.

First, some general considerations and reminders:

- "z990 compatibility code" refers to the code that was first delivered in the z/OS V1R4 z990 Compatibility Support feature; then delivered in the replacement feature, z/OS V1R4 z990 Exploitation Support (which can still be obtained for z/OS V1R4); and finally integrated into z/OS V1R5 and subsequent releases.
- The z990 compatibility code can be run on whatever processors are supported by the releases. That is, your system does *not* have to be running on a z990 or z890 server to have the code installed or IPLed.
- Do not switch your software release level at the same time that you switch hardware.
- It is good software management policy to have members of the sysplex at the same software level other than during brief migration periods.

Actions you can take before you install a z990 or z890 server

1. **Upgrade HMC microcode.** Upgrade the hardware management console (HMC) driver level to 1.8.0 (when available). IBM recommends migrating z900, z800, G5, and G6 HMCs to HMC driver level 1.8.0 before z990 or z890 installation.

2. **Install software that you will use to define the z990 or z890 server.** Install and deploy z990 compatibility support on the system that will be used to define the z990 or z890 server using HCD.

   Notes:

   a. You might want to define the z990 or z890 server from a system image that will eventually run on a z990 or z890 server because the z990 compatibility code is required not only to define a z990 or z890 server but also to run on a z990 or z890 server.

b. For z/OS (and z/OS.e), the z990 compatibility code was initially shipped with the optional unpriced z/OS V1R4 z990 Compatibility Support feature (and z/OS.e V1R4 z990 Coexistence feature). Once the z/OS V1R4 z990 Exploitation Support feature (and z/OS.e V1R4 z990 Coexistence Update feature) became available, the first set of features was withdrawn (in October 2003) and the compatibility code was shipped with the new features. For z/OS (and z/OS.e) V1R5 and later, the compatibility code is integrated.

c. For z/OS V1R4 customers, the z/OS V1R4 z990 Exploitation Support feature can be ordered using CBPDO; ShopzSeries customers can even get the features delivered electronically.

3. **Define the z990 or z890 server.** Use HCD to define the z990 or z890 server. Note that once the z990 compatibility support is installed (as part of z/OS V1R5 or later, the z/OS V1R4 z990 Compatibility Support feature, or the z/OS V1R4 z990 Exploitation Support feature), you can access the HCD code to define the z990 server by using a STEPLIB DD statement or by IPLing the system where the code was installed. (IPLing is usually preferred.)

When installing a new ("net add") z990 or z890 server, you must define the operating system and processor. You can use the copy or migrate functions of HCD to model these definitions after an existing processor.

When using a miscellaneous equipment specification (MES) package to upgrade a z900 server to a z990 server, or to upgrade a z800 server to a z890 server, or when replacing one or more z900 servers (or G5, G6, or z800 servers) with a z990 or z890 server (a "box swap" or "push/pull"), you must copy or migrate the existing definitions to a z990 or z890 Logical Channel Subsystem (LCSS). IBM recommends the following:

- Ensure that the production input/output definition file (IODF) that will be used to migrate existing definitions contains *all* the definitions for *all* the items to be migrated (operating system configurations, ESCON and FICON® switches, logical partitions, channels, control units, devices, and coupling facility processors). Using one source IODF means that there will be no conflict to be resolved during the migration process with any control unit or device for address or number definition conflict, address or number range conflict, or type definition conflict.

- If you are consolidating two processors into a z990 or z890 server, copy or migrate one processor into LCSS 0 and the other into LCSS 1. Note that z/OS V1R5 or later, or z/OS V1R4 with the z/OS V1R4 z990 Exploitation Support feature, is required for a z/OS image to be IPLed in an LPAR associated with any LCSS other than LCSS 0 (unless running as a guest under z/VM).

When making the z990 or z890 hardware definitions, you must:

- *Define the z990 or z890 processor.* Only LPAR mode is allowed. You also need to define the number of LCSSs that you intend to use. Note that increasing or decreasing the number of LCSSs will require a power-on reset of a new input/output configuration data set (IOCDS). IBM recommends that when you define a z990 or z890 server, you should initially define the number of LCSSs you expect to use — up to two LCSSs on a z890 or up to four LCSSs on a z990.

- *Define the channel subsystems.* For each channel subsystem, specify an LCSS ID, a description, and the maximum number of devices:

  Notes:

  a. z/OS V1R4 (and z/OS.e V1R4 on a z890 server) with z990 compatibility code installed can be IPLed only in LCSS 0 when running in LPAR mode.

However, these releases can run as a guest under z/VM, regardless of the LCSS z/VM is using. Therefore, you can run z/OS in an LPAR in LCSS 0 and z/VM in an LPAR in LCSS 1, with one or more additional z/OS images running as guests of the z/VM system. Note that z/OS V1R5 or later, and z/OS V1R4 with the z/OS V1R4 z990 Exploitation Support feature installed, can be run in any LPAR regardless of the LCSS of the LPAR.

b. There is no hardware system area (HSA) expansion support on the z990 or z890 support element (SE). The maximum number of devices, defined for each LCSS, replaces the HSA expansion percentages in the central processor complex (CPC) activation profile on the support element.

c. If you change the maximum number of devices in an LCSS, you cannot do an ACTIVATE; you must do a power-on reset. IBM recommends that when you define a z990 or z890 server, you initially define the maximum number of devices that you expect to use in the future.

d. Because of the increase in the number of LPARs and LCSSs, be sure that the value specified on the MAXDEV keyword is large enough. (Increasing MAXDEV requires a power-on reset). The HCD default for maximum number of devices is 63K. This could result in a large amount of HSA storage being wasted.

- *Define logical partitions.* The partition names may not be duplicated across LCSSs. On servers other than z990 and z890 servers, partition numbers are the same as Multiple Image Facility (MIF) IDs. On z990 and z890 servers, partition numbers are assigned at power-on reset based on the IOCDS. MIF IDs are still specified using HCD/IOCP. On z990 and z890 servers, the partition number can be in the range 1–30 (X'1–1E') and the MIF ID must be in the range 1–15 (X'1–F'). The partition number will be unique across all LCSSs. The MIF ID must be unique within each LCSS, but can be duplicated across LCSSs. Note that partition numbers are not related to LPAR IDs, which are specified in the HMC image profile.

  Notes:

  a. IBM recommends when you define a z990 or z890 server, you should initially define the number of logical partitions that you expect to use.

  If you plan to exploit more than 15 LPARs, then define the number of LCSSs (two or more) that you expect to use. For exploiting more than 15 LPARs and more than one LCSS, ensure that you have the correct hardware driver level. You only need to define the LCSS and LPARs (and specify the maximum devices for the LCSS). The LPAR can be defined with no I/O resources. I/O configuration definitions can be dynamically added later to a logical partition (nondisruptively). The newly defined I/O configuration definition change can be dynamically activated. Note that any G5, G6, z800, or z900 servers used as a coupling facility image in this environment need to have the CFCC z990 Compatibility MCL installed (see item 7 on page 81 for details).

  b. There is no correlation between LPAR ID and the LCSS under which an LPAR runs. There can be LPARs in LCSS 0 with LPAR IDs greater than 15, and there can be LPARs in LCSS 1 (and LCSS 2 and LCSS 3) with LPAR IDs less than or equal to 15.

- *Define channel paths.* The processor name is qualified by the LCSS ID. Channel path IDs (CHPIDs) only need to be unique within an LCSS.

  Notes:

  a. There are no default CHPIDs on the machine when configured or shipped. Physical channel IDs (PCHIDs) must be defined.

b. Cryptography functions do not require CHPIDs.

   c. Spanned channels access and candidate lists are by LCSS and partition.

   d. The internal queued direct (IQD) CHPID on the VTAM® start option IQDCHPID=*xx* must be defined as a spanned CHPID if communication with systems in other LCSSs is desired.

- Recommended: *Use the CHPID Mapping Tool* to map logical CHPIDs to physical channels (PCHIDs) and create input to HCD/IOCP. The tool is a workstation-based Java application available from the IBM Resource Link™ Web site: http://www.ibm.com/servers/resourcelink. It updates the z990 or z890 IOCP input file with the "PCHID" keyword and can generate reports to help with cabling. To obtain and use the tool, do the following:

   – If this is an initial z990 or z890 order, download a machine order file (CFReport or manufacturing order file) from Resource Link to a workstation.

   – Create a validated work IODF (an IODF that is valid except that it is missing PCHIDs) using HCD option 2.12 (Build Validated Work I/O Definition File).

   – Create an IOCP deck without PCHIDs or with some PCHIDs missing using HCD option 2.3 (Build IOCP Input Deck).

   – Download the IOCP file (which can include PCHID keywords) to the workstation.

   – Download the tool.

   – Run the tool selecting the 2084 hardware configuration file (.hwc or .cfr) and import the IOCP statements.

   – Upload the updated IOCP deck with the PCHIDs assigned using HCD option 5.1 (Migrate IOCP/OS Data). Choose migrate option 3 (PCHIDS).

   – Build a production IODF.

   – Write the IOCDS to the z990 or z890 support element using HCD or stand-alone IOCP.

- *Define control units.* A control unit is defined once in the IODF but the CHPID.link combinations for a z990 or z890 processor are defined for each LCSS because each LCSS has its own set of CHPIDs.

- *Define devices.* The channel subsystem data (for example, the preferred path and candidate lists) must be specified for each LCSS (and may be different for each LCSS).

Note: The following features and functions are not supported by the z990 and z890 servers:

  - Parallel channels. Use the IBM ESCON Converter or the Optica Technologies 34600.

  - OSA-2 adapters. Use the equivalent OSA-Express adapter. (For FDDI, use a multiprotocol switch or router with the appropriate network interface.)

  - OSA-Express ATM adapters. Use a multiprotocol switch or router with the appropriate network interface, for example, 1000BASE-T or Gigabit Ethernet.

  - 4-Port ESCON cards. Replace these with new 16-Port ESCON cards during upgrade. The 16-Port ESCON card has a MTRJ-45 connector.

  - FICON cards (pre-FICON Express). Replace these with FICON Express during upgrade. FICON Express has a different connector.

- PCICC. This feature is replaced with PCIXCC for most of the commonly used cryptography functions.
- Activation of an over-defined channel configuration.
- Systems Network Architecture (SNA) Operations Management commands and SNA based APIs are not supported on z990 and z890 servers. These commands were previously used by the System Automation for OS/390 product as well as NetView. It is recommend that you now use the Simple Network Management Protocol (SNMP) application programming interfaces (APIs) for your automation needs. If you previously used the System Automation for OS/390 product, you must now use Version 2.2 or later. This will allow you to define an automation policy for SNMP APIs rather than a policy for SNA Operations Management commands. (Note that msys for Operations was upgraded in the z/OS V1R4 z990 Exploitation Support feature to use System Automation V2R2 so that automation policies can use the SNMP APIs.) If you directly used the SNA Operations Management commands on NetView, you must now use an SNMP agent and the SNMP APIs for systems automation management. For detailed information about the SNMP API commands and environment requirements, see *zSeries Application Programming Interfaces*, SB10-7030. For more information about the SNA Operations Management command support that is not offered on z990 or z890, see *Managing Your Processors*, GC38-0452. Both publications are available on IBM Resource Link.

4. **Install z990 compatibility or exploitation software on z990 or z890 system images.** Install and deploy z990 compatibility or exploitation support on all z/OS V1R4 or later system images that will eventually run on a z990 or z890 server. Also, install and deploy the z990 compatibility support on all z/OS.e V1R4 system images that will eventually run on a z890 server. With z/OS V1R5 and later, the support is integrated. With z/OS V1R4, the support consists of the z/OS V1R4 z990 Exploitation Support feature.

   Notes:

   a. You don't have to reinstall the z990 compatibility or exploitation code if you IPL the system that was used to define the z990 or z890 server using HCD. However, if some time has passed, you should review and install all the applicable service in the 2084DEVICE (for z990) or 2086DEVICE (for z890) PSP bucket.

   b. You will need to obtain and install all service in the 2084DEVICE (for z990) or 2086DEVICE (for z890) PSP bucket. Customers ordering the z/OS V1R4 z990 Exploitation Support feature will have all the z/OS service listed in the PSP bucket delivered with their order. Anyone obtaining z990 compatibility, exploitation, or cryptography support from a Web deliverable will have to place a separate service order to receive service.

   c. If you are currently running z/OS V1R4 on a G5, G6, or Multiprise 3000 server *and* plan to move those system images to a z990 or z890 server, then you should download and install the z/OS V1R2/3/4 Bimodal Migration Accommodation. IBM recommends the use of the Accommodation so that the system images run using 31-bit (ESA/390) architecture when initially brought up on a z990 or z890 server (up to six months from licensing z/OS to the z990 or z890 server). IBM recommends not switching architecture at the same time as upgrading your hardware.

   d. If you have cryptographic workloads, you need to review the considerations listed at item 8 on page 82.

e. You may choose to install the z990 Cryptographic Support Web deliverable on z/OS.e V1R4 systems to maintain a common maintenance environment between your z/OS and z/OS.e systems.

f. z/VM V4R3 and V3R1 must have the appropriate z/VM compatibility PTF installed to IPL a z/OS V1R4 guest on a z990 or z890 server. The APAR is VM63124.

5. **Install z990 compatibility software on disaster recovery system images.** If you are currently running z/OS V1R4 or z/OS V1R3 on a z900, z800, G5, G6, or Multiprise 3000 server *and* plan to use a z990 or z890 server for disaster recovery for that image, then you must install and deploy z990 compatibility or exploitation support before any disaster recovery testing or actual recoveries. Note that if you are running z/OS V1R4 on a G5, G6, or Multiprise 3000 server, you should download and install the z/OS V1R2/3/4 Bimodal Migration Accommodation. IBM recommends the use of the Accommodation so that the disaster recovery image can run using 31-bit (ESA/390) architecture. IBM recommends not switching architecture at the same time as recovering your system to a disaster recovery site.

If your disaster recovery system is a z/OS V1R6 or later system, ensure that the correct server is available at the disaster recovery site. (It must be a z990, z890, z900, or z800 server running in z/Architecture mode.)

6. **Install z990 sysplex coexistence software.** Install and deploy z990 compatibility support on all z/OS V1R4 and z/OS.e V1R4 members of a sysplex (operating system images) that will run on G5, G6, z800, or z900 servers and participate in a sysplex that will eventually have one or more members of the sysplex (operating system image) or a coupling facility image on a z990 or z890 server with an LPAR ID of greater than 15.

All images that share DASD with any z/OS, z/VM, or VSE operating system images running on a z990 or z890 server need to have ICKDSF R17 installed. It can either be installed as part of compatibility support for z/OS or as a separate product. If ICKDSF R17 isn't already installed on z/OS systems, IBM recommends installing it with the z990 compatibility support.

IBM recommends that the z990 compatibility code be rolled out on all members of a sysplex, and ICKDSF R17 be deployed to all other systems that share DASD, before any z990 or z890 server is brought into use in the sysplex.

Notes:

a. The coupling facility image on the z990 or z890 server could either be an ICF along with other partitions running z/OS or other workloads, or it could be the only image on the z990 or z890, making it look effectively like a stand-alone coupling facility. In this document, both are called coupling facility images.

b. z990 compatibility support is not required on members of a sysplex (operating system images) that run on G5, G6, z800, or z900 servers and participate in a sysplex that will have one or more members of the sysplex (operating system images) or a coupling facility image on a z990 or z890 server, if *both* of the following are true:

- All of the members of the sysplex on the z990 or z890 server have an LPAR ID of 0–15 (X'F').
- Any coupling facility image that is used by the sysplex and resides on the z990 or z890 server has an LPAR ID of 0–15 (X'F').

If, at any time in the future, one or both of these conditions is no longer true, then z990 compatibility support will be required.

c. If a system without z990 compatibility or exploitation support is IPLed into a sysplex that contains an operating system image running on a z990 or z890 server with an LPAR ID greater than 15, the back-level system is removed from the sysplex with a wait state code of 0A3/154. Similarly, z/OS V1R4 or later images with LPAR ID greater than 15 (which requires, for z/OS V1R4, the z/OS V1R4 z990 Exploitation Support feature to be installed) will not join a sysplex unless all images in the sysplex are running with (at least) the z990 code installed.

d. If z990 compatibility or exploitation support has not been deployed on *all* members of the sysplex, then IBM recommends that you should *not* define more than 15 LPARs. Minimally, you *cannot* put any active z/OS sysplex or coupling facility images in an LPAR with ID greater than 15 (X'F').

e. In order to reduce the number of IPLs that could be required, if a CFCC upgrade is required (based on item 7) and the compatibility or exploitation code is not yet installed, you should plan to install and deploy the z990 code during the same disruptive change window.

f. Coupling facility images on G2, G3, G4, or equivalent processors cannot be connected to operating system images on a z990 or z890 server and therefore any structures in these coupling facility images also need to be moved to a coupling facility that can connect to this environment (G5, G6, z800, z900, z990, or z890 server).

g. You may choose to install z990 compatibility support on z/OS.e V1R4 systems, even if they do *not* participate in a sysplex where one of the images runs on a z990 or z890 server, to maintain a common maintenance environment between your z/OS and z/OS.e systems.

7. **Install z990 CFCC coexistence microcode.** If you intend to have an operating system image or a coupling facility image on a z990 or z890 server *and* have more than 15 LPARs defined (even if 15 or fewer are activated), you need to have CFCC compatibility code installed on:

- Any coupling facility image (stand-alone or ICF) on a G5, G6, z800, or z900 server that will connect to an operating system image on the z990 or z890 server.

- Any coupling facility image (stand-alone or ICF) that will be duplexed with a z990 or z890 coupling facility image.

IBM recommends that the CFCC z990 compatibility MCL be rolled out on all coupling facility images that will reside on a G5, G6, z800, or z900 server that will connect to an operating system image on a z990 or z890 server or be duplexed with a coupling facility image on a z990 or z890 server, before any z990 or z890 server is brought into use in the sysplex.

Notes:

a. The CFCC z990 compatibility code is provided with the GA level of CFCC Level 11 (for G5 and G6 servers) and as an MCL on CFCC Level 12 (for z900 and z800 servers). The CFLEVEL 12 MCL is disruptive, so IBM recommends that you coordinate the installation of this MCL with other disruptive MCLs, if possible. In addition, as recommended previously, if the z/OS V1R4 z990 compatibility code is not yet installed, you should plan to install and deploy it during the same disruptive change window.

b. If you are MES-upgrading to a z990 or z890 server, or replacing ("box swap") an existing server, then the "old" server does not require the CFCC compatibility MCL. However, any remaining G5, G6, z800, or z900 servers that will be connecting to the z990 or z890 server will require the MCL upgrade (if more than 15 LPARs will be defined).

c. If 15 or fewer LPARs will be defined on the z990 or z890 server, then the CFCC compatibility code is *not* required on z900 and z800 servers. If at any time in the future you define more than 15 LPARs, then the CFCC compatibility code will be required at that time.

d. Only coupling facility images on G5, G6, z800, and z900 servers are supported. While z990 and z890 servers do not offer a stand-alone coupling facility option, you could have a coupling facility image as the only image in the z990 or z890 server, making it look effectively like a stand-alone coupling facility, or you could have an ICF image along with other partitions running z/OS, or other workloads, on your z990 or z890 server (possibly using coupling facility duplexing). Alternatively, you can continue to use your existing z900 or z800 coupling facilities (2064-100) and G5/G6 coupling facilities. However, some workloads, such as data sharing, global resource serialization, and DB2 (users of locking structures) are likely to require newer technology for performance reasons. If you have such workloads, you should plan to upgrade G5 coupling facilities (9672-R06) to z900 coupling facilities, or move your coupling facilities to z990s or z890s. IBM does *not* recommend using G5 coupling facilities in a Parallel Sysplex cluster with z990 or z890 servers for these workloads. You should only use them as a temporary migration step.

e. If you have a coupling facility image (stand-alone or ICF) on a G5 or G6 server that will either connect to an operating system image on a z990 or z890 server or be duplexed with a z990 or z890 coupling facility image, then the CFCC level of the G5 or G6 coupling facility image *must* be CFCC Level 11 (or later).

f. If you have a coupling facility image (stand-alone or ICF) on a z900 or z800 server that will either connect to an operating system image on a z990 or z890 server or be duplexed with a z990 or z890 coupling facility image, then the CFCC level of the z900 or z800 coupling facility image *must* be CFCC Level 12.

Table 8. Summary of z990 CFCC coexistence support

Server	CFCC level	15 or fewer LPARs defined on a z990 or z890 server	More than 15 LPARs defined on a z990 or z890 server
Pre-G5, G5, or G6	CFCC Level 9 (or below)	Not supported	Not supported
G5 or G6	CFCC Level 11	Supported	Supported
z800 or z900	CFCC Level 9 or 10	Not supported	Not supported
z800 or z900	CFCC Level 12	Supported	Not supported
z800 or z900	CFCC Level 12 with CFCC compatibility code, or CFCC Level 13	Supported	Supported

8. **Install cryptographic software, if necessary.** If you use cryptographic services, ensure that you have the level of cryptographic support that you require on your z/OS system:

   - If you are running z/OS V1R4 or later and only need clear key cryptography (SSL and TLS functionality) using the PCI Cryptographic Accelerator (PCICA) and CP Assist for Cryptographic Functions (CPACF) DES/TDES hardware features, then this support is integrated in z/OS V1R5 and later, and is included in the z/OS V1R4 z990 Compatibility Support feature. Note that the

PCICA hardware feature is only required if you want or need improved performance (such as SSL "handshakes") using the cryptographic accelerator.

- If you require secure key cryptography, you minimally need the PCIX Cryptographic Coprocessor (PCIXCC) hardware feature and ICSF FMID HCR770A. ICSF FMID HRC770A is integrated in z/OS V1R6 and was available on z/OS V1R5 and z/OS V1R4 through the z990 Cryptographic Support Web deliverable. The z990 and z890 Enhancements to Cryptographic Support Web deliverable (which contains FMID HCR770B and which replaces the z990 Cryptographic Support Web deliverable) also provides this support.

- If you require clear key and secure key cryptography, and PKE/PKD service enhancements, Double Length Unique Key Per Transactions (DUKPT), and use of the EMV (Europay Mastercard and Visa) standard for z990 and z890 servers, you need the z990 and z890 Enhancements to Cryptographic Support Web deliverable (ICSF FMID HCR770B), which is not integrated in z/OS V1R6 and is applicable to z/OS V1R6, z/OS V1R5, and z/OS V1R4. In z/OS V1R7, this support is integrated (ICSF FMID HCR7720).

Note: The following infrequently used cryptographic functions are removed from z990 and z890 cryptography:
- Digital Signature Algorithm support
- ANSI x9.17 services and key types
- Cipher_Text Translate (CSNBCTT)
- German Bank Pool - Pin Offset
- CSFUDK (replaced with CSNBDKG)
- Commercial Data Masking Facility (CDMF) – 40-bit Encryption

Actions you can take when you order a z990 or z890 server

Determine future target I/O requirements *before* placing your order.

If required, use "Plan Ahead" for I/O cages and associated base infrastructure (adding I/O cages later is disruptive).

PCIXCC installation will be nondisruptive. Use "Plan Ahead" for the PCIXCC to ensure that slots are reserved in advance. This also balances the configuration when PCIXCC is available and installed.

Once I/O infrastructure is planned ahead, model upgrades or adding I/O cards can be nondisruptive, and Self-Timed Interconnect buses (STIs) are hot-pluggable.

Ensure that proper hardware features are ordered. For example, hardware features for cryptography are:
- PCIXCC (feature code 0868), if required (when available)
- CP Assist for Cryptographic Functions (CPACF) DES/TDES (feature code 3863)
- PCICA (feature code 0862), if required

Ensure that Driver Level 55 or later is ordered if you want support for the following features and functions on the z990 server:
- Four Logical Channel Subsystems
- Spanned external channels
- PCIX Crypto Adapter Integrated Console Controller
- OSA Integrated Console Control (OSA-ICC)
- Extended Translation Facility
- zSeries Application Assist Processor (zAAP) (requires Driver Level 55K or later)

Actions you can take after you install z990 compatibility (or exploitation) code

1. **Heed z990 and z890 IPL restrictions.** A z/OS V1R4 system that is IPLed on a z990 or z890 server (or z/OS.e V1R4 system IPLed on a z890 server) with z990 compatibility code installed, must be IPLed in an LPAR whose ID is in the range 0–15 (X'F'). If z/OS V1R5 or later, or z/OS V1R4 with the z/OS V1R4 z990 Exploitation Support feature, is IPLed, then its LPAR ID can range from 0–63 (X'3F'). If a system with z990 compatibility code is attempted to be IPLed with an LPAR ID in the range 16–63 (X'10'–X'3F'), then the system will terminate with a 07C-02 wait state.

   Notes:

   a. The LPAR ID is specified on HMC Image Profile (Partition ID).

   b. Even if z/OS V1R4 (or z/OS.e V1R4 on a z890) with z990 compatibility code is IPLed on a z990 or z890 server, you can still define LPARs with LPAR IDs greater than 15. IBM recommends not defining an LPAR ID greater than 15 for a coupling facility image (if you are running in this environment) if you don't have a current (or future) requirement for more than 15 LPARs. Otherwise, you are required to install the z990 compatibility support on all non-z990, non-z890 systems in the sysplex.

   Reminders:

   - Defining more than 15 LPARs, even if you don't activate all of them from day one, will result in a requirement to install the CFCC compatibility support on all coupling facilities that reside on G5, G6, z800, and z900 servers in the sysplex.

   - z/OS V1R4 (and z/OS.e on a z890 server) with z990 compatibility code installed can be IPLed only in LCSS 0 when running in LPAR mode. However, these releases can run as a guest under z/VM, regardless of the LCSS z/VM is using. Therefore, you can run z/OS in an LPAR in LCSS 0 and z/VM in an LPAR in LCSS 1, with one or more additional z/OS images running as guests of the z/VM system. Note that z/OS V1R5 or later, or z/OS V1R4 with the z/OS V1R4 z990 Exploitation Support feature installed, can run in any LPAR regardless of the LCSS of the LPAR. If a system with z990 compatibility code and not running as a guest under z/VM is attempted to be IPLed with an LCSS that is not 0, z/OS terminates with a 07C-01 wait state.

2. **Update CFRM policies.**

   If a coupling facility image resides on a G5, G6, z800, or z900 server, then the partition number currently specified in the CFRM policy is the same as the partition number defined in HCD. No change is required for the partition number.

   If a coupling facility image resides on a z990 or z890 server, then the partition number specified in the CFRM policy is the logical partition identifier specified in the HMC Image Profile (Partition ID). The CFRM policy utility was changed to accept a two-digit hexadecimal PARTITION value for an LPAR ID greater than 15.

   Notes:

   a. If you move a coupling facility to a z990 or z890 server in an LPAR whose ID is greater than 15, then the CFRM policy must be updated using the level of the utility provided with the z990 compatibility code. If at any time in the future the coupling facility is moved to a LPAR with ID greater than 15, then the CRFM policy must be updated at that time.

   b. In order to use two-digit partition values, the z990 compatibility or exploitation code must be installed on *all* systems in the sysplex before activating the CFRM policy change.

    c. The SETXCF START,POLICY=CFRM command to make the updated CFRM policy active should be issued on a system with the z990 compatibility or exploitation code. IBM recommends that this be done even if you are not using two-digit partition values.

3. **Update automation for new and changed messages.**

    The following messages are changed to display two-digit LPAR IDs: IOS431I, IXC101I, IXC105I, IXC357I, IXC360I, IXC361I, IXC362I, IXC500I, IXC505I, IXC506I, IXC507I, IXC515I, IXC517I, IXC518I, IXC519E, IXC551I, IXC579I, IXL008I, IXL010E, IXL141I, IXL150I, IXL157I, IXL158I, IXL160E, and IOX50xI.

    PCHID information is now displayed, when appropriate.

    The following messages are associated with changed command output:

- IEE174I – display output for D M=CPU command
- IOS506I display output for D IOS,CONFIG(HSA) and D IOS,CONFIG(ALL) command output

4. **Notify those affected by changed command output.** Command syntax is not changed for z990 and z890 support but rather the display output for the following commands is changed:

- The D M=CPU command can now display a two-hexadecimal-digit LPAR ID from partitions running on a z990 or z890 server, which supports two-digit LPAR IDs. (The message number is IEE174I.) The logical CPU address no longer appears in the CPU ID. CSS ID, MIF ID, and the like are now formatted.
- The D IOS,CONFIG(HSA) command will display zeros for the unshared subchannel and logical CUs lines in the message. (The message number is IOS506I.) Once z/OS V1R5 or later, or z/OS V1R4 with the z/OS V1R4 z990 Exploitation Support feature, is installed, subchannel and logical CUs will be displayed by LCSS.
- The D M=CHP command is changed to add PCHID to the display.
- The D CF command is changed to support two-hexadecimal-digit LPAR IDs and PCHIDs.
- The D XCF command is changed to support two-hexadecimal-digit LPAR IDs.
- If you are exploiting IRD and have an LPAR cluster with images spanning both LCSS 0 and LCSS 1, then you *must* issue the VARY SWITCH on a system that has z/OS V1R5 or later, or z/OS V1R4 with the z/OS V1R4 z990 Exploitation Support feature, installed.

5. **Modify programs affected by changed SMF records.** If you currently process SMF records 70, 74, 79, and 89, you will need to review changes and modify any user-written programs if they are affected. The changes are:

- SMF Record 70 Subtype 1 (CPU and PR/SM™ Activity) is now split into multiple records if the number of LPARs and CPs requires more than 32K. Each piece is self-containing, that is, records can be processed without reassembling the broken pieces.
- SMF Record 74 Subtype 1 (Device Activity) is changed because of I/O architecture.
- SMF Record 79 Subtype 9 (Device Activity) is changed because of I/O architecture.
- SMF Record 89 (product usage data) is changed to support 4-bit and 8-bit LPAR identifiers and more than 15 LPARs.
- SMF Record 99 Subtype 8 (WLM LPAR Management – CPU Period Table Entry) is changed to add the CSS ID.

- SMF Record 99 Subtype 9 (I/O Subsystem Info – Channel Path Data Entry) is changed to add the CSS ID.

6. **Update parmlib members.** Review parmlib changes and update members as appropriate:

    - If you use cryptography, then you should be aware that ICSF now provides IPCS support. A recently-introduced parmlib member, CSFIPCSP, will be installed into the library specified on the SMP/E PARMLIB DDDEF statement (and delivered in SYS1.IBM.PARMLIB in ServerPac). Ensure that this library is included in your IPCS concatenation. If you copy members from that library to another library, you have to copy CSFIPCSP.

    - Before the z/OS V1R4 z990 Exploitation Support feature, the CMB= parameter specified the I/O device classes for which measurement data was to be collected, in addition to the DASD and tape device classes. It also allowed you to specify the number of CMB slots to reserve for adding more devices with an ACTIVATE. Now, on z990 and z890 servers, the system ignores the CMB and uses instead the measurement data in the extended channel measurement block (ECMB).

        Note: This change to the CMB affects programs, including ISV programs (especially monitor programs), that use the CMB. Review any user-written programs and contact ISVs, if necessary, to obtain updates that use the ECMB. (Before z/OS V1R7, if ISV support was not available, you could specify ECMB=NO in parmlib member IEAOPT*xx* as a circumvention until the ISV support became available. But as of z/OS V1R7, ECMB usage is required. See "Remove ECMB=NO from parmlib member IEAOPT*xx*" on page 93.)

    - You might need to increase by one the limit for the number of SCOPE=COMMON data spaces defined on the MAXCAD IEASYS*xx* parmlib parameter, which specifies the maximum number of SCOPE=COMMON data spaces to be allowed during an IPL. (As of z/OS V1R7, the IBM Health Checker for z/OS can help you make the best MAXCAD definitions.) As of the z/OS V1R4 z990 Exploitation Support feature, a new SCOPE=COMMON data space was added. For a complete list of SCOPE=COMMON data spaces that were added, and that might impact your MAXCAD specification, see "Accommodate new SCOPE=COMMON data spaces" on page 61.

    - There is no change to member SMFPRM*xx*. However, there is a change in the description of the serial number in the SID parameter when a z990 or z890 is involved; the first two digits are the LPAR ID instead of the logical CPU address and LPAR ID.

7. **Modify programs affected by macro changes.** As with any software upgrade, you need to review any macro changes and update any user programs if they are affected.

8. **Add new services to the CICS wait list.** If you are using the CICS-ICSF Attachment Facility and you specify your own CICS wait list data set, you need to modify the wait list data set to include new services. See "ICSF: Add new services to the CICS wait list" on page 181.

Actions you might need to take once you are using a z990 or z890 server

When using ACTIVATE, adhere to the following rules:
- If z/OS V1R5 or later, or z/OS V1R4 with the z990 compatibility or exploitation code, is IPLed on a z990 or z890 server (or z/OS.e on a z890 server), then:

- You can perform a software ACTIVATE (the number of defined LCSSs is irrelevant).
- You can only perform a hardware ACTIVATE if the changed or new resources are restricted to LCSS 0.
- A power-on reset is required when adding or removing an LCSS, changing the maximum number of devices for an LCSS, adding or deleting LPARs, changing the name of an LPAR, and adding or changing a resource in an LCSS other than LCSS 0.

- If z/OS V1R5 or later, or z/OS V1R4 with the z990 compatibility or exploitation code, is installed, then you can perform full hardware or software ACTIVATE (regardless of the LCSS where the new or changed resources are defined).

Adhere to the following fallback rules:

- You cannot fall back to a software level that does *not* contain either the z990 compatibility or z990 exploitation code, and continue to run on a z990 or z890 server. This is particularly important if you do a MES upgrade or replace an existing server ("box swap" or "push/pull").
- Backing out of the software requires a backup copy and restoring to that level. SMP/E's RESTORE function cannot be used to remove the FMIDs provided with either z990 compatibility code or z990 exploitation code.
- Removing (restoring) either z990 compatibility code or z990 exploitation code from a system that will run on a G5, G6, z800, or z900 server will reintroduce sysplex coexistence considerations. That is, it will prohibit that system from participating in a sysplex with either an operating system image or coupling facility image on a z990 or z890 LPAR whose ID is greater than 15.
- Removing (restoring) the CFCC compatibility code from a G5, G6, z800, or z900 server will reintroduce sysplex coexistence considerations. That is, removing the CFCC compatibility support from a coupling facility image elsewhere in the sysplex will prohibit that coupling facility from participating in a sysplex with operating system or coupling facility images on a z990 or z890 with more than 15 LPARs defined on it (regardless of the number of LPARs that are activated).

Chapter 4. Sysplex migration actions

This chapter 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

Section title	Page or topic no.
Determine appropriate coupling facility structure sizes	71
Migrate to a z9-109 server	74
Migrate to a z990 or z890 server	74

Sysplex actions to perform before installing z/OS V1R7

Element or feature	Section title	Page or topic no.
Multiple	Install coexistence and fallback PTFs	4

Sysplex actions to perform before the first IPL of z/OS V1R7

Element or feature	Section title	Page or topic no.
BCP	Accommodate changes for coupling facility lock structures with record data	110
ICKDSF	Install ICKDSF R17 on systems that share DASD with a z9-109, z990, or z890 system	223
z/OS UNIX	Change NOAUTOMOVE to AUTOMOVE for sysplex-aware file systems	329
z/OS UNIX	Migrate from central BRLM support	330

Sysplex actions to perform after the first IPL of z/OS V1R7

Element or feature	Section title	Page or topic no.
DFSMSdfp	Ensure the integrity of SMS control data sets	204

Chapter 5. BCP migration actions

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

Some BCP data sets have been added to z/OS. See "Add references to new data
sets and paths" on page 53.

BCP actions to perform before installing z/OS V1R7

This section describes BCP migration actions that you can perform on your current
(old) system. You don't need the z/OS V1R7 level of code to make these changes,
and the changes don't require the z/OS V1R7 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 ever greater amounts of
main storage, you should evaluate whether the DASD allocated for your

stand-alone dump data continues to be adequate. z/OS V1R6 introduced support for extended format data sets that can use more than 64 K tracks per volume. If your stand-alone dump data sets are spread over more volumes than you desire, this support can help you gain better control over the number of volumes used for each stand-alone dump data set.

Element or feature:	BCP.
When change was introduced:	General migration action not tied to a specific release. Note that many enhancements related to this migration action have been incorporated in z/OS V1R7 and z/OS V1R6, with some of them rolled back to z/OS V1R4 by APARs.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
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.

Steps to take:

- 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 data sets with more than 64 K tracks per volume (after first IPL on z/OS V1R6 or later). Copy their contents to an extended-format, compressed, striped data set using the IPCS COPYDUMP subcommand prior to 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.
- Install the PTF for APAR OA08339 for performance enhancements.
- 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.

Reference information: For information about dump data set allocation, about extended format data sets that can use more than 64 K tracks per volume, and about multivolume dump data sets, see *z/OS MVS Diagnosis: Tools and Service Aids*.

Remove ECMB=NO from parmlib member IEAOPTxx

Description: On a z9-109, z990, or z890 server, when running z/OS V1R4 without the z/OS V1R4 z990 Exploitation Support feature, or earlier, CMB mode was enabled. This meant that storage obtained for the channel measurement block (CMB) was based on the number of DASD and tape devices and the CMB parameter of parmlib member IEASYS*xx*.

On a z9-109, z990, or z890 server, when running z/OS V1R4 with the z/OS V1R4 z990 Exploitation Support feature, z/OS V1R5, or z/OS V1R6, extended channel measurement block (ECMB) mode was enabled (instead of CMB mode) unless the ECMB=NO parameter was specified in parmlib member IEAOPT*xx*.

Now, in z/OS V1R7, on a z9-109, z990, or z890 server, ECMB mode is enabled unconditionally. The ECMB=NO parameter is no longer allowed. If you used this parameter before, remove it now.

Element or feature:	BCP.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4 with the z/OS V1R4 z990 Exploitation Support feature.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you use the ECMB=NO parameter of parmlib member IEAOPT*xx*.
Target system hardware requirements:	A z9-109, z990, or z890 server.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Steps to take: If you have ECMB=NO specified in parmlib member IEAOPT*xx*, convert user-written programs that use the CMB to use the ECMB, and contact ISVs to obtain updates to ISV programs that use the CMB. The type of programs that are most likely to use the CMB are monitor programs. Finally, remove your ECMB=NO specification.

Reference information: For details about coding parmlib parameters, including ECMB, see *z/OS MVS Initialization and Tuning Reference*.

Modify code that uses 1-byte console IDs

Description: z/OS V1R7 is planned to be the last release to support 1-byte console IDs. With z/OS V1R7, support for 1-byte console IDs and external interfaces supporting migration console IDs were removed from the WTO, WTOR, and MCSOPER macros, and from operator commands. Programs compiled using older versions of the macros will continue to work. In the release following z/OS V1R7, however, all 1-byte console ID support is planned to be completely removed.

A service called the Console ID Tracking Facility is available to help you identify 1-byte ID usage.

Element or feature:	BCP.
When change was introduced:	The Console ID Tracking Facility was introduced in the z/OS V1R4 Consoles Enhancements feature and subsequently integrated into z/OS V1R5. With z/OS V1R7, support for 1-byte console IDs and external interfaces supporting migration console IDs were removed from the WTO, WTOR, and MCSOPER macros, and from operator commands. In the release following z/OS V1R7, all 1-byte console ID support is planned to be completely removed.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	If you are running z/OS V1R4 with the Consoles Enhancement feature, or z/OS V1R5 or later, you can perform this migration action before installing z/OS V1R7. If you are running z/OS V1R4 without the Consoles Enhancement feature, you can perform this migration action after the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use any commands or APIs that reference 1-byte console IDs.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	If you don't modify code that uses 1-byte console IDs, either of two things can happen: • If you *don't* reassemble your code, it behaves the same as before and console messages are sent to the same place as before. • If you *do* reassemble your code, it will fail with a non-zero MNOTE and you will have to modify it.

Steps to take: Use the Console ID Tracking facility to identify 1-byte console ID usage, and then modify your code to use console names instead of the 1-byte IDs. The Console ID Tracking facility provides the following functions:

• The SETCON operator command, which is used to activate and deactivate the Console ID Tracking facility.

• The DISPLAY OPDATA,TRACKING operator command, which is used to display the current status of the Console ID Tracking facility, along with any recorded instances of violations.

• The CNIDTR*xx* parmlib member, which is used to list violations that have already been identified in order to prevent them from being recorded again. (A sample CNIDTR*xx* parmlib member is shipped in samplib as member CNIDTR00. For information about reporting instances to IBM or obtaining an updated CNIDTR*xx* parmlib member, see informational APAR II13752.)

Reference information: For more information about the Console ID Tracking facility, see *z/OS MVS Planning: Operations*.

Decide how many CPUs to bring online at IPL

Description: Before z/OS V1R7, the number of CPUs and IFAs brought online at IPL was the number defined in the initial processor counts for the logical partition profile. This was the case in z/OS V1R6 and z/OS V1R5, and in z/OS V1R4 with PTF UA03339 installed (for APAR OA03335), when running on a zSeries server (if a z900 server, GA-3 or later level).

As of z/OS V1R7, you have the option of bringing online at IPL all CPUs and IFAs that were online at the end of the prior IPL (provided that specific actions are taken, as described below). This option is also furnished back to z/OS V1R4 by APAR OA09649.

Element or feature:	BCP.
When change was introduced:	z/OS V1R7 and rolled back to z/OS V1R4 by PTFs for APAR OA09649.
Applies to migration from:	• z/OS V1R6 • z/OS V1R5 • z/OS V1R4 with PTF UA03339 installed (for APAR OA03335)
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes.
Target system hardware requirements:	A z9-109 or zSeries server (if a z900 server, GA-3 or later level).
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	CPUs that are offline when an IPL is initiated remain offline. You might want to avoid using the PRESCPU parameter (described in "Steps to take" below) when WLM CPU management is active, because that processing might have configured CPUs offline.
System impacts:	None.

Steps to take: If you want the number of CPUs and IFAs brought online at IPL to be the number defined in the initial processor counts for the logical partition profile, no action is required.

If you want the CPUs and IFAs brought online at IPL to be the same CPUs and IFAs that were online at the end of the last IPL, then install the PTF for OA09649 (which is integrated into z/OS V1R7) and use the PRESCPU parameter for parmlib member IEASYS*xx*. The PRESCPU parameter causes the system to ignore the number of initial CPUs and IFAs that PR/SM provides and bring logically online all CPUs and IFAs that the machine presents as physically online.

Reference information:
• For information about bringing CPUs online, see *z/OS MVS Planning: Operations*.

Prepare to use synchronous reserve in GRSCNF*xx*

Description: Before z/OS V1R6, the default value for the SYNCHRES (synchronous reserve) statement on the GRSCNF*xx* (global resource serialization configuration) parmlib member was NO. Beginning with z/OS V1R6, the SYNCHRES statement defaults to YES to ensure that synchronous processing is activated at all times. This new default prevents deadlocks between systems sharing DASD, which could occur when there is a delay between the time a request is made to reserve a volume and the time when the reserve of the volume is obtained.

Because of the importance of synchronous reserve processing, a check for SYNCHRES=YES is included in the IBM Health Checker for z/OS to warn you if the default is not used.

Element or feature:	BCP.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	No, but recommended to prevent deadlocks when reserving volumes.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	SYNCHRES=YES might increase RESERVE request time.

Steps to take: Examine your current settings to determine what is specified in the GRSCNF*xx* parmlib member. Then take the following action:

- If SYNCHRES=YES is specified, remove it because YES is now the default.
- If SYNCHRES=NO is specified, determine why, and take the necessary action to use the new default of YES.
    - If NO was the prior default, remove the SYNCHRES statement so the system defaults to YES.
    - If NO was specified for an application's performance purposes in a STAR environment, convert the application's RESERVE requests to global ENQs. For RESERVE conversion, see *z/OS MVS Planning: Global Resource Serialization*.
    - If NO was specified for an application's performance purposes in a RING environment, remove SYNCHRES=NO because the synchronous reserve overhead is minimal. For RESERVE conversion, see *z/OS MVS Planning: Global Resource Serialization*.
    - If NO was specified for other application purposes, change the application to use ISGENQ SYNCHRES=NO. This affects only the RESERVE requests for this application. For more information about ISGENQ, see *z/OS MVS Programming: Assembler Services Reference IAR-XCT*.

To change the default for all systems before migrating to z/OS V1R7, use the SETGRS operator command. Specify SYNCHRES=YES and then update shared parmlib member GRSCNF*xx* to specify SYNCHRES=YES.

Tip: The IBM Health Checker for z/OS provides an automated way to check your system's active configuration for conditions that can affect your system's availability and for values that should be configured for best practices. This tool provides several global resource serialization checks, including a check to see if global resource serialization with synchronous reserve processing is enabled. Before z/OS V1R7, this tool was provided as a Web deliverable and as part of base element msys for Operations. As of z/OS V1R7, it's integrated into the BCP base element. To read how to use it, see *IBM Health Checker for z/OS: User's Guide*.

Reference information:
- For details about the GRSCNF*xx* parmlib member, see *z/OS MVS Initialization and Tuning Reference*.
- For information about the synchronous RESERVE feature of global resource serialization, such as how to convert RESERVEs to GLOBAL ENQs, see *z/OS MVS Planning: Global Resource Serialization*.
- For information about the ISGENQ macro, see *z/OS MVS Programming: Assembler Services Reference IAR-XCT*.

Make updates for console enhancements

Description: The z/OS V1R4 Consoles Enhancements feature was the first deliverable in the new zSeries console strategy, which is intended to enhance the operator messaging architecture of z/OS. The feature focuses on minimizing the possibility of outages due to exhaustion of system resources used for messaging. As of z/OS V1R5, the function is rolled into the base product and is no longer an optional feature. Several tasks that were formerly best practices are now required, and some functions are no longer relevant.

Element or feature:	BCP.
When change was introduced:	Consoles Enhancements was introduced as a feature of z/OS V1R4 and subsequently integrated into z/OS V1R5.
Applies to migration from:	z/OS V1R4 without the Consoles Enhancements feature.
Timing:	Before installing z/OS V1R7.
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.

Steps to take:
- Name your consoles. Check your CONSOL*xx* parmlib members to ensure that each of the CONSOLE statements specifies a NAME parameter. (Naming is not necessary for the system console.)

- Check your CONSOL*xx* members to ensure that each of the CONSOLE statements specifies the ALTGRP keyword rather than the ALTERNATE keyword. Console switch ALTERNATE processing is no longer supported.

- Remove the UD (undelivered messages) keyword from the CONSOLE statement in member CONSOL*xx*; it is no longer supported. This keyword will not be honored on system commands.

- Instead of using a device for hardcopy, use the system log (SYSLOG), the operations log (OPERLOG), or both, because hardcopy can no longer be directed to a device. Also, remove the DEVNUM (device number) and HCPYGRP (hardcopy group) keywords from the HARDCOPY statement in member CONSOL*xx*; they are no longer supported.

- Do not use the R (reroute message queue) parameter on the CONTROL Q command; it is no longer supported. The command will remove a message backlog from the target console only. You cannot redirect messages to another console.

- Make sure that the MAXCAD value that you have defined (or defaulted to) in IEASYS*xx* is large enough to accommodate the three new common area data spaces (CADs) created by the Consoles Enhancements. For a complete list of SCOPE=COMMON data spaces that were added, and that might impact your MAXCAD specification, see "Accommodate new SCOPE=COMMON data spaces" on page 61.

Note: The MSCOPE parameter on the CONSOLE statement for the system console in CONSOL*xx* now defaults to * instead of *ALL. (* means that a console only receives messages from the local system. *ALL means that a console receives messages from local **and** other systems in the sysplex.) IBM recommends that you use the new default setting. However, while this change is related to consoles, it is not part of the new console strategy, so accepting the new default is not a requirement.

Reference information: *z/OS MVS Planning: Operations*.

BCP actions to perform before the first IPL of z/OS V1R7

This section describes BCP migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't 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.

Element or feature:	BCP.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

Steps to take: 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*.

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

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. Once the stand-alone dump program is properly created on a DASD residence volume, it resides in the SYS1.PAGEDUMP.Vvolser data set.

Element or feature:	BCP.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

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

Update programs that use SMF record type 88, subtype 1

Description: Because the Events section (SMF88ESD) of SMF record type 88, subtype 1 has increased in size, offset values to some sections have changed. Any programs that use an explicit offset from the beginning of the SMF88 record to a field in the following section might need to be updated:

Section	Related offset	Related DSECT
Structure (interim storage)	SMF88SOF	SMF88SSD

Element or feature:	BCP.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you run any programs that use explicit offsets from the beginning of the SMF88 record to the section in the table above.
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: Check any programs that use the section listed above to determine if you must make any changes. If necessary, modify the programs using the updated offsets.

Reference information:

- For details about SMF record type 88, subtype 1, see *z/OS MVS System Management Facilities (SMF)*.
- For examples of the correct offsets to use in the sort step when using SMF record type 88, subtype 1 records, see SYS1.SAMPLIB members IXGRPT1 and IXGRPT1J.

Discontinue use of the TRACK and related commands

Description: As of z/OS V1R7, the TRACK command has been removed from z/OS. Operators can no longer issue the TRACK command to display job information on an MCS or SMCS console. In addition, other commands that deal exclusively with the TRACK command have also been removed. These commands are:
- TRACK
- STOPTR
- CONTROL T (K T)
- CONTROL D,H (K D,H)
- CONTROL D,U (K D,U)
- MR TR={a,name-a}

Because CONTROL T was removed, there is no longer a need to specify the UTME value for an MCS or SMCS console in CONSOL*xx*. Therefore, the UTME keyword is no longer accepted in CONSOL*xx*.

Element or feature:	BCP.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.

Is the migration action required?	Yes, if you use the TRACK command or any of the related commands listed in "Description" above.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	Pre-z/OS V1R7 systems can still issue the TRACK command but they cannot direct TRACK displays with the MSGRT command to z/OS V1R7 or later systems.
Restrictions:	None.
System impacts:	None.

Steps to take:

- Notify operators that the TRACK command and associated commands should not be issued.
- Modify any automated procedures to eliminate the use of the TRACK command and associated commands.
- Remove the UTME keyword from the CONSOL*xx* member of parmlib.

Reference information: For more information about the removal of the TRACK command, see *z/OS MVS Planning: Operations*.

Update ENF listen exits that make use of logger ENF48 signals

Description: Programs that exploit system logger services are impacted if they need to process logger ENF48 log stream events.

Element or feature:	BCP.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use IXGENF mapping or listen for ENF signal 48.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	The PTF for APAR OA08661 that is appropriate to your release.
Restrictions:	None.
System impacts:	None.

Steps to take: Programs that listen to ENF signal 48 (ENFPC048) for any of the following logger events need to be changed to additionally listen for the new ENF information:

- *Background:* After the last disconnect to a log stream on a system that is not disconnected due to other reasons (such as Force or XES recommendation), an IxgenfLogStreamConnDisc event is issued with new event reason IxgEnfSystemLevelDisc, and the connection count of remaining systems connected to the log stream is given (IxgEnfConnDiscCount). The affected log stream no longer has connections on this system.

What to do: Change programs to take into account new event reason IxgenfSystemLevelDisc and the connection count IxgenfConnDiscCount.

- *Background:* After a successful SETLOGR FORCE,DISCONNECT command operation, existing event IxgEnfLogstreamsNotAvailable is issued with new event reason IxgEnfSetLogrForceDisconnect along with existing event specific information IxgEnfLogstreamDisconnected. This means that the affected log stream has lost all of its connections on this system.

  What to do: Change programs to take into account new event reason IxgenfSetLogrForceDisconnect for specific reason IxgenfLogstreamDisconnected.

- *Background:* After a successful SETLOGR FORCE,DELETE command operation, existing event IxgenfLogStreamDelete is issued with new event reason IxgEnfSetLogrForceDelete. This means that the log stream referred to by field IxgenfInventoryDelLogStreamName has been deleted from the LOGR couple data set as a result of the command request.

  What to do: Change programs to take into account new event reason IxgenfSetLogrForceDelete.

Reference information: For more information about the updates to logger event 48 signaling, see *z/OS MVS Programming: Authorized Assembler Services Guide* and *z/OS MVS Data Areas, Vol 3 (IVT-RCWK).*

Evaluate the MAXMSG value in COUPLExx

Description: The MAXMSG parameter in parmlib member COUPLE*xx* specifies a value that XCF uses to determine the allotment of message buffers when the MAXMSG parameter is not specified on any one of following:

- The CLASSDEF statement
- The PATHIN statement
- The SETXCF START,CLASSDEF command
- The SETXCF START,PATHIN command

Before z/OS V1R7, the default value for MAXMSG was 750. As of z/OS V1R7, the default value for MAXMSG has been increased to 2000.

Element or feature:	BCP.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you specified a value for MAXMSG that is less than the default value of 2000.
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: Examine the MAXMSG setting in the COUPLE*xx* parmlib member. If a value of less than 2000 is specified, either change it to a value greater than 2000 or accept the default value.

A check for the value of MAXMSG has been added to the IBM Health Checker for z/OS to warn you if the MAXMSG value is less than the default.

Reference information: For details about specifying the MAXMSG parameter in COUPLE*xx*, see *z/OS MVS Initialization and Tuning Reference*.

Migrate to, or start using, the IBM Health Checker for z/OS

Description: The IBM Health Checker for z/OS can identify potential problems before they impact system availability or cause outages. It checks the current active z/OS and sysplex settings and definitions for a system and compares the values to those suggested by IBM or defined by you. The open architecture of the framework supports checks written by IBM, ISVs, and users.

Before z/OS V1R7, a prototype, called the IBM Health Checker for z/OS and Sysplex, was available from the Web. As of z/OS V1R7, the code is delivered as part of base element BCP, functionality is improved, the name is shorted to IBM Health Checker for z/OS, and ServerPac provides jobs and performs procedures to set up the IBM Health Checker for z/OS framework.

Whether or not you previously used the prototype, you should now set up and use the version that comes with z/OS V1R7.

Element or feature:	BCP.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended in order to prevent potential problems that could impact system availability and cause outages.
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:

- If you are currently using the prototype, you should migrate to the IBM Health Checker for z/OS that is integrated in z/OS V1R7. There are no incompatibilities between the prototype and the IBM Health Checker for z/OS framework; they can run in parallel. However, implementation of the IBM Health Checker for z/OS is strongly recommended and provides significant improvements in functionality compared to the prototype. For instructions on migrating from the prototype to the IBM Health Checker for z/OS, see *IBM Health Checker for z/OS: User's Guide*.
- If you did not use the prototype, it is recommended that you use the IBM Health Checker for z/OS that has been integrated in z/OS V1R7. If you install with ServerPac, the setup is performed for you. If you do not install with ServerPac, you must perform all the setup steps. See *IBM Health Checker for z/OS: User's Guide* for instructions on setting up IBM Health Checker for z/OS.

- If you choose not to use the IBM Health Checker for z/OS, review the ServerPac-supplied jobs and procedures to remove the COM='START hzsproc' statement from the sample COMMND*xx* member provided with your order.

Reference information:
- For information about migration actions from the prototype, and for steps to complete setting up the IBM Health Checker for z/OS, see *IBM Health Checker for z/OS: User's Guide*.
- For information about the jobs and procedures performed by ServerPac, see *ServerPac: Installing Your Order*.

Update JCL that refers to the AMDSADDD utility

Description: Before z/OS V1R7, the AMDSADDD REXX utility, which allocates stand-alone dump data sets, was located in data set SYS1.SAMPLIB. In z/OS V1R7, as part of the enhancement to the IPCS 3.6 option that helps you create stand-alone dump data sets, AMDSADDD has been moved to SYS1.SBLSCLI0. If you have JCL that refers to AMDSADDD, update it to point to the new location.

Element or feature:	BCP.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have any JCL that refers to the AMDSADDD utility.
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: Update JCL that points to the AMDSADDD utility in SYS1.SAMPLIB to now point to SYS1.SBLSCLI0.

Reference information: For details about using the AMDSADDD utility, see *z/OS MVS Diagnosis: Tools and Service Aids*.

Remove CUNUNI*xx* parmlib members when Unicode is used for TCB callers

Description: As of z/OS V1R7, enhancements made to z/OS support for the Unicode Standard no longer require you to run the image generator program to create a conversion image and to customize the CUNUNI*xx* parmlib members with that conversion image name. As of this writing, these enhancements are made only for those callers that run in TCB mode. SRB mode callers, such as DB2, are not included in this support at this time.

All tables needed for character conversion, case conversion, normalization, and collation services are now loaded automatically when they are required and not already present in storage. The only failure that will occur is when an invalid or unsupported conversion or service is specified.

The conversion image generator program, CUNMIUTL, is still being shipped, and existing and new conversion images are still supported. If you want to continue to specify CUNUNI*xx* parmlib members, the conversion images will still be loaded into storage. The prebuilt conversion image that was added for DB2 support when Unicode services had not been set up, CUNIDHC2, is still loaded under the same conditions that it was before z/OS V1R7.

Element or feature:	BCP.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended to help avoid confusion in the future by anyone who encounters Unicode parmlib members and is unaware that they are no longer necessary.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	This support is only available starting with z/OS V1R7. If you share a parmlib between z/OS V1R7 and prior levels, the CUNUNI*xx* parmlib members still need to be made available to the pre-z/OS V1R7 systems.
Restrictions:	None.
System impacts:	None.

Steps to take: When Unicode services are used for callers that run in TCB mode, you no longer need to provide parmlib members CUNUNI*xx*. You can delete them. Remember also to remove your UNI= references in any IEASYS*xx* parmlib members. New operator commands (SETUNI ADD, SETUNI DELETE, SETUNI REPLACE, and SETUNI REALSTORAGE) are provided to manipulate conversion images and Unicode settings.

At the time of this writing, if Unicode services are used for callers that run in SRB mode (for instance, DB2), the CUNUNI*xx* parmlib member must remain.

Reference information:

- For information about using z/OS support for the Unicode Standard, see *z/OS Support for Unicode: Unicode Services*.
- For the new Unicode operator commands, see *z/OS MVS System Commands*.

Modify programs and capacity settings because of improved subcapacity reporting for native z/OS systems

Description: The Subcapacity Reporting Tool (SCRT), available to customers who take advantage of subcapacity pricing, makes use of the four-hour rolling average provided by workload manager (WLM).

Before z/OS V1R7, WLM provided a four-hour rolling average that was calculated using the total dispatch time of all logical CPs of the running LPAR. Whether wait time was included in the dispatch time was dependent on the LPAR configuration, as follows:

- *For dedicated CPs:* The dispatch time included the total wait time for all logical CPs of the LPAR.
- *For shared CPs defined with Wait Completion = Yes:* The dispatch time included the total wait time for all logical CPs of the LPAR.
- *For shared CPs defined with Wait Completion = No:* The dispatch time included no wait time for any logical CPs of the LPAR.

As of z/OS V1R7, WLM no longer includes wait time in the four-hour rolling average calculation for LPAR configurations involving dedicated CPs or shared CPs defined with Wait Completion = Yes. This results in an accurate reflection of the busy time for the system or systems running in the LPAR.

Because of the calculation change, some data areas and SMF records have changed. You should examine any programs that rely on the changed data areas and SMF records, and modify them appropriately. Also, you should reanalyze your installation-defined capacity settings.

Element or feature:	BCP.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have any programs that use affected interfaces described in "Steps to take" below.
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: Update your programs to take into account the following changes to data areas:

- *Field RCTLACS in data area IRARCT:* This field no longer includes CP wait time for systems running in LPAR mode, that is, (1) dedicated CPs and (2) shared CPs defined with Wait Completion = Yes. If you have programs that inspect RCTLACS, you might need to change them.
- *Field RCTFLAG1_LACS_RCU in data area IRARCT:* As of z/OS V1R7, this field is always turned on. When this field is turned on, it means that RCTLACS no longer includes CP wait time, as described above.
- Data area IRALPDAT is returned by SYSEVENT REQLPDAT. Field changes are:
  - *Field LPDatAvgImgService:* Because this field is a copy of the RCTLACS field, it no longer includes CP wait time for systems running in LPAR mode, that is, (1) dedicated CPs and (2) shared CPs defined with Wait Completion = Yes. If you have programs that inspect LPDatAvgImgService, you might need to change them.
  - *Field LPDatVer:* As of z/OS V1R7, a value of 2 in LPDatVer indicates the design change. This means that LPDatAvgImgService no longer includes CP wait time, as described above.

Update your programs to take into account the following changes to SMF records:

- *SMF record type 70, subtype 1, field SMF70LAC:* SMF70LAC no longer includes CP wait time for systems running in LPAR mode, that is, (1) dedicated CPs and (2) shared CPs defined with Wait Completion = Yes. If you have programs that inspect SMF70LAC, you might need to change them.
- *SMF record type 70, subtype 1, bit 3 of byte SMF70STF (SMF70RCU):* As of z/OS V1R7, SMF70RCU is always turned on. When SMF70RCU is turned on, it means that SMF70LAC no longer includes CP wait time, as described above.

If you have processors defined as dedicated CPs or as shared CPs defined with Wait Completion = Yes, reanalyze your installation-defined capacity settings. Defined capacity control is now based on actual consumed CP time and is no longer based on dispatch time for shared CPs defined with Wait Completion = Yes. As a result, you might need to lower your installation-defined capacity controls. Note that there is no need to adjust your installation-defined capacity controls for processors defined with shared CPs defined with Wait Completion = No, because wait time has never been included in the four-hour rolling average for shared CPs defined with Wait Completion = No.

Note: SCRT V5R1 provides interim support to remove wait time for configurations involving dedicated CPs. SCRT V6R1 provides interim support to remove wait time for configurations involving shared CPs defined with Wait Completion = Yes. As of z/OS V1R7, WLM formally calculates the four-hour rolling average without wait time and makes those values available to the SCRT. Because earlier versions of the SCRT removed the wait time, where appropriate, when calculating the four-hour rolling average, this z/OS V1R7 WLM change does not affect customer use of the SCRT tool itself or what SCRT reports to IBM when these type of LPAR configurations are used. However, you still need to evaluate whether the data area and SMF changes above affect programs that you have.

Reference information:

- For details about data area IRALPDAT, see *z/OS MVS Data Areas, Vol 2 (DCCB-ITZYRETC)*.
- For details about SMF records, see *z/OS MVS System Management Facilities (SMF)*.

Modify programs because of improved subcapacity reporting for z/OS guests of z/VM

Description: Before z/OS V1R7, when z/OS ran as a guest of z/VM, the Subcapacity Reporting Tool (SCRT) would report product millions of service units (MSUs) for z/OS and other subcapacity eligible z/OS products based on the maximum capacity of the LPAR in which the z/OS VM guest or guests ran.

As of z/OS V1R7, WLM is enhanced to provide better subcapacity reporting granularity for z/OS V1R7 guests of z/VM. With the enhancements made to WLM in z/OS V1R7 and SCRT V10R3, the product MSUs are based on an actual four-hour rolling average of the z/OS V1R7 z/VM guest or guests, rather than the maximum capacity of the LPAR in which the z/OS z/VM guest or guests ran. This might result in lower IBM software charges for customers who are eligible for subcapacity pricing and who run images of z/OS as a guest of z/VM. In order to obtain the benefits of this support, all z/OS guests of z/VM running on a z9-109 or zSeries processor must be at the level of z/OS V1R7 or later, and use the proper level of the SCRT tool (SCRT V10R3 or later).

Because of the improvement in subcapacity reporting granularity, some data areas and SMF records have changed. You should examine any programs that rely on the changed data areas and SMF records, and modify them appropriately.

Note: In the following z/OS z/VM guest environments, the SCRT continues to report on product MSUs based on the maximum capacity of the LPARs in which the z/OS z/VM guests run:

- z/OS z/VM guest environments that have a mix of z/OS V1R7 (and later) and z/OS V1R6 (and earlier) running on the same z9-109 or zSeries processor
- z/OS z/VM guest environments that have one or more z/OS V1R6 (and earlier) images running on the same z9-109 or zSeries processor

Element or feature:	BCP.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you are running z/OS as a VM guest and all VM guests are at the z/OS V1R7 level, and you have programs that use the interfaces described in "Steps to take" below.
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: Update your programs to take into account the following changes to data areas:

- *Field RCTFLAG1_LACS_RCU in data area IRARCT:* As of z/OS V1R7, this field is always turned on. When this field is turned on, it means that RCTLACS provides a rolling four-hour average utilization for z/OS guests running in LPAR mode. (See "Steps to take" in "Modify programs and capacity settings because of improved subcapacity reporting for native z/OS systems" on page 105 for other conditions in which this field is turned on.)
- *Field LPDatAvgImgService in data area IRALPDAT:* This field is returned by SYSEVENT REQLPDAT. Because this field is a copy of the RCTLACS field, it can now contain a four-hour rolling average for z/OS guests running in LPAR mode. If you have programs that inspect LPDatAvgImgService, you might need to change them.
- *Field LPDatVer:* As of z/OS V1R7, a value of 2 in LPDatVer indicates the design change. This means that the LPDatDefCapData section in IRALPDAT is now available for z/OS guests running in LPAR mode. (See "Steps to take" in "Modify programs and capacity settings because of improved subcapacity reporting for native z/OS systems" on page 105 for other conditions in which this field is turned on.)

Update your programs to take into account the following change to an SMF record:

- *SMF record type 70, subtype 1, bit 3 of byte SMF70STF (SMF70RCU):* As of z/OS V1R7, SMF70RCU is always turned on. When SMF70RCU is turned on, it

means that SMF70LAC now provides rolling four-hour average utilization for z/OS guests running in LPAR mode. (See "Steps to take" in "Modify programs and capacity settings because of improved subcapacity reporting for native z/OS systems" on page 105 for other conditions in which this field is turned on.)

Note: You must evaluate whether the data area and SMF changes above affect you, regardless of whether you are eligible for subcapacity pricing.

Reference information:

- For additional information about the WLM enhancement that provides better subcapacity reporting granularity for z/OS V1R7 guests of z/VM, see *Using the Subcapacity Reporting Tool* ("SCRT User's Guide") available from http://www.ibm.com/servers/eserver/zseries/swprice/scrt/.
- For details about data area IRALPDAT, see *z/OS MVS Data Areas, Vol 2 (DCCB-ITZYRETC)*.
- For details about SMF records, see *z/OS MVS System Management Facilities (SMF)*.

Update programs that use SMF record type 90, subtypes 5, 9, 13, and 15

Description: Because the IPL SMF/SET SMF/SETSMF section of SMF record type 90, subtypes 5, 9, 13, and 15 has increased in size, offset values to some sections have changed. Any programs that use an explicit offset from the beginning of the SMF90 record to a field in any of the following sections might need to be updated:

Section	Related offset	Related DSECT
SMF data set	SMF90ODA	SMF90DSE
Subsystem record	SMF90OWK	SMF90WCH
Subsystem parameter	SMF90OOT	SMF90SUB

Element or feature:	BCP.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you run any programs that use explicit offsets from the beginning of the SMF90 record to any of the sections in the table above.
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: Check any programs that use any of the sections listed above to determine if you must make any changes. If necessary, modify the programs using the updated offsets.

Reference information: For details about SMF record type 90, subtypes 5, 9, 13, and 15, see *z/OS MVS System Management Facilities (SMF)*.

Accommodate changes for coupling facility lock structures with record data

Description: z/OS V1R4 and APAR OW52437 introduced performance improvements for lock structures with record data in a system-managed coupling facility structure duplexing environment. Coexistence for the improvements is available for systems in the sysplex through APAR OW52266. The performance improvements could increase the size of an existing lock structure; perhaps an additional 300 KB of space in the coupling facility might be required. Currently allocated lock structures with record data must be reallocated through the rebuild process to acquire the additional storage in preparation for system-managed coupling facility structure duplexing.

Element or feature:	BCP.
When change was introduced:	• z/OS V1R2 by PTF UW92528 for APAR OW52437 • z/OS V1R3 by PTF UW92529 for APAR OW52437 • z/OS V1R4 by PTF UW92530 for APAR OW52437
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if all of the following are true: • You allocate lock structures with record data in your coupling facility. • You have not yet installed PTF UW92530 on your z/OS V1R4 system. • You have not yet performed the actions listed in "Steps to take" below.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	z/OS V1R4 PTF UW92486 (for APAR OW52266).
Restrictions:	None.
System impacts:	None.

Steps to take: To provide coexistence (by APAR OW52266) for the performance improvements introduced in APAR OW52437 and incorporated into z/OS V1R5 and later, take the following steps. Note that these steps might already have been performed if coexistence PTF UW92486 (on z/OS V1R4) has been installed:

1. Install PTF UW92486 for APAR OW52266 on all z/OS V1R4 systems in the sysplex.
2. Use the CFSIZER tool to determine the appropriate size for all lock structures except ISGLOCK. (The ISGLOCK structure cannot exploit the new performance enhancements because the structure does not contain record data.) You can find the CFSIZER tool at http://www.ibm.com/servers/eserver/zseries/cfsizer/.
3. Update the CFRM policy to specify the new lock structure size requirements.

To enable the functions provided in OW52437 and incorporated into z/OS V1R5 and later, take the following steps. Note that these steps can only be performed after the PTF for APAR OW52437 or z/OS V1R6 (or later) has been installed:

1. Install PTF UW92530 on z/OS V1R4 and install z/OS V1R7.

2. After coexistence PTF UW92486 (for APAR OW52266) has been installed and activated on all z/OS V1R4 systems in the sysplex, IPL z/OS V1R4 with PTF UW92530 installed or IPL z/OS V1R7.

3. Initiate a rebuild of all lock structures except ISGLOCK to activate the performance enhancements with multiple record data lists.

4. When the rebuild completes, issue the DISPLAY XCF,STR command to verify that the structure has been allocated with multiple record data lists and is ready for system-managed coupling facility structure duplexing. If the result is successful, message IXC360I will contain the insert:

```
NUMBER OF RECORD DATA LISTS PER CONNECTION: nnn
```

If this message insert does not appear, the structure was allocated by a system that does not have the support provided by APAR OW52437 and incorporated into z/OS V1R5 and later.

Reference information:
- *z/OS MVS Setting Up a Sysplex*
- *z/OS MVS System Messages, Vol 10 (IXC-IZP)*

BCP actions to perform after the first IPL of z/OS V1R7

This section describes BCP migration actions that you can perform only after you've IPLed z/OS V1R7. You need a running z/OS V1R7 system to perform these actions.

Accept the UCB overlay detection default change

Description: The unit control block (UCB) is a critical control structure in z/OS that designates the state and definition of an I/O device. Since MVS/ESA™ SP 5.2.0, applications could capture a UCB into a private virtual address. This implies that application programs could inadvertently overlay this storage and cause the real UCB contents to be overlaid, resulting in system outages. In z/OS V1R5, the input/output supervisor (IOS) was enhanced to provide read-only views for all captured UCB requests. However, you had to use an IBM internal option in DIAG*xx* to enable IOS to provide the views. In z/OS V1R7, this overlay protection mechanism is enabled by default to help prevent UCB overlays.

Element or feature:	BCP.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended to detect UCB overlays before they happen.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.

System impacts:	If a program attempts to write into storage that represents a captured UCB, a protection check abend occurs. It is the responsibility of the abending program to recover from this appropriately. Programs that wish to store into a UCB must do so using the actual UCB address and not a captured view. Obtaining the actual UCB address can be done using services provided by IOS.

Steps to take: You need do nothing to take the recommended action, which is to accept the UCB overlay detection default change. By default, z/OS V1R7 systems come up with UCB overlay protection enabled.

During operation of your system, if you encounter UCB overlays and dumps, report them to the software vendor or program owner. If you need to disable the system level trap (and thereby stop detecting UCB overlays), you can do so with either of the following methods:

- By command: `SETIOS CAPTUCB,PROTECT=NO`
- By IECIOS*xx* parmlib member: `CAPTUCB,PROTECT=NO`

Reference information:

- For details about the SETIOS command, see *z/OS MVS System Commands*.
- For details about the IECIOS*xx* parmlib member, see *z/OS MVS Initialization and Tuning Reference*.

Review the IXLLOCK hash algorithm

Description: Before z/OS V1R7, the number of XES connections to serialized structures (lock and serialized list structures) was limited to 64 structures per address space. This limit related to the number of connector-owned data spaces that can reside on an address space's PASN access list. With z/OS V1R7, the system obtains additional data spaces for each lock structure and spreads resource information across the data spaces based on the lock hash value specified on IXLLOCK requests.

Element or feature:	BCP.
When change was introduced:	z/OS V1R7 (and rolled back to z/OS V1R6, z/OS V1R5, and z/OS V1R4 by APAR OA03194).
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4, without the PTF for APAR OA03194 installed.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if your applications use coupling facility lock structures.
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: Review the hash algorithm used by your application to ensure that the algorithm produces hash values that are evenly distributed on the low-order digit of the result.

Reference information: For details about specifying IXLLOCK requests, see *z/OS MVS Programming: Sysplex Services Reference* and *z/OS MVS Programming: Sysplex Services Guide*.

Update operator procedures for certain changed MVS commands

Description: Before z/OS V1R7, certain MVS commands produced results that are different from what occurs in z/OS V1R7:

- The START DEALLOC command was used to redrive pending offline processing, often as an automated procedure. As of z/OS V1R7, the pending offline process is a timer-driven process and a redrive procedure is not required by the installation.
- Before z/OS V1R7, when message IEF238D was issued, VARY OFFLINE processing for a device could not complete until the operator responded to the message. The device entered a pending offline state (message IEF524I) and remained so for 15 minutes, at which point message IEF525E was issued and repeated at 15 minute intervals until either a response was provided or the job was canceled. As of z/OS V1R7, when message IEF238D is issued, VARY OFFLINE processing is not initiated until the message is replied to. Messages IEF524I and IEF525E are not issued until the VARY OFFLINE processing is started. Devices that were already in a pending offline state before message IEF238D was issued can be processed.

  Also, prior to the improvements in VARY OFFLINE processing in z/OS V1R7, when an operator responded to message IEF238D (Recovery Allocation) with a device number that was "pending offline", the device would remain "pending offline" after the device was unallocated (that is, when the job was finished with it). As of z/OS V1R7, it is likely that the device will go offline before the Recovery Allocation process can bring it online. Therefore, the device will no longer be marked "pending offline" after the allocation completes. You must reissue the VARY command to bring the device offline.

- Previously, when a device was "pending unload" because of being allocated when an UNLOAD command was issued, the device would remain "pending unload" after the device was unallocated (that is, when the job was finished with it). As of z/OS V1R7, because of changes in UNLOAD processing, if a volume is mounted on a device and the device is allocated, the system passes responsibility for unloading the device to the job that allocated it. The pending unload process will complete with message IEF415I.

Element or feature:	BCP.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you expect certain results from issuing any of the following MVS commands: • START DEALLOC • VARY OFFLINE • UNLOAD
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: Update your operator procedures to allow for the changed behavior of these commands.

Reference information: For details about the specified commands, see the following topics in *z/OS MVS System Commands*:
- START DEALLOC
- VARY OFFLINE
- UNLOAD

Update IPCS subcommands that require the ERROR criterion to select ASIDs

Description: Before z/OS V1R7, most IPCS subcommands that support ASID selection criteria defaulted to both CURRENT and ERROR ASIDs. As of z/OS V1R7, the default for address space selection has been changed to solely the CURRENT option. If you have specific IPCS procedures that benefit from using the ERROR option to select ASIDs, update those procedures to explicitly request the option.

Element or feature:	BCP.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have IPCS procedures that require the ERROR criterion to select ASIDs.
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: Update appropriate IPCS procedures to explicitly request the ERROR option to select ASIDs.

Reference information: For details about issuing IPCS subcommands, see *z/OS MVS IPCS Commands*.

Check the maximum number of XES connectors per address space

Description: Before z/OS V1R7, the number of XES connections to a serialized coupling facility structure (lock or serialized list) was limited to 64 per address space. With z/OS V1R7, the limit is reduced to approximately 6 lock structure connections per address space. This reduction is due to the increase in the number of data spaces owned by connectors to coupling facility lock structures. The limit for connections to serialized list structures is not changed; however, if an address

space uses connections to both lock and serialized list structures, the extra use of data spaces by the lock structure will reduce the availability of data spaces for the serialized list structure. Also, connections that support user-managed structure rebuild use double the number of data spaces, thus reducing the maximum connector limit even more.

Element or feature:	BCP.
When change was introduced:	z/OS V1R7 (and rolled back to z/OS V1R6, z/OS V1R5, and z/OS V1R4 by APAR OA03194).
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4, all without the PTF for APAR OA03194 installed.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you support connections to serialized coupling facility structures.
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: Review the use of serialized coupling facility structures per address space. If the number of connectors to lock structures from any one address space exceeds about six, reduce the number of connectors. If the connectors are associated with applications written by you, restructure the applications to connect from multiple address spaces. If the connectors are associated with vendor applications, contact the owning vendors.

Reference information:
- For details about specifying the MAXCAD parameter of IEASYS*xx*, see *z/OS MVS Initialization and Tuning Reference*.
- For details about specifying the IXLCONN macro to connect to a coupling facility structure, see *z/OS MVS Programming: Sysplex Services Reference*.
- For details about adjusting the value of the MAXCAD parameter in IEASYS*xx* to accommodate all new data spaces, including those required for serialized coupling facility structures, see "Accommodate new SCOPE=COMMON data spaces" on page 61.

Correct programs that issue erroneous WTO or WTOR messages

Description: Before the z/OS V1R4 Consoles Enhancements feature, you could create WTO and WTOR parameter lists that were invalid, yet the WTO and WTOR service would accept them with a zero return code and no abend. An example is invalid parameter combinations. In some cases the message would be partially displayed, but in other cases the message might not be displayed at all or would result in system errors.

Effective with the z/OS V1R4 Consoles Enhancements feature, the WTO and WTOR services provide stronger parameter list checking to prevent errors. In most cases, the WTO and WTOR services now record any errors as symptom records in the logrec data set and issue a D23 abend for diagnostic purposes. The message

might or might not be partially displayed in these cases. Also, your program will likely get different return codes from the WTO and WTOR service than it did in prior releases.

You should correct programs that issue erroneous WTO or WTOR messages regardless of whether the messages are actually displayed.

Element or feature:	BCP.
When change was introduced:	Consoles Enhancements was introduced as a feature of z/OS V1R4 and subsequently integrated into z/OS V1R5.
Applies to migration from:	z/OS V1R4 without the Consoles Enhancements feature.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended to prevent system errors if erroneous WTO and WTOR parameter lists are processed.
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: Look in the logrec data set for WTO and WTOR symptom records and D23 abends. Correct any erroneous WTO or WTOR parameter lists that you find.

When a logrec symptom record is produced, it may indicate the following:

- Whether the error is caused by a WTO or WTOR.
- Whether the WTO issuer was authorized or a problem program.
- As much information as could be gathered to identify the issuer. The record may contain the ASID, job name, program name, and offset into the program where the WTO was issued.
- A description of the error.
- The message line number where the error was detected.
- The WTO/WTOR parameter list (WPL). Note that the entire WPL might not be shown because of size constraints.
- The text of the first line if a multiline WTO.

The following is an example of a logrec symptom record resulting from an erroneous parameter list:

```
THE SYMPTOM RECORD DOES NOT CONTAIN A SECONDARY SYMPTOM STRING.
FREE FORMAT COMPONENT INFORMATION:
   KEY = F000     LENGTH = 000024 (0018)
   +000    C9D5C3D6    D9D9C5C3    E340E6E3    D640C9D5    |INCORRECT WTO IN|
   +010    E5D6C3C1    E3C9D6D5                            |VOCATION        |
   KEY = F000     LENGTH = 000010 (000A)
   +000    C1E4E3C8    D6D9C9E9    C5C4                    |AUTHORIZED      |
   KEY = F000     LENGTH = 000009 (0009)
   +000    C1E2C9C4    61F0F0F0    F1                      |ASID/0001       |
   KEY = F000     LENGTH = 000016 (0010)
   +000    D1D6C2D5    C1D4C561    5CD4C1E2    E3C5D95C    |JOBNAME/*MASTER*|
```

```
KEY = F000      LENGTH = 000025 (0019)
+000    C9D5E5D6    D2C5D961    C9C5C5C3    C2F9F9F9    |INVOKER/IEECB999|
+010    4EF0F0F0    F0F4C5C4    F2                      |+00004ED2       |
KEY = F000      LENGTH = 000032 (0020)
+000    C5D5C4D3    C9D5C540    C4C5E3C5    C3E3C5C4    |ENDLINE DETECTED|
+010    40C2C5C6    D6D9C540    E6D7D3D3    C9D5C5E2    | BEFORE WPLLINES|
KEY = F000      LENGTH = 000017 (0011)
+000    C3E4D9D9    C5D5E340    D3C9D5C5    61F0F0F0    |CURRENT LINE/000|
+010    F2                                              |2               |
KEY = F000      LENGTH = 000003 (0003)
+000    E6D7D3                                          |WPL             |
KEY = FF00      LENGTH = 000216 (00D8)
+000    00480050    F0F0F2F2    40C5D5C1    C2D3C5C4    |...&0022 ENABLED|
+010    4040F0F0    F2F340C5    D5C1C2D3    C5C44040    |  0023 ENABLED  |
+020    F0F0F2F4    40C5D5C1    C2D3C5C4    4040F0F0    |0024 ENABLED  00|
+030    F2F540C5    D5C1C2D3    C5C44040    F0F0F2F6    |25 ENABLED  0026|
+040    40C5D5C1    C2D3C5C4    0400007C    10000000    | ENABLED...@....|
+050    00000000    00000000    000004D2    00000000    |...........K....|
+060 LENGTH(0048) ==> ALL BYTES CONTAIN X'00'.
+090    00000000    40404040    40404040    00000000    |....        ....|
+0A0 LENGTH(0032) ==> ALL BYTES CONTAIN X'00'.
+0C0    00000000    2000C103    00103000    F0F0F2F7    |......A.....0027|
+0D0    40C5D5C1    C2D3C5C4                            | ENABLED        |
KEY = F000      LENGTH = 000010 (000A)
+000    D4C1D1D6    D940E3C5    E7E3                    |MAJOR TEXT      |
KEY = F000      LENGTH = 000034 (0022)
+000    40C9C5C5    F7F3F5C9    40F1F74B    F2F74BF3    | IEE000I 17.27.3|
+010    F940C4E4    D4D4E840    C4C9E2D7    D3C1E840    |9 DUMMY DISPLAY |
+020    F2F3F4                                          |234             |
```

As stated previously, a D23 abend may be issued for these errors. The abend is for diagnostic purposes only and no dump is taken. If you need a dump to debug the problem, you can set the following SLIP to cause the dump:

```
SLIP SET,ENABLE,COMP=D23,ACTION=SVCD,END
```

Reference information: For more information about diagnosing missing message errors and D23 abends, see the WTO and WTOR macros in *z/OS MVS Programming: Assembler Services Reference IAR-XCT* and *z/OS MVS Programming: Authorized Assembler Services Reference SET-WTO*.

Adjust accounting practices for changed WTO and WTOR processing

Description: Effective with the z/OS V1R4 Consoles Enhancements feature, WTO and WTOR processing is changed in that processing that used to be performed asynchronously now occurs in the WTO/R path (SVC 35). This processing is now done much earlier than in prior releases and results in additional processing occurring under the unit of work of the WTO or WTOR issuer.

Thus, if your accounting practices take into account the time used by an application, you might want to consider adjusting them because applications that are heavy users of the WTO and WTOR services will now use more time. Typically, most heavy users of the WTO and WTOR services are subsystems, which are often considered as system overhead for accounting purposes.

Element or feature:	BCP.
When change was introduced:	Consoles Enhancements was introduced as a feature of z/OS V1R4 and subsequently integrated into z/OS V1R5.
Applies to migration from:	z/OS V1R4 without the Consoles Enhancements feature.

Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if applications use the WTO or WTOR services and processing time is significant to your accounting practices.
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: Adjust your accounting practices based on your installation's policies.

Reference information: For information about using the WTO and WTOR macros, see *z/OS MVS Programming: Assembler Services Reference IAR-XCT* and *z/OS MVS Programming: Authorized Assembler Services Reference SET-WTO*.

Chapter 6. Communications Server migration actions

This chapter describes migration actions for base element Communications Server.

Some Communications Server data sets have been removed from z/OS. See
"Remove references to deleted data sets and paths" on page 40. Some
Communications Server data sets have been added to z/OS. See "Add references
to new data sets and paths" on page 53.

Communications Server actions to perform before installing z/OS V1R7

This section describes Communications Server migration actions that you can
perform on your current (old) system. You don't need the z/OS V1R7 level of code
to make these changes, and the changes don't require the z/OS V1R7 level of code
to run once they are made.

IP Services: Migrate from OROUTED to OMPROUTE

Description: Before z/OS V1R7, the OROUTED routing daemon could be used to
support the RIP1 and RIP2 protocols. However, the support for OROUTED is
discontinued in z/OS V1R7. As a result, you must remove OROUTED configuration
statements if you have them.

In addition, starting in z/OS V1R7, if you want to use a daemon to support the RIP protocols, you must use OMPROUTE. OMPROUTE is another routing daemon and it supports RIP1 and RIP2, as well as IPv6 RIP and Open Shortest Path First (OSPF) protocols. This document explains how to migrate to using OMPROUTE to implement the RIP protocol as you are doing with OROUTED.

An OROUTED start parameter is available to assist with migration from OROUTED to OMPROUTE. This function is invoked by specifying -c on the OROUTED startup parameters or by using the following modify command:

```
f orouted,parms=-c
```

Note: The -c parameter must be used before installing z/OS V1R7. (It must be used on your current z/OS system, not on V1R7.)

Both routing daemons use syslogd, resolver configuration files (for DATASETPREFIX and TCPIPJOBNAME), the services file (route 520/udp router routed), and have optional cataloged procedures.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you use OROUTED as your routing daemon.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	OROUTED started from an MVS cataloged procedure or started from a z/OS UNIX shell command line will fail to run.

Steps to take:

1. Start or MODIFY OROUTED with the -c parameter. If started with -c , OROUTED does not modify the IP route table, does not send or receive RIP messages, does not process RIP information, and terminates when the process is complete.

   The -c parameter uses OROUTED configuration files and the OROUTED current environment (including start parameters, routes, interfaces, filters, and MTU information) to create a file that can be used as the profile to start OMPROUTE. The default name used for the created file is cnvrouted.profile. If you would like to use a different name, specify -c filename.filetype. The created file is put in the /tmp directory of the HFS. (An MVS data set is not an option.) If the file name already exists, OROUTED does not create a conversion file and you must either erase the existing file or specify a different output file name. Even though some manual changes to the OMPROUTE profile may be required, this function saves time and effort by having OROUTED perform the majority of the configuration conversion.

2. Stop OROUTED if the daemon is active.

3. Take the conversion file and put it in the appropriate directory or data set for OMPROUTE.
4. Follow the Steps for configuring OMPROUTE in *z/OS Communications Server: IP Configuration Guide*. You must review and update the new OMPROUTE configuration file and the TCP/IP profile. The following are examples of updates you might have to make:
   - For point to point interfaces that do not support sending to a broadcast address, a nonzero destination address must be specified on the RIP interface statement if RIP version 1 is to be sent over the interface.
   - For passive entries in the gateways file for OROUTED, the conversion file provides suggested BEGINROUTES statements for the TCP/IP profile.
   - If VARSUBNETTING, NOVARSUBNETTING, or IGNOREREDIRECTS is specified on the IPCONFIG or ASSORTEDPARMS statement in the TCP/IP profile, remove them because these parameters are only relevant with OROUTED and they are automatically enabled when OMPROUTE runs. Also, if you have port 520 reserved for OROUTED, change that reservation to be for OMPROUTE.

   Note: Support for the VARSUBNETTING and NOVARSUBNETTING parameters on IPCONFIG and ASSORTEDPARMS has been removed. Variable subnetting support is always enabled in TCP/IP.

   For more information on updating the OMPROUTE configuration file and TCP/IP profile, see the conversion tables below. They show what files or commands to remove and what files or commands to add (or to use instead).
5. Remove RACF definitions for OROUTED and add new ones for OMPROUTE. See Table 15 on page 129 for more information.
6. Remove OROUTED configuration files and data sets. If necessary, remove corresponding OROUTED output records from a syslogd file. See Table 9 for more information.
7. Start OMPROUTE using the conversion file as the configuration file.

Configuration files that you must delete:

Table 9. OROUTED configuration files and data sets that you must delete

Configuration file or data set	Description
OROUTED catalogued procedure	JCL used to start OROUTED address space
/etc/orouted.env	Definitions of environmental variables defined in DD:STDENV. For example, RESOLVER_CONFIG, NLSPATH, LANG, ROUTED_PROFILE, and GATEWAYS_FILE.
OROUTED message catalog /usr/lib/nls/msg/C/routed.cat	Defined in NLSPATH or LANG environmental variable.
/etc/routed.profile hlq.ROUTED.PROFILE	Profile to configure mode of operation for OROUTED. Defined in ROUTED_PROFILE environmental variable.
/etc/gateways hlq.ETC.GATEWAYS	Gateway file to configure miscellaneous routing and interface options for OROUTED. Defined in GATEWAYS_FILE environmental variable.
/tmp/orouted.stdout	Output file for stdout stream. Defined in DD:STDOUT.

Table 9. OROUTED configuration files and data sets that you must delete (continued)

Configuration file or data set	Description
/tmp/orouted.stderr	Output file for stderr stream. Defined in DD:STDERR.
/etc/syslog.conf	Control output of syslogd. For OROUTED, its job name may be used in a rule for output control.
syslogd output file /tmp/syslog.log	May contain output records from OROUTED according to rule defined in /etc/syslog.conf.

Conversion tables: In conjunction with the steps above, use the following tables as you migrate OROUTED to OMPROUTE. Stop using the commands or files shown in the OROUTED column (the first column) of each table (remove them from your configuration if necessary) and instead use the corresponding command or file shown in the OMPROUTE column (add them if necessary).

Table 10. Converting OROUTED PROFILE.TCPIP to OMPROUTE PROFILE.TCPIP

OROUTED PROFILE.TCPIP	OMPROUTE PROFILE.TCPIP
PORT UDP 520 OROUTED	PORT UDP 520 OMPROUTE
IPCONFIG IGNOREREDIRECT or IPCONFIG VARSUBNETTING	OMPROUTE automatically enables IPCONFIG IGNOREREDIRECT and VARSUBNETTING during its initialization.
IPCONFIG DATAGRAMFWD (optional)	IPCONFIG DATAGRAMFWD (optional)
IPCONFIG SOURCEVIPA (optional)	IPCONFIG SOURCEVIPA (optional)

Table 11. Converting OROUTED profile to OMPROUTE configuration file

OROUTED profile	OMPROUTE configuration file
RIP2_AUTHENTICATION: "*authentication_key*" (16 characters)	RIP_Interface IP_address = ALL Name = <ignored> Subnet_mask = <default class mask> **Authentication_Key = "*key*"**; (16 characters)
RIP_SUPPLY_CONTROL: RIP1 (default configuration)	RIP_Interface IP_address = ALL Name = <ignored> Subnet_mask = <default class mask>; (default configuration)
RIP_SUPPLY_CONTROL: RIP2 RIP-2 multicast over multicast-capable interfaces only; no RIP messages are sent over multicast-incapable interfaces	RIP_Interface IP_address = ALL Name = <ignored> Subnet_mask = <default class mask> **RIPV2 = YES**; (RIP-1 is disabled)
RIP_SUPPLY_CONTROL: RIP2B (broadcast) **Not Recommended**	RFC recommends that RIP-2 messages are multicast.
RIP_SUPPLY_CONTROL: RIP2M (migration) RIP-2 multicast over multicast-capable interfaces; RIP-1 broadcast over multicast-incapable interfaces	Configure each individual interface for RIP-1 or RIP-2.

Table 11. Converting OROUTED profile to OMPROUTE configuration file (continued)

OROUTED profile	OMPROUTE configuration file
RIP_SUPPLY_CONTROL: NONE	RIP_Interface IP_address = ALL Name = <ignored> Subnet_mask = <default class mask> **Send_RIP = NO**;
RIP_RECEIVE_CONTROL: RIP1 (receive RIP-1 only)	RIP_Interface IP_address = ALL Name = <ignored> Subnet_mask = <default class mask>; (default configuration). However, cannot send RIP-2 since RIP-1 routers cannot receive RIP-2 multicasts; this option was used for OROUTED. RIP_SUPPLY_CONTROL: RIP2B, which is now obsolete.
RIP_RECEIVE_CONTROL: RIP2 (receive RIP-2 only)	RIP_Interface IP_address = ALL Name = <ignored> Subnet_mask = <default class mask> **RIPV2 = YES**; RIP-1 is disabled. However, cannot send RIP-1 since RIP-2 routers are expecting RIP-2 multicasts; this option was used for OROUTED RIP_SUPPLY_CONTROL: RIP2B, which is now obsolete.
RIP_RECEIVE_CONTROL: ANY (default configuration)	RIP_Interface IP_address = ALL Name = <ignored> Subnet_mask = <default class mask> **Receive_RIP = ANY**
RIP_RECEIVE_CONTROL: NONE	RIP_Interface IP_address = ALL Name = <ignored> Subnet_mask = <default class mask> **Receive_RIP = NO**;

Note: The OROUTED profile specifies the global settings for OROUTED (for example, ″RIP_SUPPLY_CONTROL: RIP2″ means all interfaces send RIP-2 messages). Individual interfaces can be configured in the gateways file, which override the profile settings.

OMPROUTE generally requires that individual interfaces be configured. However, OMPROUTE has more granular control over OROUTED in specifying interface metrics and RIP input/output filters.

Table 12. Converting OROUTED gateways file to OMPROUTE configuration file

OROUTED gateways file	OMPROUTE configuration file

net/host *name1* gateway *name2* metric *value* **external** mask *subnetmask*
 	
An external gateway parameter indicates that entries for this destination should never be added to the routing table. The OROUTED server discards any routes for this destination that it receives from other routers. Only the destination field is significant. The gateway and metric fields are ignored.
	filter = (noreceive, *dest_route*, *filter_mask*);
	
	filter = (nosend, *dest_route*,*filter_mask*);

net/host *name1* gateway *name2* metric *value* **passive** mask *subnetmask* A passive gateway does not exchange routing information. Information about the passive gateway is maintained in the local routing tables indefinitely and is only local to this OROUTED server. Passive gateway entries are not included in any routing information that is transmitted. Directly connected passive routes are included. Only one default route can be defined through OROUTED.	Define static route using BEGINROUTES/GATEWAY statement in the TCP/IP profile. The BEGINROUTES/GATEWAY statement supports multiple default routes. RIP_Interface IP_address = ALL Name = <ignored> Subnet_mask = <default class mask> Send_Static_Routes = YES; Advertise static and direct routes.
active active gateway *name2* metric *value* **active** mask *subnetmask* Indicates that the route to the gateway will be treated as a network interface. Active gateways are routers that are running RIP, but can only be reached through a network that does not allow broadcasting and is not point-to-point. (for example, HYPERchannel interface)	RIP_Interface IP_address = *address* Name = *interface_name* Subnet_mask = *subnet_mask* Neighbor = *value*; The *value* of the neighbor parameter corresponds to the *name2* IP address on the OROUTED active gateway statement. Multiple neighbor statements can be coded on an RIP_Interface to indicate adjacent RIP routers. This should be used when the interface is not point-to-point, does not support broadcast, and does not support multicast.
options gateway *ip_addr* block noreceive none Specifies that routing table broadcasts from this gateway are to be ignored.	IGNORE_RIP_NEIGHBOR IP_address = *address*"
options interface.poll.interval *timer_value* options interface.scan.interval *timer_value*	Not needed because OMPROUTE is immediately notified of interface changes by the TCP/IP stack.
options interface *name ip_addr* forward *destination* fmask *fmask*	RIP_Interface IP_address = *address* Name = *interface_name* Subnet_mask = *subnet_mask* **filter = (send,** *dest_route***,** *filter_mask***);**
options interface *name ip_addr* forward.cond *destination* fmask *fmask*	RIP_Interface IP_address = *address* Name = *interface_name* Subnet_mask = *subnet_mask* **filter = (send_cond,** *dest_route***,** *filter_mask***);**

Table 12. Converting OROUTED gateways file to OMPROUTE configuration file (continued)

OROUTED gateways file	OMPROUTE configuration file
options interface *name ip_addr* noforward *destination* fmask *fmask* (an asterisk (*) can be specified on the *destination* as a blackhole filter)	filter = (nosend, *dest_route*, *filter_mask*); (an asterisk (*) can be specified on the *dest_route* as a blackhole filter)
options interface *name ip_addr* receive *destination* fmask *fmask*	RIP_Interface IP_address = *address* Name = *interface_name* Subnet_mask = *subnet_mask* **filter = (receive ,** *dest_route***,** *filter_mask*);
options interface *name ip_addr* receive.cond *destination* fmask *fmask*	RIP_Interface IP_address = *address* Name = *interface_name* Subnet_mask = *subnet_mask* **filter = (receive_cond ,** *dest_route***,** *filter_mask*);
options interface *name ip_addr* noreceive *destination* fmask *fmask* block (an asterisk (*) can be specified on the *destination* as a blackhole filter)	filter = (noreceive, *dest_route*, *filter_mask*); (an asterisk (*) can be specified on the *dest_route* as a blackhole filter)
options interface *name ip_addr* none	Not applicable
options interface *name ip_addr* ripon	Configure as a ″RIP_Interface″.
options interface *name ip_addr* ripoff passive	Do not configure as a ″RIP_Interface″. You might need to configure as an ″Interface″ though (known to OMPROUTE but not participating in OSPF or RIP).
options interface *name ip_addr* supply on	RIP_Interface IP_address = *address* Name = *interface_name* Subnet_mask = *subnet_mask*; (default configuration)
options interface *name ip_addr* supply off	RIP_Interface IP_address = *address* Name = *interface_name* Subnet_mask = *subnet_mask* **Send_RIP = NO**;
options interface *name ip_addr* nokey	RIP_Interface IP_address = *address* Name = *interface_name* Subnet_mask = *subnet_mask* **Authentication_Key = nulls**;
options interface *name ip_addr* key ″*authentication_key*″ (16 characters)	See the ″OROUTED profile″ comparison.

OROUTED gateways file	OMPROUTE configuration file
options interface *name ip_addr* supply.control RIP1 RIP2 RIP2B RIP2M NONE options interface *name ip_addr* receive.control RIP1 RIP2 ANY NONE	See the ″OROUTED profile″ comparison

Table 13. Converting OROUTED start parameters to OMPROUTE start parameters and configuration file

OROUTED start parameters	OMPROUTE start parameters and configuration file
—ep	Not applicable
—del All dynamic routes are deleted from the routing table upon initialization of OROUTED. By default, OROUTED deletes only RIP routes at startup.	All dynamic routes are deleted from the routing table upon initialization of OMPROUTE
—t —t —t —t	—t*n*
—c	Not applicable
—d	—d*n*
—dp	—d2 (or higher)
—g	Originate_RIP_Default Cost = *cost*; RIP_Interface IP_address = ALL Name = <ignored> Subnet_mask = <default class mask> **Send_Default_Routes = YES**;
—h Include host routes in addition to network routes.	RIP_Interface IP_address = ALL Name = <ignored> Subnet_mask = <default class mask> **Send_Host_Routes = YES**;
—hv Include only virtual host routes in addition to network routes.	RIP_Interface IP_address = ALL Name = <ignored> Subnet_mask = <default class mask> **Send_Host_Routes = YES;** **filter = (nosend,** *dest_route***,** *filter_mask*); Use the filter to not advertise the 'Real″ host routes.

Table 13. Converting OROUTED start parameters to OMPROUTE start parameters and configuration file (continued)

OROUTED start parameters	OMPROUTE start parameters and configuration file
—sd Supply default route only.	Send_Only = (DEFAULT);
—sl Supply local (directly-connected) routes only.	Send_Only = (DIRECT);
—st Supply triggered updates only.	Send_Only = (TRIGGERED);
—sv Supply virtual routes only.	Send_Only = (VIRTUAL);
—svd (or —sdv) Supply virtual routes and default route only.	Send_Only = (DEFAULT, VIRTUAL);
—svh (or —shv) Supply virtual (network and host) routes.	**Send_Only = (VIRTUAL)**; RIP_Interface IP_address = ALL Name = <ignored> Subnet_mask = <default class mask> **Send_Host_Routes = YES**;
—sq (or —q)	RIP_Interface IP_address = ALL Name = <ignored> Subnet_mask = <default class mask> **Send_RIP = No**;

Table 14. Converting MODIFY OROUTED to OMPROUTE

MODIFY OROUTED	OMPROUTE
PARMS=-c PARMS=-g PARMS=-gq PARMS=-h PARMS=-hq PARMS=-hv PARMS=-hqv PARMS=-sd PARMS=-sdq PARMS=-sl PARMS=-slq PARMS=-st PARMS=-stq PARMS=-sv PARMS=-svq PARMS=-svd (or —sdv) PARMS=-svdq (or —sdvq) PARMS=-svh (or —shv) PARMS=-svhq (or —shvq) PARMS=-s PARMS=-sq (or —q)	*** No functional equivalent *** These ″MODIFY OROUTED,PARMS=″ commands have the same function as the start parameters. See Table 13 on page 127 for a comparison.
PARMS= –t —t —t —t	MODIFY OMPROUTE,TRACE=*n*

Table 14. Converting MODIFY OROUTED to OMPROUTE (continued)

MODIFY OROUTED	OMPROUTE
PARMS= –tq	MODIFY OMPROUTE,TRACE=*0*
PARMS= –d	MODIFY OMPROUTE,DEBUG=*n*
PARMS= –dp	MODIFY OMPROUTE,DEBUG=*2* (or higher)
PARMS= –dq	MODIFY OMPROUTE,DEBUG=*0*
PARMS= –k (Kill OROUTED)	MODIFY OMPROUTE,KILL
PARMS= –kdr (Kill OROUTED and delete the routing table in TCP/IP) PARMS= –f Flush all indirect routes from TCP/IP routing table. PARMS= –fh Flush all indirect host routes from TCP/IP routing table.	Not applicable — Not needed because OMPROUTE is immediately notified of route table changes by the TCP/IP stack; in addition, dynamic routes are cleared automatically upon startup.
GATEWAYS	Not applicable
GATEWAYS ,DELETE	Not applicable
PROFILE	MODIFY OMPROUTE,RECONFIG This command ignores all statements in the configuration file except new OSPF_Interface, RIP_Interface, and Interface statements. These new configuration statements must be re-read from the configuration file through this command prior to the interface being configured to the TCP/IP stack.
RECONFIG	Not applicable
TABLES Display internal routing, interface, and gateway options tables	DISPLAY TCPIP,*tcpipjobname*,OMPROUTE,RTTABLE DISPLAY TCPIP,*tcpipjobname*,OMPROUTE,RIP,FILTERS DISPLAY TCPIP,*tcpipjobname*,OMPROUTE,RIP,INTERFACE DISPLAY TCPIP,*tcpipjobname*,OMPROUTE,RIP,LIST,ALL DISPLAY TCPIP,*tcpipjobname*,OMPROUTE,RIP,LIST,INTERFACES

As you complete step 5 on page 122, use the following table for the RACF definitions that you should use.

Table 15. Converting OROUTED RACF to OMPROUTE RACF

OROUTED RACF	OMPROUTE RACF
RDEFINE OPERCMDS (MVS.ROUTEMGR.OROUTED) UACC(NONE)	RDEFINE OPERCMDS (MVS.ROUTEMGR.OMPROUTE) UACC(NONE)
PERMIT MVS.ROUTEMGR.OROUTED ACCESS(CONTROL) CLASS(OPERCMDS) ID(*userid*)	PERMIT MVS.ROUTEMGR.OMPROUTE ACCESS(CONTROL) CLASS(OPERCMDS) ID(*userid*)
SETROPTS RACLIST(OPERCMDS) REFRESH	SETROPTS RACLIST(OPERCMDS) REFRESH

Reference information: For details about configuring OMPROUTE, see *z/OS Communications Server: IP Configuration Guide*.

IP Services: Migrate from using the SNMP networking SLA subagent

Description: z/OS V1R7 is planned to be the last release that supports the SNMP networking SLA subagent (pagtsnmp). You will then have to use the SNMP Network SLAPM2 subagent (nslapm2) instead. The latter has extensive improvements in several areas, including better policy performance monitor information, more simplicity, and less platform overhead for data collection.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7 if you are migrating from z/OS V1R6 or z/OS V1R5, but after the first IPL of z/OS V1R7 if you are migrating from z/OS V1R4. (The Network SLAPM2 Subagent, nslapm2, isn't available in z/OS V1R4.)
Is the migration action required?	No, but recommended if you use the SNMP networking SLA subagent because the action is planned to become a requirement in the release following z/OS V1R7.
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: Move management applications from the SNMP networking SLA subagent to the SNMP Network SLAPM2 MIB as soon as possible.

Reference information: For more information about the Network SLAPM2 MIB, see:

* usr/lpp/tcpip/samples/slapm2.mi2
* *z/OS Communications Server: IP Configuration Guide*
* *z/OS Communications Server: IP System Administrator's Commands*

IP Services: Remove the FIREWALL parameter from IPCONFIG statements in PROFILE.TCPIP

Description: PROFILE.TCPIP is a configuration profile data set that contains system operation and configuration parameters. During TCP/IP address space initialization, the data set is read. z/OS Communications Server support for the FIREWALL parameter on the IPCONFIG TCP/IP statement is planned to be removed in a future release. Many Firewall Technologies functions have been stabilized for some time and can be replaced using IPSecurity.

Element or feature:	Communications Server.

When change was introduced:	Future removal of support for the FIREWALL parameter on the IPCONFIG statement was announced in the z/OS V1R7 time frame. (The specific future release has not been announced as of this writing.)
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	No, but recommended because the action is planned to become a requirement 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:	If a FIREWALL parameter is encountered on the IPCONFIG statement, the following message is issued: EZZ0758I FIREWALL PARAMETER ON LINE lineno WILL BE RETIRED IN A FUTURE RELEASE.

Steps to take:

- Configure the TCP/IP profile for IP Security:
    1. Replace the FIREWALL parameter with the IPSECURITY parameter on the IPCONFIG statement in the TCP/IP profile.
    2. Optionally, assign security classes to network interfaces using the SECCLASS parameter on the LINK statements in the TCP/IP profile.
    3. Optionally, assign security classes to dynamic XCF interfaces using the SECCLASS parameter on the IPCONFIG DYNAMICXF statement.
    4. Define default filter rules using the IPSEC statement in the TCP/IP profile.
- To provide IP Security Event logging, ensure that TRMD automatically starts with the stack.
- Enable IPSec configuration for the Policy Agent by specifying the CommonIpSecConfig and IpSecConfig statements in the Policy Agent configuration file for each stack that has IPSec enabled.
- Define IPSec policies within new Policy Agent configuration files:
    1. Specify the new IPSec policies in the configuration files identified with the CommonIpSecConfig and IpSecConfig statements. In addition, use one of the following methods to create the IPSec Policy Agent configuration files:
        – Use the z/OS Network Security Configuration Assistant. Through a series of wizards and online help panels, you can use a GUI to produce the Policy Agent configuration files for any number of TCP/IP stacks. Using the GUI can dramatically reduce the amount of time required to produce configurations and reduce chances of configuration errors.
        – Code the required statements directly into an HFS file or MVS data set.
    2. Update Policy Agent policies by issuing the MODIFY UPDATE command.
- Configure the IKE daemon for execution by following the steps described in the publications in "Reference information" below. In addition, use one of the following methods to create the IKE daemon configuration files:

- Use the z/OS Network Security Configuration Assistant. Through a series of wizards and online help panels, you can use a GUI to produce the Policy Agent configuration files for any number of TCP/IP stacks. Using the GUI can dramatically reduce the amount of time required to produce configurations and reduce chances of configuration errors.
- Code the required statements directly into an HFS file or MVS data set.

Reference information:

- For detailed information about the removal of the Firewall Technologies component, see "Migrate from Firewall Technologies" on page 237.
- For additional information about configuring and using IP Security, see *z/OS Communications Server: New Function Summary*, *z/OS Communications Server: IP Configuration Guide*, and *z/OS Communications Server: IP Configuration Reference*.

IP Services: Replace ASSORTEDPARMS and KEEPALIVEOPTIONS statements in PROFILE.TCPIP

Description: PROFILE.TCPIP is a configuration profile data set that contains system operation and configuration parameters. During TCP/IP address space initialization, the data set is read.

z/OS V1R7 is planned to be the last release that supports the following configuration profile block definition statements:

- ASSORTEDPARMS and ENDASSORTEDPARMS
- KEEPALIVEOPTIONS and ENDKEEPALIVEOPTIONS

Support is being discontinued for these statements because:

- Newer statements support the same parameters as ASSORTEDPARMS and KEEPALIVEOPTIONS.
- Every time an ASSORTEDPARMS or KEEPALIVEOPTIONS statement is processed, any unspecified parameter is set to its default value. On the newer statements, a parameter is set to a value only if it is specified on the statement.

Element or feature:	Communications Server.
When change was introduced:	Future removal of support for ASSORTEDPARMS and KEEPALIVEOPTIONS was announced in the z/OS V1R2 time frame. The specific future release was announced on 15 February 2005 in the z/OS V1R7 preview announcement.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	No, but recommended if you use the ASSORTEDPARMS and KEEPALIVEOPTIONS statements because the action is planned to become a requirement in the release following z/OS V1R7.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.

Restrictions:	None.

System impacts:	If an ASSORTEDPARMS statement is encountered, the following message is issued:
	
	`EZZ0717I ASSORTEDPARMS STATEMENT ON LINE lineno WILL BE RETIRED IN A FUTURE RELEASE`
	
	If a KEEPALIVEOPTIONS statement is encountered, the following message is issued:
	
	`EZZ0717I KEEPALIVEOPTIONS STATEMENT ON LINE xx WILL BE RETIRED IN A FUTURE RELEASE`
	
	The default PROFILE.TCPIP data set does not contain ASSORTEDPARMS and KEEPALIVEOPTIONS statements.

Steps to take: Replace the ASSORTEDPARMS and KEEPALIVEOPTIONS statements in your PROFILE.TCPIP data set with the following newer profile statements:

IPCONFIG
> Provides settings for the IPv4 IP layer of TCP/IP.

TCPCONFIG
> Provides settings for the TCP layer of TCP/IP.

UDPCONFIG
> Provides settings for the UDP layer of TCP/IP.

GLOBALCONFIG
> Provides settings for the entire TCP/IP stack.

To migrate from the ASSORTEDPARMS and KEEPALIVEOPTIONS statements to the newer profile statements, use Table 16 and Table 17 on page 134 to determine which newer profile statements support the same parameters.

The use of ASSORTEDPARMS and KEEPALIVEOPTIONS in combination with the newer statements that support the same parameters can cause undesirable results.

Table 16. Specifying ASSORTEDPARMS parameters on other profile statements

ASSORTEDPARMS	IPCONFIG	TCPCONFIG	UDPCONFIG	GLOBALCONFIG
CLAWUSEDoublenop	CLAWUSEDoublenop			
IGNORERedirect	IGNORERedirect			
NOFWD	NODATAGRamfwd			
NOUDPQueuelimit			NOUDPQueuelimit	
RESTRICTLowports		RESTRICTLowports	RESTRICTLowports	
STOPONclawerror	STOPONclawerror			
TCPIPStatistics				TCPIPStatistics
VARSUbnetting	VARSUbnetting			
SOURCEVIPA	SOURCEVIPA			

Table 17. Specifying KEEPALIVEOPTIONS parameters on other profile statements

KEEPALIVEOPTIONS	TCPCONFIG
INTerval	INTerval
SENDGarbage	SENDGarbage

Reference information: For TCP/IP initialization parameters, as well as specifications for network interfaces and routing, see *z/OS Communications Server: IP Configuration Reference*.

IP Services: Migrate from BIND DNS 4.9.3

Description: In a future release of z/OS, support for BIND DNS 4.9.3 is planned to be discontinued. If you are using this name server, you are encouraged to find a replacement as soon as you can.

Element or feature:	Communications Server.
When change was introduced:	The removal of BIND DNS 4.9.3 function was announced in October 2003. At that time, z/OS V1R7 was planned to be the last release in which the function is available. Subsequently, the removal was delayed to a future release. (The specific future release has not been announced as of this writing.)
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	No, but recommended if you use BIND DNS 4.9.3 function because the action is planned to become a requirement 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.

Steps to take: You should implement BIND DNS 9.2.0 as a replacement. BIND DNS 9.2.0 is included in z/OS beginning with V1R4. If you exploit the Connection Optimization (DNS/WLM) feature of BIND 4.9.3, you should investigate alternative solutions, such as the Sysplex Distributor function.

Reference information: For information about setting up the BIND 9.2.0 name server, see *z/OS Communications Server: IP Configuration Guide* and *z/OS Communications Server: IP Configuration Reference*.

IP Services: Remove customization of SNMP sysObjectID MIB object in OSNMPD.DATA file

Description: The SNMP agent allows you to provide some initial settings for a small set of MIB objects by using the OSNMPD.DATA file. One of the objects for which an initial value can be provided is sysObjectID.0. The sysObjectID.0 object is the vendor's authoritative identification of the network management subsystem contained in the entity. That is, it is intended to uniquely identify the SNMP agent.

| | Changing this value is not recommended and the ability to change it will be disabled in a future release. As of z/OS V1R4, warning message EZZ6317I is written to the syslog daemon if the object is set by using the OSNMPD.DATA file.

Element or feature:	Communications Server.
When change was introduced:	Future removal of the ability to customize the sysObjectID value was announced in the z/OS V1R4 time frame.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	No, but recommended because the ability to customize the sysObjectID value is planned to be removed 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.

Steps to take: Review the statements in your OSNMPD.DATA configuration file. If this file contains a statement for the sysObjectID object, remove the statement from the file.

Reference information: For details about statements in the OSNMPD.DATA configuration file, see the network management chapter of *z/OS Communications Server: IP Configuration Guide*.

IP Services: Verify the correct VLANID value on LINK and INTERFACE profile statements

Description: Before z/OS V1R6, TCP/IP allowed a VLANID value on the LINK statement for IPAQENET, or INTERFACE statement for IPAQENET6, to be from 1–4095. As of z/OS V1R6, a value of 4095 is no longer supported. Therefore, if you have specified a VLANID value of 4095 on a LINK IPAQENET profile statement or an INTERFACE IPAQENET6 profile statement, you must change the value to a number from 1–4094.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you have specified a VLANID value of 4095.
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: Change the VLANID value to a number from 1–4094.

Reference information: *z/OS Communications Server: IP Configuration Reference.*

IP Services: Specify the Policy schema version for schema version 2

Description: Because of a Policy code restructure, the default value for the LDAP_SchemaVersion parameter on the Policy Agent ReadFromDirectory configuration statement is changed from 2 to 3. Schema version 2 is still supported; schema version 3 is now the newest standard.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5 (Policy code restructure)
Applies to migration from:	z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you are using the Policy Agent, schema version 2 objects are defined, and the default is taken for LDAP_SchemaVersion.
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:

1. Examine the default Policy Agent schema version.
2. If the LDAP_SchemaVersion parameter on the Policy Agent ReadFromDirectory configuration statement is not specified, verify the schema version of the policy objects defined on the LDAP server.
3. If schema version 3 objects are defined, no action is necessary. Otherwise, specify the correct schema version on the ReadFromDirectory statement.

Reference information: For details about using the policy code restructure, see *z/OS Communications Server: IP Configuration Reference.*

IP Services: Receive return code value of UNAUTHORIZEDuser for SMTP

Description: The PASCAL application programming interface (API) MonQuery function has a possible return code value of UNAUTHORIZEDuser in certain error scenarios. The UNAUTHORIZEDuser return code value existed previously in some applications but it is new in z/OS V1R5 Communications Server for Simple Mail Transfer Protocol (SMTP).

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5 (SMTP and return code value of UNAUTHORIZEDuser).
Applies to migration from:	z/OS V1R4.

Timing:	Before installing z/OS V1R7.
Is the migration action required?	No, but recommended to assist in problem determination. Users of this API may want to add specific checks for this return code or enhance error messages.
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: Be aware that the PASCAL API MonQuery function has an additional return code value of UNAUTHORIZEDuser as a possible return code in certain error scenarios for SMTP. Modify applications that use this API as recommended above.

Reference information: For details about using the PASCAL Application Programming Interface (API), see *z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference*.

IP Services: Use an alternative method of tracing SNALINK DLCs with GTF

Description: Some SNALINK DLCs used GTF whereas all other TCP/IP traces use CTRACE. SNALINK GTF data tracing requirements can be met by using the VTAM buffer trace from the SNA LU side and the TCP/IP packet trace from the stack side. To avoid redundancy and provide consistency in problem determination, the SNALINK GTF trace is deleted.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you use SNALINK DLCs and trace data using GTF.
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: Change any procedures that use GTF for SNALINK LU0, LU62, and X25 to now use the VTAM buffer trace or the TCP/IP packet trace (SYSTCPDA), or both, to gather equivalent information. The MODIFY PKTTRACE command is no longer supported for SNALINK LU0, LU 6.2, and X25.

Reference information:

- For information about using VTAM BUFFER trace, see *z/OS Communications Server: SNA Operation*.
- For more information about using the TCP/IP packet trace, see *z/OS Communications Server: IP Diagnosis Guide*.

SNA Services: Change your method of defining parallel EE TGs

Description: z/OS V1R7 is planned to be the last release in which Communications Server supports the definition of parallel Enterprise Extender Transmission Groups (TGs) by specifying multiple SAP addresses. After z/OS V1R7, this capability is planned to be removed from the product.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	No, but recommended if you define parallel EE TGs by specifying multiple SAP addresses because the action is planned to become a requirement in the release following z/OS V1R7.
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: If you need parallel EE TGs, consider defining them by using different EE VIPAs on one (or both) of the endpoints. In z/OS V1R7, this is optional; however, in future releases, this method of definition will be necessary if you require parallel EE TGs.

Reference information: Enterprise Extender connections chapter of *z/OS Communications Server: SNA Network Implementation Guide*.

SNA Services: Migrate from AnyNet

Description: z/OS V1R7 is planned to be the last release that supports AnyNet®.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	No, but recommended if you use AnyNet function because the action is planned to become a requirement in the release following z/OS V1R7.
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: You can implement Enterprise Extender (EE) as the replacement for AnyNet.

Reference information: For more information about configuring Enterprise Extender, see *z/OS Communications Server: SNA Network Implementation Guide* and *z/OS Communications Server: IP Configuration Guide*.

Communications Server actions to perform before the first IPL of z/OS V1R7

This section describes Communications Server migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

IP Services: Change FTP general resource profiles in the CSFSERV and CSFKEYS classes

Description: In z/OS V1R7, the z/OS FTP server supports delegated general resource profiles defined in the CSFSERV and CSFKEYS classes to protect ICSF cryptographic hardware keys and resources. Because of this new support, you might need to make some changes in order for your system to continue working as it did prior to z/OS V1R7.

Specifically, you will need to make changes if **all** of the following conditions are true:

- You are using the z/OS FTP server
- Your server is configured to allow or require FTP users to log in using TLS security
- You are using an SAF-compliant security product, such as RACF
- You have applied APAR PQ80574 so that you do not need to allow FTP client user IDs access to general resource profiles in the CSFSERV and CSFKEYS classes that protect ICSF cryptographic keys and services

   or if

   You are migrating from z/OS V1R6, and you use the general resource profiles in the CSFSERV and CSFKEYS classes that protect ICSF cryptographic keys and services.

If the above conditions are true, follow the steps shown after the table below.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Two steps before the first IPL of z/OS V1R7 and two steps after the first IPL of z/OS V1R7.

Is the migration action required?	Yes, if the conditions stated above are true.
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 before the first IPL of z/OS V1R7:

1. Change the general resource profiles in the CSFSERV and CSFKEYS classes that protect ICSF cryptographic keys and services to indicate they are delegated.

   For example, you could use the following command to change the profile CSFENC in class CSFSERV to indicate that it is a delegated profile:

   ```
   RALTER CSFSERV CSFENC APPLDATA('RACF-DELEGATED')
   ```

2. Permit the FTP daemon RACF user ID to the resource profiles.

   For example, if you assigned the RACF ID FTPD to the FTP daemon, you could use the following command to permit FTPD to the resource CSFENC in class CSFSERV:

   ```
   PERMIT CSFENC CLASS(CSFSERV) ID(FTPD) ACCESS(READ)
   ```

Steps to take after the first IPL of z/OS V1R7: If you performed the actions in "Steps to take before the first IPL of z/OS V1R7" above, make the following RACF changes **after** the first IPL of z/OS V1R7 but before starting the z/OS FTP server for the first time:

1. Remove authorizations for any FTP end users permitted to the resource profiles.

   For example, if you permitted the ID FTPUSER to resource CSFENC in class CSFSERV, you could use the following command to remove the authorization:

   ```
   PERMIT CSFENC CLASS(CSFSERV) ID(FTPUSER) DELETE
   ```

2. Once you have made the changes to the general resource profiles, refresh the class associated with those profiles.

   For example, if you changed profiles in the class CSFSERV, you could use the following command to refresh that class:

   ```
   SETROPTS RACLIST(CSFSERV) REFRESH
   ```

Reference information: For details about using FTP general resource profiles in the CSFSERV and CSFKEYS classes, see the following:

- FTP: Security Server enhancements in *z/OS Communications Server: New Function Summary*
- *z/OS Communications Server: IP Configuration Guide*

IP Services: Use the SO_CLUSTERCONNTYPE option of the GETSOCKOPT API

Description: The SO_CLUSTERCONNTYPE option of the GETSOCKOPT API allows applications using TCP communications on z/OS to determine the location of the partner application (for example, at the other end of the TCP connection). The information returned includes indicators on whether the partner application is running in the same image or in the same sysplex, allowing the applications to

optimize their communication based on this knowledge. In the case where the partner application is located in the same sysplex, an additional indicator is returned that describes the types of communication links/interfaces used for the TCP connection. If the communications links/interfaces are not exposed outside the sysplex, then the communication path for the connection is described as internal and applications can use this information to further optimize their processing (such as to avoid encryption of data).

Starting with z/OS V1R7, this internal communication indicator is no longer set if the destination IP address for a connection (such as the partner's IP address) is a Dynamic VIPA or Distributed Dynamic VIPA residing in the sysplex. The reason is that traffic destined to these IP addresses can now be forwarded to the target TCP/IP stacks over links or interfaces that are external to the sysplex. Applications exploiting this internal indicator should continue to function properly from a communication perspective, but they may no longer optimize their processing when the destination address being used is a Dynamic VIPA or a Distributed Dynamic VIPA.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended if you are using the SO_CLUSTERCONNTYPE option on the GETSOCKOPT socket API.
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: If you have applications that exploit this feature with Dynamic VIPAs or Distributed Dynamic VIPAs, you should consider modifying their configuration to use real IP addresses or static VIPAs as the destination addresses if optimized processing is an issue.

Reference information:
- For more information about modifying the configuration of Dynamic VIPAs or Distributed Dynamic VIPAs so that they use real IP addresses or static VIPAs as the destination addresses, see *z/OS Communications Server: IP Configuration Reference*.
- For more information about the SO_CLUSTERCONNTYPE option, see TCP/IP in the sysplex in *z/OS Communications Server: IP Programmer's Guide and Reference*.
- For more information about allowing Sysplex Distributor to distribute incoming packets to target stacks using the best available IP route, see Optimized routing for Sysplex Distributor in *z/OS Communications Server: New Function Summary*.

IP Services: Use IPV6_PKTINFO in a multilevel secure environment

Description: In z/OS V1R7, the IPV6_PKTINFO socket option authorization checks in a multilevel secure environment have been changed to require READ access to the EZB.SOCKOPT.sysname.tcpname.IPV6_PKTINFO SERVAUTH resource. Prior to V1R7, the IPV6_PKTINFO socket option did not require READ access to this resource.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if running in a multilevel secure environment and any applications enable the IPV6_PKTINFO socket option.
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: Define the EZB.SOCKOPT.sysname.tcpname.IPV6_PKTINFO SERVAUTH resource using the RACF definition sample that is shipped in EZARACF. Permit the appropriate users or programs access to the EZB.SOCKOPT.sysname.tcpname.IPV6_PKTINFO resource using the RACF permit sample that is shipped in EZARACF. EZARACF is shipped in data set TCPIP.SEZAINST.

Reference information: For details about using IPV6_PKTINFO in a multilevel secure environment, see the following:

- IPv6 Advanced Socket APIs in *z/OS Communications Server: New Function Summary*
- Required configuration in a multilevel secure environment and Socket option access control in *z/OS Communications Server: IP Configuration Guide*.
- *z/OS Communications Server: IP Configuration Reference*
- *z/OS Communications Server: IP System Administrator's Commands*

IP Services: Modify the FTPOSTPR exit routine

Description: In z/OS V1R7, the FTP user exit routine FTPOSTPR has an additional parameter, increasing the total number of parameters to 18. The new parameter is a 1-byte confidence level descriptor. If you do not activate FTP confidence checking in the FTP server by coding CHKCONFIDENCE TRUE in FTP.DATA, the confidence level is always set to X'04' — Confidence level checking is not active.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.

Is the migration action required?	Yes, if you are migrating the FTPOSTPR exit routine.
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:

1. Verify that your exit routine will tolerate the additional parameter.
2. Modify FTPOSTPR if needed.

Reference information: For details about using the FTP user exit routine FTPOSTPR, see the following:

- FTP reliability of data transfer in *z/OS Communications Server: New Function Summary*
- The FTPOSTPR user exit in *z/OS Communications Server: IP Configuration Guide*

IP Services: Update programs for the TCP segmentation offload performance enhancement

Description: Before z/OS V1R7, the TCP/IP stack performed all outbound TCP segmentation processing. Starting in z/OS V1R7, if you are using an OSA-Express2 Ethernet feature in QDIO mode that supports TCP segmentation offload, the stack offloads most IPv4 outbound TCP segmentation processing to the OSA.

If you have programs that analyze formatted packet trace output, your programs might need changes. If you have programs that format packet trace data using the TCP/IP real-time packet trace interface, your programs might need additional changes.

Note: These improvements are automatically enabled for an OSA-Express2 Ethernet feature in QDIO mode that supports the TCP segmentation offload function. You cannot disable them.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have programs that analyze formatted packet trace output or if you have programs that format packet trace data using the TCP/IP real-time packet trace interface.
Target system hardware requirements:	A z9-109, z990 or z890 server with any of the OSA-Express2 features (Gigabit Ethernet SX and LX, 10 Gigabit Ethernet LR) configured in QDIO mode.
Target system software requirements:	None.

Other system (coexistence or fallback) requirements:	None.
Restrictions:	The TCP segmentation offload function is only available when the OSA-Express2 Ethernet feature is running in QDIO mode and only applies to outbound IPv4 TCP packets. This function does not apply to the following:
	• Packets that go to another stack sharing the same OSA-Express2
	• IPSEC encapsulated packets
	• When multipath is in effect (unless all interfaces in the multipath group are enabled for TCP segmentation offload)
System impacts:	None.

Steps to take: Change any programs affected by the TCP segmentation offload packet trace changes by following the steps outlined in the referenced publications (below).

Reference information:

- If you have programs that analyze formatted packet trace output, see Formatting packet traces using IPCS in *z/OS Communications Server: IP Diagnosis Guide* to determine if the programs need to change and, if so, for details about what to change.
- If you have programs that format packet trace data using the TCP/IP real-time packet trace interface, see Application interfaces for TCP/IP network monitoring in *z/OS Communications Server: IP Programmer's Guide and Reference* to determine if the programs need to change and, if so, for details about what to change.
- For a description of how to use the function, see QDIO OSA-Express segmentation offload in *z/OS Communications Server: New Function Summary*.

IP Services: Allocate buffer size for Network Management Interface real-time packet trace data

Description: Before z/OS V1R7, users of the Network Management Interface (NMI) for TCP/IP real-time packet tracing (SYSTCPDA) were expected to allocate a 64 KB buffer when copying the trace buffer into their storage. Starting in z/OS V1R7, the TMI initialization record sent to the NMI user provides the size of the data buffer that the user must allocate to receive the trace data.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended to improve storage usage.
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: Although the default size of the data buffer is 64 KB, the same as the default in prior releases, IBM recommends that applications use the TMI initialization record field to determine the size of the buffer required to collect the trace data, and then allocate the buffer accordingly. For NMI applications that work with previous z/OS releases, the buffer size in the initialization record is zero, meaning that a 64 KB buffer is required.

Reference information:
- *z/OS Communications Server: IP Programmer's Guide and Reference*
- *z/OS Communications Server: New Function Summary*

IP Services: Remove customization of PPT entries in SCHEDxx parmlib members previously added for z/OS Load Balancing Advisor

Description: The z/OS Load Balancing Advisor function, which is integral to z/OS V1R7, was first shipped as new function PTFs for z/OS V1R6, z/OS V1R5, and z/OS V1R4. The PTF documentation for this function instructed you to add PPT entries to the SCHEDxx parmlib members for the z/OS Load Balancing Advisor (Advisor) and Agent (Agent).

z/OS V1R7 ships with the PPT entries already present. If you installed the PTFs and manually added the PPT entries on any of the back-level systems, you should remove the entries to avoid duplication when z/OS V1R7 is installed.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6 if the PTF for APAR PQ96293 is installed, z/OS V1R5 if the PTF for APAR PQ96293 is installed, and z/OS V1R4 if the PTF for APAR PQ90032 is installed.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended to remove the SCHED*xx* entries that are no longer needed after you've installed z/OS V1R7.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	You must restore the PPT entries if falling back from z/OS V1R7 or if PPT entries are shared with pre-z/OS V1R7 systems.
Restrictions:	None.
System impacts:	None.

Steps to take: Remove the PPT entries with PGMNAME of EZBLBAGE and EZBLBADV from the SCHED*xx* parmlib member.

IP Services: Modify the TN3270E server profile to continue SSLV2 support

Description: Before z/OS V1R7, Telnet SSLV2/NOSSLV2 parameter statements did not exist and the SSLV2 protocol was always available. Starting in z/OS V1R7, Telnet's default setting is to prohibit the use of the SSLV2 protocol and to require that the SSLV2 parameter be specified to allow that protocol. This might affect migration for older Telnet clients that only support the SSLV2 protocol for secure connections.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have Telnet clients that only support the SSLV2 protocol for secure connections.
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: Determine if your installation has any Telnet clients that only support the SSLV2 protocol. If so, upgrade those clients or add the SSLV2 Telnet parameter statement to allow the use of this protocol.

Reference information:

- SSLV2 and NOSSLV2 statement in *z/OS Communications Server: IP Configuration Reference*
- TN3270E SSLV2 protocol default changes in *z/OS Communications Server: New Function Summary*

IP Services: Make changes for Netstat enhancements

Description: The Netstat command displays the status of a local host. Each release, the Netstat reports are changed in ways that can affect automation or front-end programs.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7, z/OS V1R6, and z/OS V1R5.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.

Is the migration action required?	Yes, if the changed or removed settings affect automation running off Netstat or front-end programs to Netstat.
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: Accommodate Netstat changes in your automation and front-end programs. You can begin planning your changes by reviewing the ways in which the displays are updated each release. For details about how each Netstat report has changed, see *z/OS Summary of Message and Interface Changes*. However, you will have to execute the commands to know with certainty what changes to make.

Reference information:
- For details about using Netstat, see *z/OS Communications Server: IP System Administrator's Commands*.
- For details about 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.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7 and z/OS V1R5.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have customized a configuration file (listed in Table 18 on page 148) 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.

Steps to take: If you added installation-dependent customization to any of the IBM-provided configuration files listed in Table 18, 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.

Note: Some `/etc` files were removed because of discontinuance of support for OROUTED. See Table 9 on page 122.

Table 18. Changed Communications Server configuration files

Utility	IBM-provided sample file	File to which you copy the sample	What changed and when
getprotocolbyname() API	/usr/lpp/tcpip/samples/protocol	/etc/protocol	In z/OS V1R7, support for hopopt, encapsulating security payload, and authentication header protocol was added.
OMPROUTE	/usr/lpp/tcpip/samples/services	/etc/services	In z/OS V1R5, support for IPv6 routing daemons was added.
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.

Reference information: For more details about configuration files, see *z/OS Communications Server: IP Configuration Guide*.

IP Services: Stop inferring TCP/IP stack status or system capability from certain GetAddrinfo results

Description: With APAR PQ92830, the GetAddrinfo resolver API was modified in three specific situations to return slightly different results depending on whether IPv6 capability is available in the system. This change has been integrated into the base code for z/OS V1R7.

The specific situations are:

- Applications invoking GetAddrinfo with a null hostname and specifying AF_INET6 or AF_UNSPEC as the output address family will get different results in some instances. Previously, the z/OS resolver would return the default loopback address for an IPv6 address (::1) or IN6ADDR_ANY, regardless of whether IPv6 was supported by the system. Now, those addresses are only returned when IPv6 support is available.

- Applications invoking GetAddrinfo with an input IPv4 address in presentation format, and specifying AF_UNSPEC as the output address family and requesting IPv4-mapped IPv6 addresses as output, will get different results in some instances. Previously, the z/OS resolver would not provide the mapped address when IPv6 support was available on the system but no stack that provided IPv6 support had been activated. Now, the addresses are returned in mapped format, regardless of the status of the stack.

- Applications invoking GetAddrinfo with an input IPv6 address in presentation format, and specifying AF_UNSPEC as the output address family, will get different results in some instances. Previously, the z/OS resolver would fail the invocation when IPv6 support was not available on the system, or when IPv6 support was available but no stack that provided IPv6 support had been

activated. Now, the input IPv6 addresses are returned when IPv6 support is available, regardless of the status of the stack.

While it never was intended that the GetAddrinfo resolver API provide you with an understanding of the system IPv6 capability, or of the status of the TCP/IP stacks in the system, some applications could have used the information returned in these instances to infer information about the system capability or the TCP/IP stack status. Applications that did use the information returned previously by GetAddrinfo invocations must be modified to handle the changes in what GetAddrinfo returns in these situations.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R6 by PTF UQ92871 (APAR PQ92830).
Applies to migration from:	z/OS V1R6 without PTF UQ92871 (APAR PQ92830) installed, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you used the results of GetAddrinfo invocations in the situations described above as a means to infer the capability of the system in terms of IPv6 or as a means to infer the status of the TCP/IP stack.
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: Modify the application logic to no longer assume certain system capabilities or TCP/IP stack status if GetAddrinfo is invoked in any of the following situations:

- GetAddrinfo is invoked with a null hostname and ai_family=AF_INET6 or AF_UNSPEC.
- GetAddrinfo is invoked with an input IPv4 address in presentation format, ai_family=AF_UNSPEC, and ai_ V4MAPPED=1.
- GetAddrinfo is invoked with an input IPv6 address in presentation format, and ai_family=AF_UNSPEC.

Reference information: For specifics about how GetAddrinfo is invoked using the methods above, see *z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference*.

IP Services: Remove the backslash from double quotation marks when submitting REXEC and TSO requests in batch

Description: Starting in z/OS V1R5, the REXEC and RSH TSO client commands are written in C. This changes the way special characters are passed to the remote execution server for processing. However, there was a problem in z/OS V1R6 and z/OS V1R5 such that if the command to be executed on the remote host contained double quotation marks, you had to precede the quotation marks with a backslash

(\\) in order for the quotation marks to be passed to the remote execution server. For example, you had to specify \\"value\\" if you wanted the character string "value" to be passed to the remote server. If you did not add the backslash, then the quotation marks would be replaced by blanks.

APAR PQ96308 fixed the problem. If you installed the appropriate PTF (PTF UQ95549 on z/OS V1R6 or PTF UQ95548 on z/OS V1R5), you didn't have to use the backslash. But if you didn't install the appropriate PTF, and you therefore used the backslash, remove the backslash in z/OS V1R7 because it is no longer needed and, if not removed, will cause an error.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R6 without PTF UQ95549 (for APAR PQ96308) and z/OS V1R5 without PTF UQ95548 (for APAR PQ96308).
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use double quotation marks on REXEC and RSH commands to be executed on the remote host and you have not installed PTF UQ95549 on z/OS V1R6 or PTF UQ95548 on z/OS V1R5.
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: Remove the backslash that precedes double quotation marks in commands to be executed on remote hosts.

Reference information: *z/OS Communications Server: IP User's Guide and Commands*.

IP Services: Use socket option access control

Description: Socket option access control gives system administrators the ability to assign permission for z/OS users to set selected socket options using an SAF security server. Access control is provided for the SOL_SOCKET level, SO_BROADCAST option.

You may need to define a profile in the SERVAUTH class for the EZB.SOCKOPT.sysname.tcpname.SO_BROADCAST resource. Programs that send datagrams to broadcast addresses may fail if the user is not permitted at least READ authority to this profile.

TCP/IP's default behavior in a *nonmultilevel*-secure environment is to *allow* all users to set the SO_BROADCAST socket option so they may send broadcast datagrams when this profile is not defined. Some security products do not distinguish between a resource profile not defined and a user not permitted to that resource. If your security server does not make this distinction, you must define the socket option resource profile and permit users to it whenever the SERVAUTH class is active.

TCP/IP's default behavior in a *multilevel*-secure environment is to *disallow* all users to set the SO_BROADCAST socket option so they may send broadcast datagrams when this profile is not defined. If you plan to run in a multilevel-secure environment, you must define the socket option resource profile and permit users to it.

You will need to determine the TCP/IP programs that set the socket option SO_BROADCAST and send datagrams to a broadcast address. The users of these programs will require permission to this profile. A list of TCP/IP programs that would require users to have permission to this new profile can be found in the security chapter of *z/OS Communications Server: IP Configuration Guide*.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if either of the following is true: • You are running a multilevel-secure environment. • Your security product distinguishes between a resource profile not defined and a user not permitted to that resource.
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:
1. Determine if your security product distinguishes between a resource profile not defined and a user not permitted to that resource.
2. Determine if you are running a multilevel-secure environment (that is, if the RACF MLACTIVE option is active).
3. If step 1 or 2 is TRUE, then you must define a profile in the SERVAUTH class for the EZB.SOCKOPT.sysname.tcpname.SO_BROADCAST resource and permit programs that send datagrams to broadcast addresses with at least READ authority to this profile.

Reference information:
- For details about using socket option access control, see Socket option access control in *z/OS Communications Server: New Function Summary*.
- *z/OS Communications Server: IP Configuration Guide*.
- For information about multilevel security, see *z/OS Planning for Multilevel Security and the Common Criteria*.

IP Services: Define a profile in the SERVAUTH class for VIPARANGE

Description: A RACF SERVAUTH class profile can control which applications may bind() to define a Dynamic Virtual IP Address (DVIPA) using VIPARANGE. To restrict applications that can bind() to a DVIPA within a VIPARANGE, define the

EZB.BINDDVIPARANGE.sysname.tcpname profile in RACF, and permit the applications that are allowed to bind(). If the profile is not defined, then the bind() is processed and no checking is performed.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if your security product does not distinguish between a resource profile not defined and a user not permitted to that resource.
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: Define a profile in the SERVAUTH class for the EZB.BINDDVIPARANGE.sysname.tcpname resource.

Reference information:
- IPv6 support for Sysplex enhancements in *z/OS Communications Server: New Function Summary*
- *z/OS Communications Server: IP Configuration Guide*

IP Services: Remove duplicate VIPADYNAMIC statements for the same dynamic VIPA address

Description: The processing of VIPADYNAMIC statements is changed to work the same whether the statements are specified within a single profile or with separate profiles. In previous releases, if a Dynamic Virtual IP Address (DVIPA) was specified in more than one VIPADEFINE or VIPABACKUP statement within a single profile, only the last VIPADEFINE or VIPABACKUP statement containing the DVIPA would be processed. Now all statements within a single profile are processed.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if your TCPIP profile has multiple VIPADEFINE or VIPABACKUP statements for the same dynamic VIPA address (DVIPA).
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: Edit your profile and remove all VIPADEFINE and VIPABACKUP statements for the same dynamic VIPA address so that only the one desired definition remains.

Reference information:
- Section on processing of VIPADYNAMIC statements in *z/OS Communications Server: New Function Summary*
- *z/OS Communications Server: IP Configuration Reference*

IP Services: Ensure that TCPSTACKSOURCEVIPA is coded correctly

Description: The types of addresses allowed for the TCPSTACKSOURCEVIPA configuration option are now restricted to the following:
- Static VIPAs
- Active dynamic VIPAs

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have a TCPSTACKSOURCEVIPA configuration option coded with an address that is neither a static VIPA nor an active dynamic VIPA.
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: Ensure that your TCPSTACKSOURCEVIPA configuration option is coded with an address that is a static VIPA or an active dynamic VIPA.

Reference information:
- IPv4 Sysplex enhancements for TCPSTACKSOURCEVIPA in *z/OS Communications Server: New Function Summary*
- *z/OS Communications Server: IP Configuration Reference*
- *z/OS Communications Server: IP Configuration Guide*

IP Services: Update handling of policy statistics because of changed FLUSH processing

Description: In releases before z/OS V1R6, the MODIFY REFRESH command for the Policy Agent performs FLUSH processing if both of the following are true: (1) the FLUSH parameter is specified on the TcpImage statement and (2) the HFS configuration is changed. Starting in z/OS V1R6, only the first condition needs to be true; the second condition is irrelevant. That is, starting in z/OS V1R6, the MODIFY

REFRESH command for Policy Agent performs FLUSH processing if FLUSH is specified on the TcpImage statement, regardless of whether the HFS configuration is changed.

Policy statistics are affected by this change. They might not accumulate over as great a period of time as they did before z/OS V1R6. If you have applications or automation procedures that rely on policy statistics to be collected over a certain period of time, you might need to alter them to account for the fact that a MODIFY REFRESH command resets those statistics. For example, you might have to delay issuing a MODIFY REFRESH command in your automation procedures until after policy statistics are collected.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have applications or automation procedures that deal with policy statistics and that use the MODIFY REFRESH command to perform FLUSH processing.
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: Update applications and automation procedures to take into consideration that policy statistics being collected in the TCP/IP stack are now always reset by MODIFY REFRESH with FLUSH because the command now always deletes and reinstalls all policies.

Reference information:

- For details about the MODIFY REFRESH command, see *z/OS Communications Server: IP System Administrator's Commands*.
- For details about the FLUSH parameter on the TcpImage configuration statement, see *z/OS Communications Server: IP Configuration Reference*.

IP Services: Update the TCP/IP sample profile to start the SNMP TCP/IP subagent

Description: The TCP/IP sample profile is installed in data set *hlq*.SEZAINST(SAMPPROF). Before z/OS V1R6, the SACONFIG profile statement, which governs the SNMP TCP/IP subagent, appeared in the sample profile as follows:

```
SACONFIG ENABLED COMMUNITY public AGENT 161
```

This caused the SNMP TCP/IP subagent to be started during TCP/IP stack initialization. Because the TCP/IP subagent requires other configuration and other functions to be started outside of stack initialization in order to successfully initialize, as of z/OS V1R6 the SACONFIG profile statement in the sample profile is changed to only include the DISABLED keyword. If you use the sample profile as the base

for your TCP/IP profile, and don't change the SACONFIG profile statement, the TCP/IP subagent is not started during stack initialization.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use the sample profile and want the SNMP TCP/IP subagent to be started during stack initialization.
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: Do either of the following:

- Remove the SACONFIG statement. If no SACONFIG statement is present in the profile, then the SNMP TCP/IP subagent is started with the default parameter values of public for the COMMUNITY keyword and a port of 161 for the AGENT keyword.

- Change the DISABLED parameter to ENABLED. The SNMP TCP/IP subagent will be started with the default parameter values of public for the COMMUNITY keyword and a port of 161 for the AGENT keyword.

Reference information: For more information about the SACONFIG profile statement, see *z/OS Communications Server: IP Configuration Reference*.

IP Services: Migrate from the SMIv1 version of the SNMP IBM MVS TCP/IP Enterprise-specific MIB Module

Description: Until z/OS V1R6, two versions of the SNMP IBM MVS TCP/IP Enterprise-specific MIB module were shipped and installed in HFS directory `/usr/lpp/tcpip/samples`, with the following filenames:
- `mvstcpip.mib` — the SMIv1 language version of the MIB module
- `mvstcpip.mi2` — the SMIv2 language version of the MIB module

As of z/OS V1R6, the SMIv1 version is no longer shipped. If you want to continue using SMIv1, you can use publicly available tools to convert the SMIv2 MIB module to an SMIv1 MIB module.

Element or feature:	Communications Server.
When change was introduced:	The removal of support for the SMIv1 version of the MIB module was announced in May 2003. z/OS V1R5 was the last release in which the function was available.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use the SMIv1 version of the MIB module.

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: If you want to continue using SMIv1, you can use publicly available tools to convert the SMIv2 MIB module (`mvstcpip.mi2`) to an SMIv1 MIB module.

Reference information: IPv6 support for SNMP TCP/IP Subagent in *z/OS Communications Server: New Function Summary*.

IP Services: Verify Originate_RIP_Default settings if running OMPROUTE RIP

Description: Before z/OS V1R5, when OMPROUTE was running RIP, the Originate_RIP_Default statement did not behave as documented. The documented default value for the Condition parameter is ALWAYS, but OMPROUTE was using NEVER as the default value.

Starting in z/OS V1R5, OMPROUTE has been fixed to follow the defaults as documented. This means that, by default, OMPROUTE always attempts to originate a default route on all RIP interfaces whose filters allow default route origination. This also means that OMPROUTE does not accept any RIP default routes learned from the network, because the default values of Accept_Default=NO and COST=1 preclude OMPROUTE from learning any RIP default routes that are lower cost than the one it is originating. This may cause undesirable results, specifically, the inability to learn RIP default routes from the network.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended in case you were relying on the incorrect default values.
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: If you are running OMPROUTE RIP and want to be able to learn default routes from the RIP network, code parameter value Condition=NEVER on the ORIGINATE_RIP_DEFAULT statement. This causes OMPROUTE's behavior to match the previous incorrect default.

Reference information: ORIGINATE_RIP_DEFAULT statement in *z/OS Communications Server: IP Configuration Reference*.

IP Services: Update automation for changed display of OMPROUTE interface details responses

Description: Before z/OS V1R5, the response to a DISPLAY TCPIP,,OMPROUTE,OSPF,INTERFACE,NAME=xxxxxxxx command would have the same set of fields listed regardless of the type of interface specified. As of z/OS V1R5, specification of a VIPA interface does not include several of the fields whose values do not apply to that kind of interface.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5 (OMPROUTE enhancements).
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if automated operator procedures that read EZZ7850I messages are being used.
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:

- Examine any automated operator procedures to see if they issue DISPLAY TCPIP,,OMPROUTE,OSPF,INTERFACE,NAME=xxxxxx (or the equivalent MODIFY OMPROUTE,OSPF,INTERFACE,NAME=xxxxxx) commands, or if they capture or examine the resultant output (EZZ7850I message).
- Ensure that any VIPA interface names will not be specified on these commands, or update the routines that handle the response messages to recognize the new format.

Reference information: *z/OS Communications Server: IP System Administrator's Commands*.

IP Services: Update automation for SNTP daemon activation

Description: In z/OS V1R4 and prior releases, the SNTP daemon (SNTPD) was not APF authorized. As of z/OS V1R5, it is APF authorized. As a result, message EZZ9600I has a different display. It now displays as `EZZ9600I SNTP SERVER READY`, indicating that the task is APF authorized. In z/OS V1R4 and prior releases, it displayed as `+EZZ9600I SNTP SERVER READY`, the plus sign indicating it was issued from a problem program (non-APF authorized).

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you automate on the EZZ9600I SNTP SERVER READY message.
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: Update any automation processes that are looking for `+EZZ9600I SNTP SERVER READY` to now look for `EZZ9600I SNTP SERVER READY`. In general, automation processes should not be written to key off the special character that prefaces the message number.

Reference information: See the section about appending special screen characters in *z/OS MVS System Commands*.

IP Services: Examine OMPROUTE CTRACE options

Description: Before z/OS V1R5, the ALL option of OMPROUTE CTRACE would cause OMPROUTE trace information to be written to DASD files. As of z/OS V1R5, the new DEBUGTRC option of OMPROUTE CTRACE diverts the OMPROUTE trace information to CTRACE. As part of this change, the ALL option now includes the DEBUGTRC option behavior, diverting the OMPROUTE trace information to CTRACE rather than writing it to DASD.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5 (OMPROUTE enhancements).
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if the OMPROUTE CTRACE option ALL is enabled and you want OMPROUTE debug and trace to continue writing to DASD files.
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:

1. Examine your OMPROUTE CTRACE options.
2. If you want the OMPROUTE debug trace to be diverted to CTRACE, ensure that you are using the ALL option or the DEBUGTRC option.
3. If you want OMPROUTE debug and trace to continue writing to DASD files, ensure that neither the new DEBUGTRC option nor the ALL option are enabled. Ensure that all desired options are enabled.

Reference information:

- *z/OS Communications Server: IP Diagnosis Guide*
- *z/OS Communications Server: New Function Summary*

IP Services: Use additional SMF record data

Description: The existing use of system management facilities (SMF) is enhanced to provide additional information for system management and accounting. Specifically, the SMF recording enhancements include the following:

- IPv6 enablement of SMF records is complete.
- Security information is added to the various FTP server and client SMF records, for the purpose of identifying the security mechanism and levels for FTP transfers.
- The TCP Connection Termination record is modified to report Telnet-specific information, such as LU name, application name, and protocol, for those connections that are TN3270 connections.
- The formats for several of the type 119 SMF records are changed to add additional subsections reflecting new information.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5 (IPv6 support for SMF).
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended in order to obtain full system management and accounting information from SMF records.
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:

1. Be aware of the changes in format for several of the type 119 SMF records.
2. Update any automated SMF processing tools to make use of the additional information now provided. Utilize EZASMF77 to get the correct mappings of the changes.

Reference information: For details about IPv6 support for SMF, see:

- *z/OS Communications Server: IP Configuration Reference*
- *z/OS Communications Server: IPv6 Network and Application Design Guide*

IP Services: Migrate the TSO remote execution server user exit for IPv6

Description: z/OS V1R5 Communications Server enhanced the TSO rexec and rsh commands and RXSERVE so that they can operate over IPv6 networks.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5 (IPv6 support for TSO rexec, rsh, and associated MVS daemons).
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.

Is the migration action required?	Yes, if you are running in an IPv6 environment and you want to preserve operation of user exits that do not support IPv6.
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: In order for existing RXSERVE user exits to function when TCP/IP is IPv6-enabled, start RXSERVE with the IPV6=N option. This option defaults to YES.

Reference information: For details about using RXSERVE, see:
- *z/OS Communications Server: IP Configuration Guide*
- *z/OS Communications Server: IP Configuration Reference*
- *z/OS Communications Server: New Function Summary*
- *z/OS Communications Server: IPv6 Network and Application Design Guide*

IP Services: Accommodate changes in the Sendmail default directory

Description: The sendmail program was upgraded to version 8.12.1 in z/OS V1R5 Communications Server to enable IPv6 support and mail filters, and enhance security. Because of the upgrade, the default directory for sendmail configuration files has changed from /etc to /etc/mail.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5 (IPv6 support and upgrade for Sendmail).
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

Steps to take: The default directory for sendmail configuration files has changed from /etc to /etc/mail. If you are using the previous default directory (/etc), you must now use the new default directory (/etc/mail). Create the /etc/mail directory, properly set the permissions, and move your configuration files to it, or alternatively, explicitly specify the directories you use.

Note: The `sendmail.org` changes from 8.8 to 8.12.1 are extensive. As a result, you must reference the IPv6 support and upgrade for Sendmail section in *z/OS Communications Server: New Function Summary* as you convert your configuration file.

Reference information: For details about using sendmail, see:
- *z/OS Communications Server: IP Configuration Guide*
- *z/OS Communications Server: IP Configuration Reference*
- *z/OS Communications Server: IPv6 Network and Application Design Guide*
- *z/OS Communications Server: New Function Summary*

IP Services: Accommodate Telnet display format for IPv6 and IPCONFIG FORMAT LONG

Description: In z/OS V1R5 Communications Server, the Telnet Server supports IPv6 format IP addresses, depending on the support level of the TCP/IP stack. If the stack is running IPv6, Telnet completely supports IPv6. If the stack is running IPv4, Telnet is IPv4 capable. There is no external parameter needed in Telnet to turn on IPv6 support. Telnet is always IPv6 capable if the stack supports IPv6. If the TCP/IP stack is running in IPv4 mode, no IPv6 function is available in Telnet.

Displays that are tabular in style will use a two-line format to display the data when a client identifier appears on the line if either of the following IPv6 switch conditions are met:
- The stack is running IPv6 mode.
- The configuration statement FORMAT LONG is specified.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5 (IPv6 support for TN3270).
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if the TCP/IP stack is IPv6 enabled, or if FORMAT LONG is coded in the TELNETGLOBALS section of PROFILE.TCPIP, and if there is existing message automation that keys off of TN3270 messages.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	The WLM statement does not support the IPv6 format.
System impacts:	None.

Steps to take: Changes to existing message automation programs may be necessary to accommodate the new two-line message format. If the two-line format is used, it is always used even when the data would fit on a single line. This will ensure uniformity of output for displays. Modify any automation programs that might key off the TN3270 messages that may be displayed in the modified format.

Reference information: For details about using IPv6 support for TN3270, see:

- *z/OS Communications Server: IP Configuration Reference*
- *z/OS Communications Server: IPv6 Network and Application Design Guide*

IP Services: Use Stack Access Control for applications issuing gethostname() or gethostid() calls

Description: When using a GetHostId/GetHostName vnode operation (a call made to the stack PFS by the USS LFS when an application issues the gethostid() or gethostname() function), be aware that starting in z/OS V1R5 Communications Server, the stack will verify the caller has authorization to the STACKACCESS resource in the SERVAUTH class. This will prevent applications in a Common INET environment from receiving the host name or default IP address of a stack that they are not then permitted to use. If the resource profile exists and the user does not have READ authority, they will receive a return and reason code of EACCES and JRNOTAUTHSTACK. The user should set affinity to the stack he is permitted to use before running the application.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5 (Stack Access Control for applications issuing gethostname() or gethostid() calls).
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if the STACKACCESS resource is restricted by your security product (for example, RACF).
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: If the STACKACCESS resource of one or more TCP/IP stacks in a Common INET configuration is restricted by your security product (such as RACF), then applications that issue gethostid() or gethostname() need to establish stack affinity to the TCP/IP stack that they are permitted to use by their security product. If your security product is RACF, this applies to situations where the SERVAUTH class is active, and RACF profiles exist that cover the STACKACCESS resource.

Reference information: For details, see *z/OS Communications Server: IP Configuration Reference*.

IP Services and SNA Services: Use new VTAM start options to adjust the QDIO or iQDIO storage

Description: The amount of storage used for read processing for both queued direct input/output (QDIO) and internal queued direct input/output (iQDIO) devices has increased. (Communication between iQDIO devices is known as HiperSockets communication.) This storage increase affects the CSM 4K data space (64-bit, if supported) and is page fixed. Table 19 on page 163 and Table 20 on page 163 show the old and new values. Note that the increases are on a per-active-data-device basis.

Table 19. OSA Express (QDIO) storage for read processing

	Old value	New default value
zSeries (64-bit)	.5 MB	4 MB
non-64-bit	.5 MB	1 MB

Table 20. HiperSockets (iQDIO) storage for read processing

CHPID maximum frame size	Old value	New default value
64 KB	4 MB	8 MB
40 KB	4 MB	5 MB
24 KB	3 MB	3 MB (no change)
16 KB	2 MB	2 MB (no change)

As a result of this increase, two new VTAM start options allow you to adjust the QDIO or iQDIO storage used for each data device (read processing). The options are global, which means they affect all QDIO or iQDIO devices. The VTAM global values can be overridden by the READSTORAGE parameter on the TCP/IP LINK or INTERFACE statement. For most users, the defaults of these start options are appropriate, and you will probably never have to change them. However, there are valid configurations (such as many OSA adapters, or multiple TCP/IP stacks per LPAR, or many second-level guests under VM) in which you may need to adjust this storage. The new options are as follows:

- The QDIOSTG (QDIO storage) option allows you to define how much storage VTAM keeps available for read processing for all OSA QDIO data devices.
- The IQDIOSTG (iQDIO storage) option allows you to define how much storage VTAM keeps available for read processing for all HiperSockets (iQDIO) data devices that use a maximum frame size (MFS) of 64 KB.

Element or feature:	Communications Server.
When change was introduced:	Introduced in z/OS V1R4 by PTF UA00132 and rolled back to z/OS V1R3.
Applies to migration from:	z/OS V1R4 without PTF UA00132 installed.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you want to override the new default storage values and have not already done so as part of implementing PTF UA00132 or UA00131 in an earlier release.
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: Review the IVTPRM00 parmlib member for communications storage manager (CSM) fixed storage. If necessary, change the storage options as follows:

- Define how much storage VTAM keeps available for read processing for all OSA QDIO data devices by coding the QDIOSTG (QDIO storage) start option.

- Define how much storage VTAM keeps available for read processing for all HiperSockets (iQDIO) data devices using a maximum frame size (MFS) of 64 KB by coding the IQDIOSTG (iQDIO storage) start option.

Reference information:
- For information about reviewing and altering the IVTPRM00 parmlib member for CSM fixed storage, see *z/OS MVS Initialization and Tuning Reference*.
- For information about VTAM start options, see *z/OS Communications Server: SNA Resource Definition Reference*. For additional CSM information made available after the book was published, see informational APAR II13235.

SNA Services: Accept the VTAMMAP CSMCMPID ALLCMPID default change

Description: The default value of VTAMMAP CSMCMPID ALLCMPID has changed. Before z/OS V1R7, the default displayed the details of all the addresses of all CSM buffers currently used by all component IDs. As of z/OS V1R7, the default of ALLCMPID is to display the summary.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you want the display to show the details of the CSM buffers.
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: If you want the display to show the details of all the CSM buffers (as VTAMMAP CSMCMPID ALLCMPID did by default before z/OS V1R7), use the new DETAIL keyword with ALLCMPID. For example:

```
VTAMMAP CSMCMPID ALLCMPID DETAIL
```

Reference information: *z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures*.

SNA Services: Make changes to PPO, SPO, or CLISTs

Description: In z/OS V1R7, several VTAM display enhancements were introduced in regard to Enterprise Extender. These changes may affect operations of your Primary Program Operator (PPO), Secondary Program Operator (SPO), or existing CLISTs. The following display commands are affected:
- **DISPLAY NET,RTPS** — Message IST1454I, which shows the number of RTPs displayed, is no longer issued as part of this output. Instead, a new message, IST2084I, is issued.

  Message IST1454I follows:

  ```
  IST1454I  count  RTP(S) DISPLAYED
  ```

  New message IST2084 follows:

```
IST2084I  count  OF total  MATCHING RTP PIPES DISPLAYED
```
- **DISPLAY NET,SESSIONS,SID=** — New message IST2064I is an optional message that is issued in the display output when this command is issued on the application owning host. Message IST1635I displays a HSCB TYPE of FMCB for either the PLU, SLU, or both, when this display is issued at the application owning host. Message IST2064I has been inserted between existing messages IST1635I and IST1636I.

  Message IST2064I follows:
```
IST2064I PLU TO SLU RU SIZE = plu_to_slu_rusize
    SLU TO PLU RU SIZE = slu_to_plu_rusize
```
- **DISPLAY NET,ID=rtppuname,HPRDIAG=YES** — Three new messages, IST2085I, IST2086I, and IST2087I, have been included in the OUTBOUND TRANSMISSION INFORMATION section of the HPRDIAG display for an RTP PU. These new messages display information about the RTP outbound work queue. These new messages have been inserted between existing messages IST1978I and IST1511I.

  The new messages follow:
```
IST2085I NUMBER OF NLPS ON OUTBOUND WORK QUEUE = num_nlps
IST2086I MAXIMUM NUMBER OF NLPS ON OUTBOUND WORK QUEUE = max_num_nlps
IST2087I OUTBOUND WORK QUEUE MAX REACHED ON date AT time
```
- **D NET,ID=generic_resource,IDTYPE=GENERIC** — Message IST1360I has been modified to contain a new status for whether a generic resource is selectable. The new status is DEL, indicating the application was deleted as a generic resource. Previously, the status could only be YES or NO.
- **D NET,AUTOLOG,SCOPE=ALL** — A new message, IST2100I, is issued in the display output when there are LUs that have normally terminated their controlling application session with the named PLU. It is followed by one or more IST1997I messages listing those LUs. These messages are at the end of the IST1990I message group. Message IST2100I follows:
```
IST2100I pluname - NORMALLY LOGGED OFF LUS
```

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if your existing PPO, SPO, or CLISTs automate on the affected output displays.
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: Make any necessary changes to your automation procedures to handle the described display changes.

Reference information: For details about the VTAM display enhancements, see the following:

- Enterprise Extender enhancements and VTAM command to remove Generic Resource from a Sysplex in *z/OS Communications Server: New Function Summary*

- *z/OS Communications Server: SNA Operation*
- *z/OS Communications Server: SNA Diagnosis Vol 1, Techniques and Procedures*

SNA Services: Exclude new session failure RSCV messages

Description: Before z/OS V1R7, several session failure problems could have been more easily resolved if the Route Selection Control Vector (RSCV) that was computed and used for the session was displayed before the session information was freed. Therefore, z/OS V1R7 introduces a new VTAM start option, RSIRFSMG, that indicates that the RSCV data should be displayed (when available) for sessions that fail to reach the ACTIVE state.

In addition to introducing the new start option RSIRFSMG, z/OS V1R7 also changes the behavior of two existing start options. You can expect to see some new messages and existing messages issued in new cases. These changes might affect operations of your Primary Program Operator (PPO). Specifically, the behavior of the following two start options has changed:

- DSIRFMSG — New messages are optionally issued with the DSIRFMSG message group based on the new RSIRFMSG start option. The DSIRFMSG message group starting with IST663I is optionally issued when a search fails.
- SIRFMSG — New messages are optionally issued with the SIRFMSG message group based on the new RSIRFMSG start option. The SIRFMSG message group starting with IST663I is optionally issued when a session initiation request fails.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if your existing PPO, SPO, or CLISTs automate on the affected output displays, or if the new messages are not desired.
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: If you decide you want the new behavior, you should set the RSIRFMSG start option value appropriately for your system in your start list and you should be aware of the DSIRFMSG and SIRFMSG changes. If, however, you want to maintain the behavior of your previously existing system and have the same output as prior releases, you must explicitly specify RSIRFMSG=NONE on the START command or use the MODIFY VTAMOPTS,RSIRFMSG=NONE command.

Reference information: For details about excluding the new session failure RSCV messages or setting the RSIRFMSG start option value, see the following:

- VTAM start option to display RSCVs in *z/OS Communications Server: New Function Summary*
- *z/OS Communications Server: SNA Operation*
- *z/OS Communications Server: SNA Resource Definition Reference*

SNA Services: Prevent VTAM subarea nodes from automatically joining the ISTXCF sysplex group

Description: In z/OS V1R7, XCFINIT is supported as a start option on pure subarea VTAM nodes (nodes without the NODETYPE start option specified) and the default value for XCFINIT on a pure subarea node is XCFINIT=DEFINE. Therefore, if you have pure subarea VTAM nodes in your sysplex when you upgrade to z/OS V1R7, those nodes will automatically join the ISTXCF sysplex group. Furthermore, as they learn of other nodes in the sysplex group, they will add definitions for XCF connectivity to those nodes.

The XCF connectivity definitions can be used by TCP/IP to communicate across XCF to other stacks in the sysplex. If you do not want this to happen for a specific pure subarea VTAM node, you must add XCFINIT=NO to your start option list for that pure subarea VTAM node.

In z/OS V1R7, APPN nodes that specify an HPR start option value other than RTP and have the XCFINIT start option either specified as or defaulted to YES will have XCFINIT forced to DEFINE. Before z/OS V1R7, XCFINIT had been forced to NO.

If you do not want these APPN nodes to connect to the XCF group, you must add XCFINIT=NO.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you want to prevent an APPN node that specifies an HPR value other than RTP, or a pure subarea node, from joining the ISTXCF sysplex group.
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: If you have a subarea VTAM node that you want to prevent from automatically joining the ISTXCF sysplex group, add XCFINIT=NO to your start option list.

If you have an APPN node specifying an HPR value other than RTP and you do not want it to automatically join the ISTXCF sysplex group, add XCFINIT=NO to your start option list.

Reference information: For details about XCFINIT and the subarea VTAM XCF support, see the following:
- Subarea VTAM XCF support in *z/OS Communications Server: New Function Summary*
- *z/OS Communications Server: SNA Network Implementation Guide*
- *z/OS Communications Server: SNA Resource Definition Reference*

SNA Services: Eliminate messages caused by improved APPN search diagnostics

Description: A new VTAM start option, LSIRFMSG, is introduced to provide additional information to help diagnose the reason for APPN locate search failures using the IST663I message group. LSIRFMSG processing is affected by the SIRFMSG= and CPNAME= operands on CDRSC definitions. Therefore, you might see an increase in the number of messages that are displayed for resources that you currently have defined with these operands. If you have existing CDRSC definitions with SIRFMSG=ALLSSCP or SIRFMSG=OLUSSCP and CPNAME=, consider whether you still want SIRFMSG coded.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended to reduce the large number of messages that could be issued.
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: If you no longer want to see messages displayed as a result of SIRFMSG, DSIRFMSG, and LSIRFMSG processing, remove the SIRFMSG coding from CDSRC definitions.

Reference information:
- LSIRFMSG start option in *z/OS Communications Server: New Function Summary*
- *z/OS Communications Server: SNA Resource Definition Reference*
- *z/OS Communications Server: SNA Operation*
- *z/OS Communications Server: SNA Network Implementation Guide*

SNA Services: Adjust automation for changed RTP PU display responses

Description: Problems in the data link control (DLC) layer used by a High-Performance Routing (HPR) PU might cause data flow to stall. Before z/OS V1R6, the operator was not informed of the stall and there was no automatic recovery. Starting in z/OS V1R6, a stalled HPR pipe solution is provided to detect the stall, inform the operator, and attempt to recover. As a result of the stalled HPR pipe solution, there is a difference in some of the display RTP PU command responses. Specifically, stall information fields are included in the DISPLAY NET,RTPs and DISPLAY NET,ID=*name*,HPRDIAG=YES command responses. Because of these new fields, the message formats are changed and might adversely affect automation. The changed messages are IST1695I, IST1858I, and IST1859I. In addition, message IST1696I is replaced by message IST1960I.

Element or feature:	Communications Server.

When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if in the previous release you were using one or both of the display commands in the "Description" above and automating on the responses.
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: Change any programs that automate on IST1695I, IST1696I, IST1858I, and IST1859I to take into consideration the new format of the messages.

Reference information:
- *z/OS Communications Server: New Function Summary*
- *z/OS Communications Server: SNA Operation*

SNA Services: End automation on message EZZ4313I using Enterprise Extender

Description: If, in previous releases, you were using Enterprise Extender and automating on the message EZZ4313I to activate VTAM definitions, be aware that you can no longer do this as of z/OS V1R5. In previous releases, TCP/IP issued message EZZ4313I for MPCPTP devices before the LINK became active. In z/OS V1R5 Communications Server, TCP/IP does not issue message EZZ4313I until the LINK is marked active.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5 (Enterprise Extender and automating on message EZZ4313I).
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if in the previous release you were using Enterprise Extender and automating on the message EZZ4313I to activate VTAM definitions.
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: Change any programs that automate on message EZZ4313I to activate VTAM definitions, so that they no longer do so.

Reference information: None.

SNA Services: Accommodate host name resolution changes for Enterprise Extender

Description: In z/OS V1R5 Communications Server, the support for Enterprise Extender (EE) is enhanced to be IPv6 enabled. It is also enhanced to allow specification of a hostname when using either IPv4 or IPv6 addressing. Several changes were made in the area of hostname resolution with these enhancements that might require migration actions.

The default value of the IPRESOLV operand on the PATH statement is changed from 45 seconds to 0 seconds (no timeout). Also, a length limitation has been imposed on the HOSTNAME operand of the PATH statement in the Switched Major Node.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5 (IPv6 support for Enterprise Extender).
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you are currently using the default value for IPRESOLV.
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:

1. If you are currently using the default value for IPRESOLV, you must explicitly code IPRESOLV=45 on your Enterprise Extender PATH statements if you want z/OS V1R5 and later Communications Server to operate the same as it did in z/OS V1R4 Communications Server.

2. Be aware that the HOSTNAME operand on the PATH statement is limited to 64 characters in z/OS V1R5 and later Communications Server. IBM recommends that HOSTNAME be a fully qualified domain name. However, if making HOSTNAME a fully qualified domain name causes the 64 character limitation to be exceeded, only the hostname portion of the name can be specified. In this case, the hostname by itself could be mapped to an IP address by way of the IPNODES file or the local HOSTS files, or the resolver could append domain names, depending on your resolver configuration.

Reference information: For details about Enterprise Extender enhancements, see:

- *z/OS Communications Server: New Function Summary*
- *z/OS Communications Server: SNA Operation*
- *z/OS Communications Server: IPv6 Network and Application Design Guide*

SNA Services: Migrate exit routines and supporting files for IPv6 TN3270 capability

Description: VTAM supports the association of LU names with IP addresses when the APPL, LU, or CDRSC represents a TN3270 client. In z/OS V1R5 Communications Server, the TN3270 server supports IPv6 addresses. In addition, VTAM functions that provide the LU name and IP address association now support IPv6 addresses. You might need to make several changes to associated exit routines and supporting files.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5 (IPv6 support for SNA display of IP addresses).
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use TN3270 in an IPv6 environment.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	See the "Steps to take" below.
Restrictions:	None.
System impacts:	None.

Steps to take: In order to adjust to changes in TN3270 function in the IPv6 environment, follow these steps:

1. Consider the following incompatibilities and take appropriate action:

   - Changed messages. Applications that process the following messages must plan for the described changes:

     – IST1669I IPADDR..PORT ipaddr..portno: This message is part of a group of messages issued in response to a DISPLAY ID command for a TN3270 client LU , application resource, or CDRSC, or for a DISPLAY ID,IDTYPE=IPADDR command when only one TN3270 client LU or application is associated with the specified IP address. It is also part of the IST075I message group issued for D NET,TSOUSER. The ipaddr may now be either an IPv4 address displayed in dotted decimal or an IPv6 address displayed as colon hexadecimal.

     – IKT122I IPADDR..PORT ipaddr..portno: TSO/VTAM issues this message when a TN3270 client attempts to log on to TSO/VTAM but fails to do so. The ipaddr may now be either an IPv4 address displayed in dotted decimal or an IPv6 address displayed as colon hexadecimal.

   - When the SNA portion of the TN3270 session is cross-domain and the host where the PLU resides is downlevel (at least to OS/390 V2R10 Communications Server), the host where the PLU resides is not able to display an IPv6 address. Therefore, it would not display IP information for DISPLAY ID commands for CDRSC or for a DISPLAY ID, IDTYPE=IPADDR. Also, any VTAM exits that are associated with this session, such as LOGON or Session Management Exit, would not receive the TCP/IP Information Control Vector as input.

   - Users of the TSO/VTAM GTTERM macro that request IPADDR or DOMAIN information but have not made changes to support IPv6 information could

receive unpredictable results as output from this macro if the TN3270 client represents an IPv6 address. In this case, the IP address returned will be X'FFFFFFFF'. The port and the DNS name information (if present) will be returned.

Refer to *z/OS TSO/E Programming Services* for information on changes needed to support IPv6.

- TSO/VTAM exit IKTCASX1 — The IKTCASX1 exit parameter list structure, IKTWESTD contains the IP address of an associated TN3270 client in the WE_IP_ADDR field. Until now, this address could only be an IPv4 address. VTAM now supports an LU that is associated with an IPv6 TN3270 client. If the client is IPv6 and the exit has not been modified to support IPv6, the WE_IP_ADDR field will contain X 'FFFFFFFF', making the real IP address unavailable. To resolve this incompatibility, refer to *z/OS Communications Server: SNA Customization* for changes needed to support IPv6.

- USSMSG macro Buffer operand — Before z/OS V1R5 Communications Server, the USSMSG macro's BUFFER operand allowed for IP address substitution using @@@@@@@@@IPADDR, which represents the length of a textual IPv4 address. If an existing USSMSG BUFFER is coded to specify this string, but the IP address associated with the TN3270 client is an IPv6 address, the address will be replaced with the text IPV6 ADDRESS, making the real client IP address unavailable. Refer to *z/OS Communications Server: SNA Resource Definition Reference* for the new IPv6 substitution string.

2. Allow CMIP Topology Managers to support an LU that is associated with an IPv6 TN3270 client. To do this, modify CMIP Topology Managers to accept the LU attribute of tn3270ClientIpAddress. It has been expanded to allow a CMIP Topology Manager to display an LU that is associated with an IPv6 TN3270 client.

Reference information: For details about using IPv6 support for SNA display of IP addresses, see:

- *z/OS Communications Server: SNA Customization*
- *z/OS Communications Server: CMIP Services and Topology Agent Guide*
- *z/OS Communications Server: SNA Resource Definition Reference*
- *z/OS Communications Server: New Function Summary*
- *z/OS Communications Server: IPv6 Network and Application Design Guide*
- *z/OS TSO/E Programming Services*

SNA Services: Use CSM buffer tracking to help diagnose storage problems

Description: The CSM monitor function is available to monitor CSM buffers between many components of z/OS Communications Server. This function is used by IBM Software Support to help diagnose CSM storage problems. This function can be controlled using the Modify CSM command with the MONITOR operand.

As a result of a CSM buffer tracking enhancement, z/OS V1R5 and later Communications Server will operate differently than previous releases if the default value for the CSM MONITOR function (DYNAMIC) is used. You must set CSM MONITOR to OFF in order for this to operate as it did previously.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5 (CSM buffer tracking).

Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended to assist in problem determination.
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: The default value for CSM MONITOR is DYNAMIC. IBM recommends that you keep the CSM MONITOR value as DYNAMIC. If you choose to maintain the CSM behavior of previous releases, you can turn CSM MONITOR off using the following command: F procname,CSM,MONITOR=OFF.

Reference information: For details about CSM buffer tracking, see *z/OS Communications Server: SNA Operation*.

SNA Services: Use the MAXSLOW parameter for slowdown monitoring

Description: A MAXSLOW parameter for slowdown monitoring is added in z/OS V1R5 Communications Server. The default value for detecting an extended period of an XCA subchannel slowdown is 180 seconds.

Before this function, an operator could not determine and was not made aware that an XCA subchannel was in slowdown.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5 (MAXSLOW parameter for slowdown monitoring).
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you want to know if the XCA subchannel is in slowdown.
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: Be aware of the MAXSLOW parameter for slowdown monitoring. It is specified on the XCA port definition statement where a CUADDR is specified. You can follow these steps:

1. Determine if an XCA device is in slowdown by issuing the following command: D net,ID=xca_major_node.
2. Set the slowdown time value for an XCA device to 200 seconds for operator notification by coding MAXSLOW=(,200) on the XCA major node.

3. Optionally add the steps above to appropriate automation scripts.

Reference information: For details about the MAXSLOW parameter for slowdown monitoring, see:

- *z/OS Communications Server: SNA Operation*
- *z/OS Communications Server: SNA Resource Definition Reference*

SNA Services: Adjust automation for additional SNA session setup messages

Description: z/OS V1R5 Communications Server provides three areas of enhancement for session setup and problem determination:

- DSIRFMSG start option
- Allow non-sysplex network nodes (NNs) for generic resource (GR) end nodes (ENs)
- SSCPORD search option

As a result of the DSIRFMSG start option enhancement, there is an operational difference between z/OS V1R5 and later Communications Server and previous releases when SIRFMSG=OLUSSCP or ALLSSCP is coded on a CDRSC definition statement. Previously, this resulted in the IST663I message group being issued whenever a SESSION SETUP search fails and the CDRSC in question represents the OLU or DLU of the search. In z/OS V1R5 and later Communications Server, this same setting for the SIRFMSG operand on CDRSCs results in the IST663I message group also being displayed for searches that do not result in sessions.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R5 (session setup and problem determination enhancements).
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if SIRFMSG=OLUSSCP or ALLSSCP is coded on a CDRSC definition statement.
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: Be aware of the operational difference when SIRFMSG=OLUSSCP or ALLSSCP is coded on a CDRSC definition. Consider whether you still want the SIRFMSG operand coded on CDRSC definitions. Modify any automation programs that might be adversely affected by the additional message group display.

Reference information: For details, see:

- *z/OS Communications Server: New Function Summary*
- *z/OS Communications Server: SNA Resource Definition Reference*

Communications Server actions to perform after the first IPL of z/OS V1R7

This section describes Communications Server migration actions that you can perform only after you've IPLed z/OS V1R7. You need a running z/OS V1R7 system to perform these actions.

IP Services: Rejoin a sysplex group

Description: In z/OS V1R7, a new keyword, AUTOREJOIN/NOAUTOREJOIN, was added to the SYSPLEXMONITOR parameter on the GLOBALCONFIG statement in the TCP/IP profile to control whether the TCP/IP stack should automatically rejoin the sysplex group when all detected problems (that caused the stack to leave the group) have been relieved. The default value of the parameter is to disable this function and not to automatically rejoin the sysplex group. However, even if you choose to not use the new function and you do not change the default to enable it, you will still see some changes.

Specifically, starting in z/OS V1R7, when a stack leaves the sysplex group (either by the VARY TCPIP,,SYSPLEX,LEAVEGROUP command, or by the Sysplex Autonomics function), you will notice the following changes:

- The stack's VIPADYNAMIC configuration information is no longer discarded when the stack leaves the sysplex group. Instead, it is saved and restored when the stack rejoins the group.
- The way to cause the stack to rejoin the sysplex group has changed.
- DYNAMICXCF and VIPADYNAMIC statements are ignored when the stack has left the sysplex group. However, as with the previous release, existing DYNAMICXCF links remain active but new DYNAMICXCF links cannot be activated while the stack is out of the sysplex group.

In addition, the Netstat VIPADCFG/-F report has changed in z/OS V1R7. See *z/OS Summary of Message and Interface Changes* for details about how Netstat reports have changed.

Note: Although the default keeps the stack from automatically rejoining the sysplex group, it is recommended that you enable this function; it is intended to benefit you. To enable it, specify the existing keyword RECOVERY and the new keyword AUTOREJOIN. The documents listed in "Reference information" below include more information.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you want the stack to automatically rejoin the sysplex group (without operator intervention) after all detected problems are cleared.
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: If a stack leaves the sysplex group (either by the VARY TCPIP,,SYSPLEX,LEAVEGROUP operator command or by the Sysplex Autonomics function), running an OBEYFILE containing DYNAMICXCF and/or VIPADYNAMIC statements no longer causes the stack to rejoin the sysplex group, and any DYNAMICXCF or VIPADYNAMIC statements are ignored while the stack has left the group.

Two new ways of rejoining the sysplex group are now available: by operator command and automatically. The method used depends on how the stack left the group and how the stack is configured.

- **After leaving the sysplex group by operator command:** If you use the VARY TCPIP,,SYSPLEX,LEAVEGROUP operator command to take the stack out of the sysplex group, do the following to cause the stack to rejoin the group and restore its saved VIPADYNAMIC configuration:
  1. Use the VARY TCPIP,,SYSPLEX,DEACTIVATE operator command to deactivate any DVIPA that you do not want restored when the stack rejoins the sysplex group.
  2. Issue the VARY TCPIP,,SYSPLEX,JOINGROUP operator command.
- **After leaving the sysplex group automatically:** If the Sysplex Autonomics function detects a problem and takes the stack out of the sysplex group, choose the appropriate action for your configuration:
  - Configure AUTOREJOIN. When it is configured, the stack automatically rejoins the group and restores its saved configuration when the sysplex monitor determines that all detected problems have been relieved. (See Summary of problems monitored and actions taken in *z/OS Communications Server: IP Configuration Guide* for specific details about the different monitored conditions.)
  - Configure NOAUTOREJOIN (or simply do nothing; it is the default). When it is configured, the stack does not automatically rejoin the group. In this case, to cause the stack to rejoin the group and restore its saved configuration, do the following:
    1. Use the VARY TCPIP,,SYSPLEX,DEACTIVATE operator command to deactivate any DVIPA that you do not want restored when the stack rejoins the sysplex group.
    2. Issue the VARY TCPIP,,SYSPLEX,JOINGROUP operator command.

Reference information: For details about rejoining a sysplex group, see the following:

- Operator commands for DVIPA management in *z/OS Communications Server: New Function Summary*
- *z/OS Communications Server: IP Configuration Guide*
- *z/OS Communications Server: IP Configuration Reference*
- *z/OS Communications Server: IP System Administrator's Commands*

IP Services: Run the TN3270E Telnet server as a separate address space

Description: The TN3270E server can now run in a separate address space from the TCP/IP stack address space. This enhancement provides visibility and control over the TN3270 function separate from the TCP/IP stack. For example, users can

run the TN3270 server at a different priority than the TCP/IP stack. The enhancement also provides the ability to stop and restart the TN3270 server without stopping the TCP/IP stack. This makes it easier to reset the server or install maintenance. Overall, problem diagnosis is easier and better when the TN3270 server and the TCP/IP stack are separate.

If desired, users can continue to run the TN3270E server as part of the TCP/IP address space.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended in order to take advantage of the benefits described in "Description" above.
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:

1. Set up a superuser user ID with an OMVS segment, which may include adding a RACF user ID. See the Telnet chapter in *z/OS Communications Server: IP Configuration Guide* for details.
2. Associate a RACF user ID with the Telnet procedure using the RACF STARTED class or other equivalent security measure.
3. In z/OS V1R6, the default program property table (PPT) has been updated for the EZBTNINI program. Ensure that your SCHED*xx* parmlib member does not specify EZBTNINI or modify the IBM defaults for EZBTNINI (NOCANCEL, KEY(6), PRIV, NOSWAP, and SYST).
4. Change the priority of Telnet by assigning Telnet to a service class other than the default SYSSTC class in the STC subsystem.
5. Remove the TN3270E Telnet server profile statements from the TCP/IP profile.
6. Create JCL to run Telnet in its own address space. The Telnet profile statements data set is specified in the JCL. Samples of each are in hlq.SEZAINST. Member EZBTNPRC contains the JCL sample and member TNPROF contains a sample profile.
7. Update any automated operator scripts to specify the name of the Telnet address space as the PROCNAME field in any DISPLAY or VARY commands for TELNET options.

   Restriction: The obsolete options described for the DISPLAY TCPIP,,TELNET command are not supported by the Telnet server address space. Any use of these will also need to be converted to the equivalent ObjectID or ClientID forms. For further details, see *z/OS Communications Server: IP System Administrator's Commands*.

Once these steps are done, the stand-alone Telnet JCL can be started.

Reference information:
- TN3270E server address space option in *z/OS Communications Server: New Function Summary*
- *z/OS Communications Server: IP Configuration Guide*
- *z/OS UNIX System Services Planning*
- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Security Server RACF Command Language Reference*

IP Services: Use multilevel security configuration consistency check

Description: Secure communication in a multilevel-secure environment requires configuration of several statements in the TCPIP.PROFILE and security server resource profiles in the SERVAUTH, SECLABEL, and STARTED classes. Inconsistencies in this configuration can allow unintended communication or prevent intended communication.

When the RACF MLACTIVE option is set, TCP/IP automatically checks the TCPIP.PROFILE and security server resource profiles for consistency. Consistency checking occurs at TCP/IP initialization when a VARY,TCPIP,,OBEYFILE command is processed and when a RACLIST REFRESH is done on the SERVAUTH or SECLABEL class.

TCP/IP writes an informational message to the job log for each inconsistency detected. If inconsistencies are found, a final message, EZD1217I, summarizing the number of problems found is written to the system console.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended in a multilevel-secure environment to remove inconsistencies found in your TCPIP.PROFILE and security server resource profiles.
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: While running with the RACF MLACTIVE option active:

1. Specify NOMLSCHECKTERM on the GLOBALCONFIG statement in the TCPIP.PROFILE to continue running the TCP/IP stack when inconsistent configuration information is detected.
2. Check the job log for messages in the range EZD1218I–EZD1234I whenever message EZD1217I appears on the system console.
3. Correct your configuration as indicated by the job log messages until TCP/IP no longer detects any errors.

4. Specify MLSCHECKTERM on the GLOBALCONFIG statement in the TCPIP.PROFILE to bring down the TCP/IP stack when inconsistent configuration information is detected.

Reference information: For details about using multilevel security configuration consistency check, see the following:

- Multilevel security configuration consistency check in *z/OS Communications Server: New Function Summary*
- *z/OS Communications Server: IP Configuration Reference*
- *z/OS Communications Server: IP Configuration Guide*

IP Services: Make changes to continue using old X Windows System and Motif libraries

Description: z/OS V1R6 and later Communications Server provides new versions of the X Window System and Motif libraries. The new libraries are based upon X Window System X11R6.6 and Motif 2.1.30.

The old X Window System and Motif libraries (X11R6.1 and Motif 1.2) are still provided and are compatible with existing programs. They are compiled with 31-bit non-XPLINK and use IBM Hexadecimal Floating Point. These DLLs do not contain new function. Existing applications that use the old libraries will continue to run unchanged. However, if you want to compile and link with the old libraries, some changes are necessary to use the correct headers and libraries.

Element or feature:	Communications Server.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you want to continue using the old X Window System and Motif libraries (X11R6.1 and Motif 1.2).
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: If you want to recompile existing 31-bit X Window applications to use the old libraries (X11R6.1 and Motif 1.2) and the old header files for these releases, then you must change your makefile or JCL to use the -I option and specify the HFS directory that contains the old header files. For example, specify `-I/usr/lpp/tcpip/X11R6/include`. If you do not do this, your application will pick up the new header files by default and might not compile or operate correctly. For static linkage, the library names have not changed. However, the symbolic links from /usr/lib now point to the new libraries. To use the old static libraries, use the -L option on the link step to tell the binder where to find the X and Motif libraries. For example, specify `-L/usr/lpp/tcpip/X11R6/lib`. For dynamic linkage, the DLL and side deck names have not changed.

Be aware that the C++ class wrapper programming interface to Motif is no longer supported by the new Motif libraries. If you require this function, then you must continue to use the Motif 1.2 libraries or change your application.

Reference information:

- Support 64-bit virtual addresses for X Windows and Motif in *z/OS Communications Server: New Function Summary*
- *z/OS Communications Server: IP Programmer's Guide and Reference*

Chapter 7. Cryptographic Services migration actions

This chapter 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).

PKI Services is new in Cryptographic Services. Before z/OS V1R5, PKI Services was in optional feature Security Server.

Some Cryptographic Services data sets have been removed from z/OS. See "Remove references to deleted data sets and paths" on page 40.

Note: This chapter contains a migration action that pertains to z990 and z890 servers: "ICSF: Add new services to the CICS wait list." For the rest of the z990 and z890 migration actions, see "Migrate to a z990 or z890 server" on page 74.

Cryptographic Services actions to perform before installing z/OS V1R7

This section describes Cryptographic Services migration actions that you can perform on your current (old) system. You don't need the z/OS V1R7 level of code to make these changes, and the changes don't require the z/OS V1R7 level of code to run once they are made.

ICSF: Add new services to the CICS wait list

Description: If you are using the CICS-ICSF Attachment Facility and you specify your own CICS wait list data set, you need to modify the wait list data set to include the new services listed in "Steps to take" below.

Element or feature:	Cryptographic Services.
When change was introduced:	z990 Cryptographic Support Web deliverable (which contains FMID HCR770A; the FMID is integrated in z/OS V1R6).
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4, all without the Cryptographic Support for z/OS V1R6/R7 and z/OS.e V1R6/R7 Web deliverable installed. (The Web deliverable contains FMID HCR7730.)
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you use the CICS-ICSF Attachment Facility and you specify your own CICS wait list data set.

Target system hardware requirements:	One of the following hardware features: • The Crypto Express2 feature on a z9-109 server • The PCI X Cryptographic Coprocessor (PCIXCC) feature on a z990 or z890 server • The PCI Cryptographic Coprocessor (PCICC) feature on a z900 or z800 server
Target system software requirements:	See *z/OS Cryptographic Services ICSF System Programmer's Guide*.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	See *z/OS Cryptographic Services ICSF System Programmer's Guide*.

Steps to take: Modify your CICS wait list data set to include the following services:

* If your z9-109 server has the Crypto Express2 hardware feature, or your z990 or z890 server has the PCIXCC hardware feature, include:

    CSNBCKI
    CSNBCKM
    CSNBDEC
    CSNBDKG
    CSNBENC
    CSNBKTC
    CSNBKYTX
    CSNBMGN
    CSNBMVR
    CSNBPEXX
    CSNBRNG
    CSNBSKY
    CSNBSPN

    In addition, if z/OS has the z990 and z890 Enhancements to Cryptographic Support Web deliverable (which contains FMID HCR770B) or a later Web deliverable (FMID HCR7720 or HCR7730) installed, include:

    CSFIQF
    CSNBPCU
    CSNBTRV

* If your z900 or z800 server has the PCICC hardware feature, and if z/OS has the z990 and z890 Enhancements to Cryptographic Support Web deliverable (which contains FMID HCR770B) or a later Web deliverable (FMID HCR7720 or HCR7730) installed, include:

    CSFIQF

Reference information: *z/OS Cryptographic Services ICSF System Programmer's Guide*.

System SSL: Migrate to JSSE for secure socket support

Description: As of z/OS V1R6, System SSL Java class support is removed from z/OS. Applications that need to use SSL function through Java classes must use JAVA Secure Socket Extension (JSSE), which is included in the product SDK for z/OS, Java 2 Technology Edition, V1 (5655-I56).

Element or feature:	Cryptographic Services.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you use System SSL to obtain SSL function through Java classes.
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: Follow the instructions at
http://www.ibm.com/developerworks/eserver/articles/migra_zos.html.

Reference information: For an overview of IBM JSSE, see
http://www.ibm.com/servers/eserver/zseries/software/java/jsse14.html.

Cryptographic Services actions to perform before the first IPL of z/OS V1R7

This section describes Cryptographic Services migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

OCSF: Migrate the directory structure

Description: If you had previously installed Open Cryptographic Services Facility (OCSF), you need to verify that the OCSF directories have been migrated to the target system.

Element or feature:	Cryptographic Services.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

Steps to take: Migrate the OCSF `/var` directory structure to the target system. If you installed z/OS V1R7 with CBPDO or by cloning an already-installed V1R7 system, you can either copy the `/var/ocsf` directory from your old system or rerun the installation script. If you installed z/OS V1R7 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 stated above).

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 32. 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++ run-time 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 define user IDs for that class:
   - 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++ run-time 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: *z/OS Open Cryptographic Services Facility Application Programming*.

PKI Services: Add VSAM alternate indexes

Description: VSAM alternate indexes must be added to access the ObjectStore data set and the issued certificate list (ICL) data set of PKI Services. PKI Services will not initialize after z/OS V1R5 or later is installed unless alternate indexes are added.

Element or feature:	Cryptographic Services.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use PKI Services.
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: First, if you run multiple instances of PKI Services in a Parallel Sysplex (one per image), perform the steps described in the "(Optional) preliminary steps for establishing VSAM RLS" chapter of *z/OS Cryptographic Services PKI Services Guide and Reference*.

Then, add VSAM alternate indexes to access the ObjectStore and ICL data sets using the following steps:

1. Copy the sample JCL in 'SYS1.SAMPLIB(IKYMVSAM)' to your JCL data set.

2. Update your data set as directed in the instructions in the prolog of the sample JCL:

   a. Change the JOB card.

   b. Change the VOL statements.

      - If you are using VSAM record level sharing, remove the VOL statements.

      - If you are not using VSAM record level sharing, replace the *vvvvv* in the VOL statements with a `VOL=SER` suitable for your VSAM data sets.

   c. You can optionally change the data set names but remember to make equivalent changes in the `pkiserv.conf` file if you do so.

   d. Update the primary and secondary extent track allocations based on your anticipated future needs. The default allocations on the **DEFINE ALTERNATEINDEX** statements for alternate indexes is `TRK(5,1)`.

   Recommendation: Do not change any numeric values, other than the primary and secondary space allocation values for the alternate index data sets.

3. Submit the job when your changes are complete.

Reference information: For guidelines on determining the space you will need and other details about adding alternate indexes, see *z/OS Cryptographic Services PKI Services Guide and Reference*.

Cryptographic Services actions to perform after the first IPL of z/OS V1R7

This section describes Cryptographic Services migration actions that you can perform only after you've IPLed z/OS V1R7. You need a running z/OS V1R7 system to perform these actions.

ICSF: Initialize the PKDS

Description: You must initialize the public key data set (PKDS) if it is not already initialized.

Element or feature:	Cryptographic Services.
When change was introduced:	z/OS V1R4 with the z990 Cryptographic Support Web deliverable (FMID HCR770A).
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if the PKDS is not already initialized.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	See *z/OS Cryptographic Services ICSF Administrator's Guide*.

Steps to take: Start ICSF and ensure that the master keys (SYM-MK, ASYM-MK, DES, and PKA) are valid. Initialize the PKDS using the ICSF ISPF panels.

Reference information: *z/OS Cryptographic Services ICSF Administrator's Guide*.

Chapter 8. DFSMS migration actions

This chapter describes migration actions for base element DFSMSdfp and optional
features DFSMSdss, DFSMShsm, DFSMSrmm, and DFSMStvs.

DFSMS actions to perform before installing z/OS V1R7

This section describes DFSMS migration actions that you can perform on your
current (old) system. You don't need the z/OS V1R7 level of code to make these
changes, and the changes don't require the z/OS V1R7 level of code to run once
they are made.

Redefine existing VSAM data sets that contain the IMBED, REPLICATE, and KEYRANGE attributes

Description: No supported release of z/OS allows you to use the IMBED,
REPLICATE, and KEYRANGE attributes for new VSAM data sets. In fact, using
these attributes can waste DASD space and often degrades performance. Servicing
these VSAM data sets has become increasingly difficult. In some cases, unplanned
outages have occurred. To provide an environment in which outages are less likely,
IBM has announced the intent to remove (in a future release) the support in existing
VSAM data sets for the IMBED, REPLICATE, and KEYRANGE attributes.

IMBED and REPLICATE were intended as performance improvements and have
been obsoleted by newer, cached DASD devices. Striped data sets provide much
better performance than KEYRANGE and should be viewed as a candidate for any
existing KEYRANGE data sets.

Element or feature:	DFSMSdfp.
When change was introduced:	Support in existing VSAM data sets for the IMBED, REPLICATE, and KEYRANGE attributes will be removed in a future release. (The specific future release has not been announced as of this writing.)
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	No, but recommended because it will become a requirement 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.

Steps to take:

1. Determine which VSAM data sets were defined with the IMBED, REPLICATE, or KEYRANGE attribute. To help you perform this task, you can get a tool that reads existing VSAM data sets and reports which ones have these attributes. The tool is available from the software server (ftp.software.ibm.com) in the s390/mvs/tools directory as IMBDSHIP.JCL.TRSD. Download the file in binary format and unterse it on your z/OS system using TRSMAIN. Instructions for using the tool are included in the downloaded JCL. See APAR II13894 for additional information.

2. Install the PTF for APAR OA10952. The PTF fixes the problem in which an exported copy of a VSAM data set that has the IMBED or REPLICATE attribute (or both) does not remove the attribute when the IMPORT is done. Note that this change helps further remove, through normal processing, data sets that have the IMBED or REPLICATE attribute. The PTFs for APAR OA10952 are UA17230 for z/OS V1R6, UA17229 for z/OS V1R5, and UA17237 for z/OS V1R4.

3. Schedule a time for the affected VSAM data sets to be unavailable, and redefine them.

Reference information: For information about using the DFSMSdss COPY command to move data sets, see *z/OS DFSMSdss Storage Administration Guide* and *z/OS DFSMSdss Storage Administration Reference*.

Convert ISAM data sets and programs to VSAM

Description: In z/OS V1R7, IBM removed most support for the indexed sequential access method (ISAM) and indexed sequential data sets. Users are no longer able to process (create, open, copy, or dump) ISAM data sets. Current ISAM data sets can still exist, and users can display information about them and delete them. Before migrating to z/OS V1R7, any ISAM data sets still in use should be copied or converted to VSAM data sets. Subject to existing restrictions, programs that use ISAM will continue to work using the ISAM interface to VSAM.

Element or feature:	DFSMSdfp.
When change was introduced:	z/OS V1R7.

Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you have ISAM data sets in use or programs that use ISAM.
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:

1. Find out if you have ISAM data sets or programs that use ISAM:

   For data sets: If you know your system has no ISAM data sets, you do not have to take migration steps. If you are not sure whether your system has ISAM data sets in use, you can take one of the following actions to find out:

   - Check for SYS1.ISAMLPA — if SYS1.ISAMLPA is not in your existing LPA concatenation or LINKLST concatenation, then programs are not using ISAM to access ISAM data sets. (They could still be using the ISAM interface to VSAM.) Note that the system data set SYS1.ISAMLPA and the distribution library SYS1.AOSD8 no longer exist in z/OS V1R7. If SYS1.ISAMLPA is in your LPA concatenation, you should remove it. This will save you about 177,528 bytes below the 16 MB line in LPA. Removing this will not affect programs that use the ISAM interface to VSAM data sets.

   - Use the DCOLLECT function of IDCAMS to search online volumes for a data set that has IS or ISU indicated for the DSORG value.

   - Check system logs for message IEC134I – starting in OS/390 V2R10, this message has been issued whenever ISAM data sets are opened, to warn that ISAM support is being discontinued.

   For programs: To find programs that use ISAM services, do the following:

   - Search for DSORG=IS in assembler source code and JCL. It appears on the DCB macro for BISAM and QISAM and on the DD statements. Search for equivalent statements in COBOL and PL/I programs. Then find the data sets used by these programs or JCL.

   - It is possible that you have an assembler language program that uses certain internal IBM macros that are no longer distributed. They were previously shipped in the SYS1.AMODGEN macro library. Their names, and any alternatives to use, are:

     – IGGDEBD. As an alternative, use the regular mapping macro, IEZDEB. It is documented for EXCP use in *z/OS DFSMSdfp Advanced Services*

     – IGGIOBD. As an alternative, use the regular mapping macro, IEZIOB. It is documented for EXCP use in *z/OS DFSMSdfp Advanced Services*

     – IGGLDCP. This macro only maps areas that are internal to ISAM.

     – IGGLOAD. This macro only maps areas that are internal to ISAM.

     – IGGSCAN. This macro only maps areas that are internal to ISAM.

     – IGGWKNCP. This macro only maps areas that are internal to ISAM.

   - Look for any invocations of the IEBISAM utility program and remove them or ensure that they are not used.

2. For ISAM data sets and the programs that use them, take one of the following actions before migrating to z/OS V1R7:
    *   Delete the data sets or programs if they are no longer needed.
    *   Copy the data to VSAM data sets and switch to using the ISAM interface to VSAM.
    *   Convert the programs and data sets to VSAM.

Reference information: For details about converting data sets and programs to use the ISAM interface to VSAM, see Appendix E in *z/OS DFSMS Using Data Sets*. For details about converting data sets directly to VSAM, see IDCAMS REPRO information in *z/OS DFSMS Access Method Services for Catalogs*.

Remove the CATALOG parameter from DEFINE PAGESPACE commands unless RECATALOG is specified

Description: Before z/OS V1R7, it was possible to specify a catalog on the access method services command to define a new page space. However, IBM recommended against the use of this CATALOG parameter because it could conflict with the allocate specifications for the main page space data set. As of z/OS V1R7, the CATALOG parameter is no longer supported on the AMS DEFINE PAGESPACE command unless it is used together with the RECATALOG parameter. Commands specifying the CATALOG parameter without RECATALOG will fail with message IDC3171I.

Element or feature:	DFSMSdfp.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you specified the CATALOG parameter on a DEFINE PAGESPACE command without the RECATALOG parameter.
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: In jobs that issue the access method services DEFINE PAGESPACE command with the CATALOG parameter, delete the CATALOG parameter unless the RECATALOG parameter is also specified.

Reference information: For details about the DEFINE PAGESPACE command, see *z/OS DFSMS Access Method Services for Catalogs*.

Ensure that the DFSMShsm journal is allocated correctly

Description: The DFSMShsm journal data set must be allocated with the following attributes:
*   Single volume
*   Single extent
*   Contiguous space

- No secondary space allocation
- Non-striped

Before z/OS V1R7, definition of the attributes was not enforced by the DFSMShsm code even though the attributes were documented in *z/OS DFSMShsm Implementation and Customization Guide*. Starting with z/OS V1R7, their definition is enforced by the code. Therefore, you should make sure that you've defined your journal data set correctly.

Element or feature:	DFSMShsm
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
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.

Steps to take: Review the data set organization for the DFSMShsm journal. Failure to define the journal with the attributes in "Description" above causes DFSMShsm to shut down. These attributes are required even if you use a large format data set for the journal.

Reference information: For the steps required to define the DFSMShsm journal, see *z/OS DFSMShsm Implementation and Customization Guide*.

Evaluate the need to increase DFSMSrmm control data set size

Description: As of z/OS V1R5, the required space for your DFSMSrmm control data set increases over time. This requirement for additional space is caused by an increase in the size of the volume record caused by APAR OW56584 and extended bin support when it is enabled. For example, each time a volume record is updated (such as during inventory management) or a new data set is written on a volume, the associated control data set volume records migrate to a new level dynamically. This increases the size of the volume record by 64 bytes. When extended bin support is enabled, the size of the bin records also increases by 24 bytes if the move is to or from a bin-managed storage location. In addition, larger control data set records for volumes and bins require larger journal records.

Element or feature:	DFSMSrmm.
When change was introduced:	z/OS V1R5 by APAR OW56584.
Applies to migration from:	z/OS V1R4.
Timing:	Before installing z/OS V1R7.
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.

Steps to take:

1. Determine how much additional space you need for the DFSMSrmm control data set for updated volumes and if extended bin support is enabled. To do this, multiply the number of volumes by 64 and then add that number to the number of bin records multiplied by 24. This equals the amount of additional space required for records.

2. Confirm that the additional space needed is available in your DFSMSrmm control data set as imbedded free space. To find out, list the catalog entry for your DFSMSrmm control data set and compare the High Allocated RBA and the High Used RBA for the DATA component. Ensure that the difference is at least equal to the additional space required for your control data. Knowing how much additional space is required in your DFSMSrmm control data set for records is different than how much space VSAM needs to manage the records that grow in size. For example, if there is no free space available in a VSAM Control Interval or Control AREA, a CI/CA split is required. Each split effectively doubles the amount of space occupied by the CI/CA after the split. As an example, if your DFSMSrmm control data set was loaded using FREESPACE(0 0), it is likely that the DFSMSrmm control data set needs to almost double in size to handle the longer records. However, if you followed the recommendations in the DFSMSrmm samples and *z/OS DFSMSrmm Implementation and Customization Guide*, it is likely that the records can grow in place and avoid CI/CA splits. Review the list catalog output and use your judgment to decide on what action, if any, is needed.

3. Secondary space should be defined for the DFSMSrmm control data set and, when needed, VSAM simply allocates a new secondary extent. If your DFSMSrmm control data set is near the maximum size, consider reallocating a larger control data set or reorganizing the control data set.

4. Review the latest recommendations for allocation of the DFSMSrmm control data set, in particular, the changes to FREESPACE and CISZ. Even if you do not enlarge your DFSMSrmm control data set, using EDGBKUP with BACKUP(REORG) to reorganize your control data set and implement the recommended FREESPACE(15 0) reduces the amount of VSAM CI/CA splits during inventory management as the volume records increase in size over time.

5. Also, DFSMSrmm writes an additional 0.3 KB to the journal for each confirm of a move into, and for each start of a move from, a bin-managed storage location. When running inventory management with parameter STORE(INSEQUENCE), DFSMSrmm writes an additional 1.6 KB to the journal for each start of a move into a bin-managed storage location. Thus, ensure that the journal data set is large enough that it does not get full during inventory management.

Reference information: For an overview of the latest recommendations for allocation of the DFSMSrmm control data set, see *z/OS DFSMSrmm Implementation and Customization Guide*.

Remove security-related parameters from IDCAMS ALTER

Description: As of z/OS V1R5, security information is no longer supported in catalogs. As a result, security-related parameters are no longer supported on the

IDCAMS ALTER command. The unsupported parameters are READPW, UPDATEPW, MASTERPW, CONTROLPW, ATTEMPTS, CODE, and AUTHORIZATION. An attempt to alter a data set's security information using any of those parameters results in message IDC3009I with return code 18 and reason code 12.

Element or feature:	DFSMSdfp
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you use the ALTER command with any of the security-related parameters listed in "Description" above.
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: Remove security-related parameters from the ALTER command.

Reference information: *z/OS DFSMS Access Method Services for Catalogs* and *z/OS DFSMS Managing Catalogs*.

DFSMS actions to perform before the first IPL of z/OS V1R7

This section describes DFSMS migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

Ensure that the Language Environment run-time library is available for DLLs

Description: Language Environment provides common services and language-specific routines in a single run-time environment. You can use Language Environment to build and use dynamic link libraries (DLLs) for applications.

Element or feature:	DFSMSdfp.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

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 run-time libraries (SCEERUN and SCEERUN2), or each job that creates or uses a DLL must include a STEPLIB DD statement referencing these libraries.

Reference information:
- *z/OS Language Environment Run-Time Application Migration Guide*
- *z/OS Language Environment Customization*
- *z/OS Language Environment Programming Guide*

.

Build the IPLable stand-alone DFSMSdss image

Description: If you intend to use the Stand-Alone Services provided by DFSMSdss, you must use the DFSMSdss BUILDSA function to create the Stand-Alone Services IPL-capable core image.

Element or feature:	DFSMSdss.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you intend to use the Stand-Alone Services provided by DFSMSdss.
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:	• 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.
	• If you IPL from DASD and later change the volume serial number, you must rerun the BUILDSA function to create a new core image data set with the new volume serial number in the name.

Steps to take:

1. Prepare for Stand-Alone Services by creating a Stand-Alone Services IPLable core image with the BUILDSA command. With the BUILDSA command you can

specify the device (card reader, tape drive, or DASD volume) from which Stand-Alone Services will be IPLed. You can also specify the operator console to be used for Stand-Alone Services.

The BUILDSA function builds the IPLable core image under the current operating system and determines a record size based on whether the IPL is from card, tape, or DASD.

2. Use RACF or another external security system to protect the SYS1.ADR.SAIPLD.V*volser* data set and the Stand-Alone Services modules.

3. If you haven't done so already, make 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 Guide*.

Reference information:
- *z/OS DFSMSdss Storage Administration Reference*

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.

Element or feature:	DFSMSdfp.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

Steps to take:

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*.

Use the catalog search order instead of JOBCAT and STEPCAT

Description: As a first step toward removal of the DFSMSdfp JOBCAT and STEPCAT facilities, in z/OS V1R5 the JOBCAT and STEPCAT DD statements were disabled by default, but you could still enable or disable them. Now, in z/OS V1R7, they have been removed and you can no longer enable or disable them.

By way of background, the JOBCAT and STEPCAT facilities have been in existence for many years, predating the introduction of ICF (integrated catalog facility) catalogs. JOBCAT and STEPCAT were designed to address some of the functional shortcomings of VSAM catalogs, such as:

- VSAM volume ownership, that is, all data sets on a volume having to be in the same VSAM catalog. Multiple catalogs could not point to data sets on the same volume.
- Performance problems resulting from no multilevel alias support, as well as lack of ability to subset catalog data for recovery purposes.
- Restrictions in the definition of the catalog SVC interface.

The introduction of ICF catalogs in the mid-1980s and other catalog enhancements (such as the multilevel alias support) directly addressed those problems. In addition, processes were developed for system build to use system specific aliases instead of JOBCAT or STEPCAT. CBIPO introduced these processes and they are used today by offerings such as ServerPac to create data set entries in the new master catalog of the system being built.

At the time ICF catalogs were introduced, the JOBCAT and STEPCAT facilities were functionally stabilized. Neither SMS-managed data sets nor UCBs above the 16 megabyte line may be used with JOBCAT or STEPCAT. ICF catalogs contain sufficient functional capabilities that all functions that previously could only be performed with JOBCAT or STEPCAT can now be done without them.

Furthermore, the use of JOBCAT and STEPCAT could actually cause significant problems. Data sets were generally not cataloged according to the normal predictable search order when JOBCAT or STEPCAT was used. This impacted the ability to do comprehensive installation storage management and could increase staff requirements. For example, interval migration and recall using DFSMShsm was effectively unusable when the data sets could not be found using the standard catalog search order. The use of JOBCAT and STEPCAT could also result in noticeable increases in the time required to perform catalog requests.

Element or feature:	DFSMSdfp.
When change was introduced:	The removal of the JOBCAT and STEPCAT facilities was announced before z/OS V1R5. The first step in their removal, disablement by default, was part of z/OS V1R5. The final step, actual removal, is part of z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use the JOBCAT or STEPCAT facilities.
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: Change the jobs that use JOBCAT and STEPCAT to use the normal catalog search order, as described in *z/OS DFSMS Access Method Services for Catalogs*.

Reference information:
- *z/OS DFSMS Using the New Functions*
- *z/OS DFSMS Access Method Services for Catalogs*
- *z/OS DFSMS Managing Catalogs*

Tune DFSMShsm for the SSM multiple tasks enhancement

Description: The secondary space management (SSM) function is enhanced to run with multiple tasks in a single DFSMShsm host, allowing the function to complete more quickly. As a result of this enhancement, the following performance improvements have been made, and you might want to retune DFSMShsm because of them:

- The default number of tasks for SSM has increased from one to three: two cleanup tasks and one tape movement task.
- The default number of recall tasks has increased from 5 to 15 to aid in the processing of deletions that SSM initiates.
- Small data set packing (SDSP) data sets are no longer allocated for the entire SSM window.
- Deletion requests for expired migrated data sets are given a low priority so that user recalls and user-initiated deletions are processed before SSM-generated deletions.

In addition, a new SETSYS parameter, MAXSSMTASKS, allows you to specify the number of SSM tasks that you want to run concurrently.

Element or feature:	DFSMShsm.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended if you use SSM.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	This function requires coexistence PTFs. See "Install coexistence and fallback PTFs" on page 4.
Restrictions:	None.
System impacts:	None.

Steps to take:
- Determine the maximum number of SSM tasks that should be processed concurrently. Before z/OS V1R6, the default was 1. Now the default is 3: two cleanup tasks and one tape movement task. You can set the maximum by using the SETSYS MAXSSMTASKS command. Note that each SSM tape movement

task requires two tape drives if you are using DUPLEXing for migration; this might affect the number of SSM tasks that you want to allow.

- Determine the maximum number of recall tasks that can be processed concurrently. Before z/OS V1R6, the default was 5. Now the default is 15 to accommodate SSM deletion requests. You can set the maximum by using the SETSYS MAXRECALLTASKS command. If a DFSMShsm host will not be performing SSM, you will probably want to reduce the maximum number of recall tasks.

- Because SDSPs are no longer allocated for the entire SSM window, you might want to reconsider your SDSP reorganization procedures.

- Reconsider any procedures you have in place to reduce or eliminate user-initiated recalls or deletes during SSM processing because SSM-initiated deletes are processed only after all user-initiated recalls and deletes have been processed.

- Determine the number of SDSP data sets that should be defined to your DFSMShsm system, now that the number of SSM tasks has increased from one to three (or more). It is important to plan the number of SDSP data sets in relation to the number of concurrent migration tasks and the amount of processing performed by functions with a higher usage priority for the SDSP data sets.

Reference information: For details about using DFSMShsm SSM multiple tasks, see:

- *z/OS DFSMShsm Storage Administration Guide*
- *z/OS DFSMShsm Storage Administration Reference*
- *z/OS DFSMShsm Implementation and Customization Guide*
- *z/OS DFSMShsm Diagnosis*
- *z/OS MVS System Messages, Vol 2 (ARC-ASA)*

Modify ARCMDEXT and ARCMMEXT exit routines to handle data set processing

Description: Before z/OS V1R5, neither the ARCMDEXT nor the ARCMMEXT installation exits were called during command data set migration. Beginning with z/OS V1R5, both are called for command data set migration, either by the HMIGRATE end-user command or the MIGRATE storage administrator command specified with the DATASETNAME parameter. The ARCMDEXT exit is called when migrating from Level0 DASD to migration level (ML) 1 disk, ML2 disk, or ML2 tape. The ARCMMEXT exit is called when migrating an already migrated data set to ML1 disk, ML2 disk, or ML2 tape.

You should modify your ARCMDEXT and ARCMMEXT exit routines to first determine why they are called (volume processing or data set processing) and then perform the volume processing (as before) or data set processing (which is new).

Element or feature:	DFSMShsm.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use the ARCMDEXT or ARCMMEXT installation exits.
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: If necessary, update any applications to use the following new and changed exit flags:

- *ARCMMEXT installation exit:* A new flag is defined at offset 08 (X'08'). This flag indicates that a data set is migrating from a data set command, not from volume migration. The following input flags continue to be set even if the migration is due to a data set migration request:
  - Level 1 to level 2 migration is to DASD or tape.
  - The target volume is always a level 2 volume.

  The following flag is not valid on a data set migration and is set to zero:
  - FREEVOL command was specified

- *ARCMDEXT installation exit:* A new flag is defined in the input data structure at offset 12 (X'0C'). This flag indicates that a data set is migrating from a data set command, not from volume migration. The following input flags continue to be set even if the migration is due to a data set migration request:
  - Data set is a candidate for reconnection
  - Interval migration is in progress
  - Primary space management is in progress
  - CONVERT parameter specified in the MIGRATE DSNAME command
  - Migration eligibility age is valid

  The following flags are not valid on a data set migration and are set to zero:
  - DAYS parameter for MIGRATE command
  - Data set is being processed for extent reduction

Reference information:

- *z/OS DFSMS Installation Exits*
- *z/OS DFSMShsm Managing Your Own Data*
- *z/OS DFSMShsm Storage Administration Guide*
- *z/OS DFSMShsm Storage Administration Reference*

Modify HQUERY REQUEST commands that don't have request numbers

Description: Previously, you could list all pending DFSMShsm requests for a particular user ID by specifying an HQUERY command with no parameters, or by specifying an HQUERY command with the REQUEST parameter but no request numbers. For example, the following command:

```
HQUERY
```

Would yield the same result as this command:

```
HQUERY REQUEST
```

Starting with z/OS V1R5, only the HQUERY command (without parameters) lists all pending requests. The HQUERY REQUEST command fails and message ARC0165I is

issued. This change is necessitated by the DFSMShsm RACF FACILITY class enhancement.

Element or feature:	DFSMShsm.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use the HQUERY REQUEST command with no parameters.
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: Remove the REQUEST parameter from any HQUERY commands that are used to obtain a list of all pending DFSMShsm requests for a particular user ID.

Reference information:
- For a complete description of the HQUERY command, see *z/OS DFSMShsm Managing Your Own Data*.
- For information about protecting DFSMShsm commands with RACF FACILITY class profiles, see *z/OS DFSMShsm Implementation and Customization Guide*.

Define RACF FACILITY class profiles for DFSMShsm

Description: In z/OS V1R5, the DFSMShsm RACF FACILITY class enhancement provides a way to protect all DFSMShsm command access through the use of RACF FACILITY class profiles. An active RACF FACILITY class establishes the security environment. An active RACF FACILITY class means that DFSMShsm uses RACF protection for all commands instead of using only simple AUTH command protection.

If the RACF FACILITY class is active, DFSMShsm uses RACF FACILITY class checking. If you have not defined the new profiles, every DFSMShsm command fails.

Element or feature:	DFSMShsm.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if the RACF FACILITY class is active.
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: If you have the RACF FACILITY class active, you must define the new profiles before starting DFSMShsm V1R7. If the new profiles are not defined, all storage administrator commands and user commands fail.

Inform users that they can no longer use the following DFSMShsm commands. They must use the equivalent commands with the "H" prefix.

Old Command	New Command
QUERY	HQUERY
CANCEL	HCANCEL
BDELETE	HBDELETE
ALTERDS	HALTERDS

Perform the following steps to define new profiles for access to DFSMShsm commands. These profiles provide DFSMShsm users and storage administrators the equivalent access to DFSMShsm commands that they had before installing z/OS V1R7:

1. To allow all users to access all user commands, define a generic profile of STGADMIN.ARC.ENDUSER.* with a default access of READ. For example: RDEFINE FACILITY STGADMIN.ARC.ENDUSER.* UACC(READ).

2. To prevent all users from issuing storage administrator commands, define a generic profile of STGADMIN.ARC.* with a default access of NONE. For example: RDEFINE FACILITY STGADMIN.ARC.* UACC(NONE).

3. To permit storage administrators to issue all DFSMShsm storage administrator commands, use the RACF PERMIT command. For example: PERMIT STGADMIN.ARC.* CLASS(FACILITY) USER(*userid*) ACCESS(READ).

Reference information:

- For information about protecting DFSMShsm commands with RACF FACILITY class profiles, see *z/OS DFSMShsm Implementation and Customization Guide*.
- For a discussion of the changes to the DFSMShsm commands, see *z/OS DFSMShsm Managing Your Own Data*.

Make sure your VOLCAT is large enough to support 255 media types

Description: When the system-managed tape library was originally designed, it supported up to eight media types and 15 recording technologies. Four of the eight media types (MEDIA1/CST, MEDIA2/ECCST, MEDIA3/HPCT, and MEDIA4/EHPCT) and five of the 15 recording technologies (18-TRACK, 36-TRACK, 128-TRACK, 256-TRACK, and 384-TRACK) are used today. As of z/OS V1R5, the tape library supports 255 media types and recording technologies to allow you to easily use additional media types and recording technologies as they become available.

As a result of this change, the LIBRARYENTRY in the volume catalog (VOLCAT) has increased in size. You should examine the size of your volume catalog to ensure that it is large enough to hold your catalog records.

Element or feature:	DFSMSdfp, DFSMShsm, and DFSMSrmm.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.

Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use more than four media types or more than five recording technologies.
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: Determine whether you have free space in the catalog and have secondary allocation defined for the volume catalog. In most cases, there should be room in your existing volume catalog to accommodate the expanded library record length, which has grown by 1976 bytes.

Note: The first time (and first time *only*) that a specific LIBRARYENTRY is updated (for *any reason*), the length of the record is changed to the new length.

Review any DFSMShsm PATCH commands that patch the YGCB control block. Two offsets have changed. If you are patching the following two YGCB areas, you need to update your PATCH commands:

- The reuse capacity table for migration tapes has moved from YGCB.+2C to YGCB.+1EC.
- The reuse capacity for backup tapes has moved from YGCB.+6C to YGCB.+22C.

Reference information:
- *z/OS DFSMS Managing Catalogs*

Convert the optical configuration database to z/OS V1R5 and later format

Description: In z/OS V1R5, an Object Access Method (OAM) object enhancement allows OAM to expire object tape volumes and to expire tape and optical volumes that belong to object backup storage groups. This enhancement significantly reduces the amount of private storage that the OAM address space uses at larger installations.

Even if you don't take advantage of this enhancement, you must run the CBRSMR15 samplib job to convert the optical configuration database to the new format.

Element or feature:	DFSMSdfp.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	None.

Other system (coexistence or fallback) requirements:	This function requires coexistence PTFs. See "Install coexistence and fallback PTFs" on page 4.
Restrictions:	None.
System impacts:	None.

Steps to take: Run the CBRSMR15 job in SYS1.SAMPLIB to add two new columns, OUNITNAM and DATACLAS, to the DB2 TAPEVOL table.

If you will retain expired tape volumes in their original storage group, or release expired volumes to MVS scratch, then it is appropriate to leave the OUNITNAM and DATACLAS names blank. However, in order for object tape volumes introduced into the OAM inventory before z/OS V1R5 to be eligible for reuse when they are returned to OAM scratch status, you must either manually update their OUNITNAM and DATACLAS fields in the TAPEVOL table or, if appropriate, enable SETOAM OAMSCRATCHSYNCH mode in the CBROAM*xx* PARMLIB member.

Reference information: See *z/OS DFSMS OAM Planning, Installation, and Storage Administration Guide for Object Support*. See "Chapter 3. Migrating, Installing, and Customizing OAM" for general migration information and a checklist, and "Synchronizing OAM Scratch Tape" in "Chapter 4. Administering OAM".

Recompile exit ADRUIXIT or your UIM because the ADRUFO parameter list increased

Description: The length of the ADRUFO parameter list has increased to support new functions. You might have to recompile installation exit ADRUIXIT or the user interaction module (UIM) with the updated ADRUFO macro.

Element or feature:	DFSMSdss
When change was introduced:	z/OS V1R5 and rolled back to z/OS V1R4, z/OS V1R3, and z/OS V1R2 by APAR OW57347 (PTF UA03442 on z/OS V1R4 and z/OS V1R3, and PTF UA03443 on z/OS V1R2).
Applies to migration from:	z/OS V1R4 without PTF UA03442 installed.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if your ADRUIXIT or UIM is sensitive to ADRUFO length change.
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: If you use installation exit ADRUIXIT or invoke DFSMSdss with an application program, perform the following steps:

1. If you use ADRUIXIT to change installation options with the ADRUFO parameter list, review the updated ADRUFO macro to determine if you need to recompile and link-edit installation exit ADRUIXIT using the z/OS V1R7 macro libraries.

UFOFUNCT and UFOPARM sizes have increased. New keyword indicators are added and the existing UFOT0IND is changed to UFO4FLGS.

2. If you invoke DFSMSdss using the API and change options with the ADRUFO parameter list on EIOPTION 13, review the updated ADRUFO macro to determine if you need to recompile and link-edit your user interaction module (UIM) using the z/OS V1R7 macro libraries. The increased UFOFUNCT and UFOPARM lengths and changes to some fields in the ADRUFO parameter list might affect the UIM.

Reference information:

- For details about DFSMSdss application programming interfaces and EIOPTION 13, see *z/OS DFSMSdss Storage Administration Reference*.
- For ADRUFO mapping, see *z/OS DFSMS Installation Exits*.

DFSMS actions to perform after the first IPL of z/OS V1R7

This section describes DFSMS migration actions that you can perform only after you've IPLed z/OS V1R7. You need a running z/OS V1R7 system to perform these actions.

Ensure the integrity of 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 strongly 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. If you do not translate your ACS routines and validate your SCDS on the latest level of DFSMS, the translation and validation might fail. This failure occurs because some constructs and definitions are known only to later levels of DFSMS. It can also occur because of changes in validation rules between releases. Once the control data sets are formatted by the later-level system, the SMS control blocks reflect the new rather than the back-level lengths and control information.

Element or feature:	DFSMSdfp.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	No, but strongly recommended when using SMS in a mixed-level sysplex.
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 4 if they are not already installed.

Restrictions:	None.
System impacts:	None.

Steps to take:

1. Install all coexistence PTFs in "Install coexistence and fallback PTFs" on page 4 if you haven't already done so.
2. Save the active ACDS as an SCDS with the SETSMS SAVESCDS command.
3. Update, translate, validate, and activate SMS policies using a z/OS V1R7 system. Remember, once you've translated using a z/OS V1R7 system, you risk failure if you update and translate using a back-level system.

Reference information:
- *z/OS DFSMS Implementing System-Managed Storage*
- *z/OS DFSMSdfp Storage Administration Reference*

Chapter 9. DFSORT migration actions

This chapter describes migration actions for optional feature DFSORT.

DFSORT actions to perform before installing z/OS V1R7

This section describes DFSORT migration actions that you can perform on your current (old) system. You don't need the z/OS V1R7 level of code to make these changes, and the changes don't require the z/OS V1R7 level of code to run once they are made.

Use means other than ISPF to invoke DFSORT

Description: The DFSORT ISPF panels are used to generate and execute DFSORT jobs, and are available in both English and Japanese. The panels are planned to be removed from z/OS at some time in the future. No replacement is planned for this limited function interactive facility.

All other previously supported methods for invoking DFSORT are planned to still be supported.

Element or feature:	DFSORT.
When change was introduced:	Future removal of the panels was announced on 10 August 2004 in the z/OS V1R6 availability and z/OS V1R7 preview announcement. (The specific future release has not been announced as of this writing.)
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	No, but recommended because it is planned to become a requirement in the future.
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: You will no longer be able to use the ISPF Panels to generate or execute DFSORT jobs, but instead will have to invoke DFSORT using batch jobs or from programs. While you still have access to the DFSORT ISPF panels, you can use the "SAVE GENERATED JOB IN A DATA SET" function to save all of the generated DFSORT jobs you need in data sets so that you can execute them as batch jobs.

DFSORT actions to perform before the first IPL of z/OS V1R7

This section describes DFSORT migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

Update automation that handles message ICE000I

Description: Message ICE000I is updated to reflect the current level of DFSORT. Formerly, the message contained the product number and release level of the DFSORT product:

```
ICE000I - CONTROL STATEMENTS FOR 5740-SM1, DFSORT REL 14.0 - hh:mm ON day
 mmm dd, yyyy -
```

Now that DFSORT is available only as an optional feature of z/OS (and not also as a separate product), the message contains the z/OS product number and release:

```
ICE000I - CONTROL STATEMENTS FOR 5694-A01, Z/OS DFSORT V1R5 - hh:mm ON day
 mmm dd, yyyy -
```

Element or feature:	DFSORT.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use automation to process message ICE000I.
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: Update any automation that processes message ICE000I.

Reference information: *z/OS DFSORT Messages, Codes and Diagnosis Guide*.

DFSORT actions to perform after the first IPL of z/OS V1R7

This section describes DFSORT migration actions that you can perform only after you've IPLed z/OS V1R7. You need a running z/OS V1R7 system to perform these actions.

Use the new IBM-supplied defaults for the ICEMAC macro

Description: The following IBM-supplied ICEMAC (installation) defaults are changed to provide more efficient DFSORT processing:
- COBEXIT is changed from COB1 to COB2.
- DSA is changed from 32MB to 64MB.

- TMAXLIM is changed from 4MB to 6MB.
- ZDPRINT is changed from NO to YES.

Using the new defaults is recommended. However, you can continue to use one or more of your prior values if appropriate.

Element or feature:	DFSORT.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended for more efficient DFSORT processing.
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 DFSORT to use the new IBM-supplied ICEMAC default values listed in "Description" above (which is recommended), do nothing. However, if you do not want DFSORT to use one or more of the new values, receive and apply a user modification (usermod) specifying the default value or values you want to use (for example, the old values). You can find sample jobs in SICESAMP as members ICEOPREC (for receive) and ICEOPAPP (for apply) to create the usermod.

Reference information: For details about the ICEMAC macro, see *z/OS DFSORT Installation and Customization*.

Chapter 10. Distributed File Service

This chapter describes migration actions for base element Distributed File Service.

Distributed File Service actions to perform before installing z/OS V1R7

This section describes Distributed File Service migration actions that you can perform on your current (old) system. You don't need the z/OS V1R7 level of code to make these changes, and the changes don't require the z/OS V1R7 level of code to run once they are made.

Discontinue use of multi-file system aggregates

Description: z/OS V1R7 is planned to be the last release to allow mounting of zFS file systems contained in multi-file system aggregates that are to be shared across systems in a sysplex. IBM has previously recommended that these multi-file system aggregates not be shared in a sysplex environment. Once this support has been removed, attempts to mount zFS file systems contained in multi-file system aggregates will fail in a z/OS UNIX shared file system environment. Mounting zFS compatibility mode aggregates, which have a single file system per data set, will continue to be supported in all environments.

In a future release, IBM plans to withdraw support for zFS multi-file system aggregates. When this support is withdrawn, only zFS compatibility mode aggregates will be supported. (A zFS compatibility mode aggregate has a single file system per data set.)

Element or feature:	Distributed File Service.
When change was introduced:	15 February 2005 in the z/OS V1R7 preview announcement.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	No, but recommended if you are using zFS multi-file system aggregates because the action is planned to become a requirement 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.

Steps to take: Determine if you are using zFS multi-file system aggregates. You can determine this by scanning your zFS IOEFSPRM configuration options file for

define_aggr statements. You should also scan your /etc/rc file for any zfsadm attach commands. If you are using zFS multi-file system aggregates, you should copy the data from each file system into its own compatibility mode file system.

Reference information: For information about the zFS IOEFSPRM configuration options file or about copying data from a file system into another file system, see *z/OS Distributed File Service zSeries File System Administration*.

Distributed File Service actions to perform before the first IPL of z/OS V1R7

This section describes Distributed File Service migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

Remove extraneous characters in the FILESYSTYPE PARM option for zFS

Description: Before z/OS V1R6, any value specified in the PARM option of the FILESYSTYPE statement for zFS (in BPXPRM*xx*) was ignored. Starting in z/OS V1R6, the zFS FILESYSTYPE PARM option is interpreted as the zFS parmlib search specification. Therefore, any non-parmlib specification in the zFS FILESYSTYPE PARM option causes the initialization of the zFS physical file system to fail. (If you are not using zFS PARMLIB support, that is, if you have an IOEZPRM DD statement in your ZFS PROC, this type of failure does not occur. However, you should still remove any non-parmlib support specification from your zFS FILESYSTYPE PARM option so that you can use zFS parmlib support in the future.)

Element or feature:	Distributed File Service.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use zFS parmlib support (that is, if you do not have an IOEZPRM DD statement in your ZFS PROC). Even if you are not using zFS parmlib support, this action is recommended to avoid future problems.
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: Ensure that you do not have any extraneous characters in your zFS FILESYSTYPE PARM specification. Your zFS FILESYSTYPE statement should either have no PARM option, such as:

```
FILESYSTYPE TYPE(ZFS) ENTRYPOINT(IOEFSCM) ASNAME(ZFS,'SUB=MSTR')
```

Or it should have the parmlib support type specification, such as:

```
FILESYSTYPE TYPE(ZFS) ENTRYPOINT(IOEFSCM) ASNAME(ZFS,'SUB=MSTR') PARM('PRM=(00)')
```

Note: An incorrect sample statement appears in *z/OS V1R6 Distributed File Service zSeries File System Administration*, SC24-5989-04. It is in Chapter 2, topic "zFS installation and configuration steps", step 2. The note in step 2 says that if you have overridden the default for the MSGFILE, you need to set it back to the default. The note then shows a sample zFS FILESYSTYPE statement. You should not use the sample PARM option shown in that statement. If you already coded it, remove it before IPLing z/OS V1R6. If you have this sample PARM in your zFS FILESYSTYPE statement, you will see messages such as:

```
IOEZ00516E PRM not found at position 1
IOEZ00507E Error in FILESYSTYPE PARM specification MSGFILE(SYSOUT,FBA,121,0,NOENQ)/
BPXF006I A FILE SYSTEM WITH FILESYSTYPE ZFS FAILED TO INITIALIZE. IT TERMINATED DURING INITIALIZATION.
```

Reference information: For information about parmlib support, see *z/OS Distributed File Service zSeries File System Administration*.

Distributed File Service actions to perform after the first IPL of z/OS V1R7

None.

Chapter 11. HCD migration actions

This chapter describes migration actions for base element Hardware Configuration Definition (HCD).

Some HCD data sets have been removed from z/OS. See "Remove references to deleted data sets and paths" on page 40. Some HCD data sets have been added to z/OS. See "Add references to new data sets and paths" on page 53.

HCD actions to perform before installing z/OS V1R7

None.

HCD actions to perform before the first IPL of z/OS V1R7

This section describes HCD migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

Use the new HCD profile keyword defaults

Description: The default values of the following keywords in the HCD profile have changed from NO to YES:

- IODF_DATA_SPACE
- SHOW_IO_CHANGES
- BATCH_IODF_NAME_CHECK

The new defaults provide more information and data integrity, and avoid restrictions on the size of the IODF.

Element or feature:	HCD.
When change was introduced:	z/OS V1R4 with the z/OS V1R4 z990 Compatibility Support feature (and the z990 Compatibility for Selected Releases Web deliverable on earlier releases).
Applies to migration from:	z/OS V1R4 without the z/OS V1R4 z990 Compatibility Support feature or z/OS V1R4 z990 Exploitation Support feature.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended because the new defaults provide more information and data integrity, and avoid restrictions on the size of the IODF.
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: Either specify, or default to, YES on the changed keywords in the HCD profile (HCDPROF). However, if you want the behavior to be the same as in releases before z/OS V1R6 (which is not recommended), specify NO on the changed keywords, as follows:

- `IODF_DATA_SPACE = NO`. This tells HCD that the IODF is to be loaded into the user address space. If you were to specify YES, or allow it to default, the IODF would be loaded into a data space, thereby removing restrictions on the size of the IODF imposed by address space limitations.

- `SHOW_IO_CHANGES = NO`. This tells HCD, when you're performing both a hardware and software change, not to display information about channel paths, control units, and devices that are deleted, modified, or added. If you were to specify YES, or allow it to default, the information would be displayed.

- `BATCH_IODF_NAME_CHECK = NO`. This tells HCD not to check the IODF names specified for batch jobs. If you were to specify YES, or allow it to default, HCD would check whether the IODF specified for a batch job conforms to the naming convention described in *z/OS HCD User's Guide*. Processing of IODFs with invalid names is limited to deletion.

Reference information: *z/OS HCD User's Guide*.

HCD actions to perform after the first IPL of z/OS V1R7

This section describes HCD migration actions that you can perform only after you've IPLed z/OS V1R7. You need a running z/OS V1R7 system to perform these actions.

Upgrade the IODF to V5

Description: A new IODF level, called V5, is introduced in z/OS V1R7. This new IODF level reduces the size of the IODF and improves the processing performance of large configurations.

Element or feature:	HCD.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you need to update the IODF but the IODF is not yet at the z/OS V1R7 level (that is, not yet at IODF V5).
Target system hardware requirements:	None.
Target system software requirements:	None.

Other system (coexistence or fallback) requirements:	To read from, IPL with, and dynamically activate an IODF at the V5 level, the PTFs for coexistence APARs OA07875 and OA08197 are required on back-level systems. If you attempt to IPL with a V5 IODF from a back-level z/OS system that does not have the PTF for APAR OA08197 installed, a wait state occurs. The coexistence PTF for APAR OA07875 allows you to view and dynamically activate the V5 IODF, but does not allow you to update the V5 IODF from back-level systems. Once the IODF has been upgraded to V5, the z/OS V1R7 HCD libraries must be used to process updates to it. (A STEPLIB or JOBLIB from a back-level system to the z/OS V1R7 HCD libraries, or to a copy of the libraries, is acceptable.)
	Note: APAR OA07875 is available for z/OS V1R4 systems that have the z/OS V1R4 z990 Compatibility Support feature installed (that is, HCD FMID HCS7708). z/OS V1R4 HCD **without** the z990 Compatibility Support feature (that is, HCD FMID HCS6091) does **not** have an applicable coexistence PTF. (**Tip:** HCD FMID HCS7708 shows up as "z/OS V1.4 HCD" on its primary panel and is described as "z/OS V1.4 HCD" in the documentation. HCD FMID HCS6091 shows up as "OS/390 Release 9 HCD" on its primary panel.)
	If you are running z/OS V1R4 **without** the z990 Compatibility Support feature, an additional coexistence and fallback requirement applies: you cannot read or dynamically activate a V5 IODF from the z/OS V1R4 system. If you want to read or dynamically activate a V5 IODF from the z/OS V1R4 system, install the z/OS V1R4 z990 Compatibility Support feature (or its replacement, the z/OS V1R4 z990 Exploitation Support feature,) and install the PTF for APAR OA07875.
	Other methods to satisfy this coexistence requirement are: • Do not share the IODF. Use EXPORT/IMPORT or COPY to create a second IODF. • Delay making IODF updates from the z/OS V1R7 system until all systems are at the level of the z/OS V1R4 z990 Compatibility Support feature (FMID HCS7708) or later.
Restrictions:	Once z/OS V1R7 is running, updates are only allowed to an IODF that has been upgraded to the V5 level.
System impacts:	None.

| **Steps to take:** Upgrade your IODF to the V5 level in order to allow updates to
| device configurations, following the instructions in *z/OS HCD User's Guide*.

| If you wish to make updates to your V5 IODF from back-level systems, ensure that
| you invoke the z/OS V1R7 HCD libraries to make the updates. A STEPLIB or
| JOBLIB from the back-level system to the z/OS V1R7 HCD libraries, or to a copy of
| the libraries, is acceptable

| **Reference information:** *z/OS HCD User's Guide*.

Chapter 12. HLASM migration actions

This chapter describes migration actions for base element High Level Assembler
(HLASM).

HLASM actions to perform before installing z/OS V1R7

None.

HLASM actions to perform before the first IPL of z/OS V1R7

This section describes HLASM migration actions that you can perform after you've
installed z/OS V1R7 but before the first time you IPL. These actions might require
the z/OS V1R7 level of code to be installed but don't require it to be active.

Migrate from use of SYSUT1

Description: Previously, the assembler used the SYSUT1 work file as an
intermediate storage area if there was insufficient virtual storage allocated to
assemble the program in storage. HLASM no longer uses a work file. As a result,
you might need to increase the amount of virtual storage allocated to assemblies. In
addition, you may remove SYSUT1 DD statements from JCL, procedures, and
execs, but if they remain, HLASM ignores them.

Element or feature:	HLASM.
When change was introduced:	V1R5 of the HLASM for MVS & VM & VSE product (5696-234), which is the same level as the HLASM base element in z/OS V1R6 and later.
Applies to migration from:	z/OS V1R5 without the V1R5 level of the HLASM product, and z/OS V1R4 without the V1R5 level of the HLASM product.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if your assembly source program is large enough that it required utility-file activity on previous releases. (This information is printed on the final summary page of the HLASM listing.)
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:

- Increase the amount of virtual storage allocated to assemblies, if necessary. The last page of each assembly created by previous HLASM releases (the "Assembly Summary" page) gives an estimate of the amount of storage needed to assemble a program without a work file (SYSUT1) and do the assembly entirely in virtual storage. If your REGION specification is less than this amount, increase it to a greater value. If the program has not been assembled on previous releases of HLASM, estimate an appropriate REGION size.

- Remove SYSUT1 DD statements from JCL, procedures, and execs, if desired. Any that remain are ignored, but removing them can avoid confusion. Retaining them allows JCL, procedures, and execs to work with older releases of HLASM, if required.

Reference information: For information about specifying the REGION parameter, see *z/OS MVS JCL Reference*.

Accommodate changes to the High Level Assembler's associated data file format

Description: Associated data (ADATA) is assembler language program data. This support includes a general-use programming interface that lets you write programs to use the associated data records produced by the High Level Assembler (HLASM). The associated data file contains language-dependent and language-independent records. Language-dependent records contain information that is relevant only to programs assembled by HLASM. Language-independent records contain information that is common to all programming languages that produce ADATA records, and includes information about the environment in which the program is assembled. You use the ADATA assembler option to produce this file.

The format of the ADATA in HLASM V1R5 (which is in z/OS V1R6 and later) has changed. Consequently, any programs that read this file, such as source level debugger programs, might need to be changed to accommodate the new format. HLASM V1R5 provides an optional ADATA reformatting exit, ASMAXADR, which converts the new format to the previous format. Its use is described in "Appendix I" of *HLASM Programmer's Guide*.

Element or feature:	HLASM.
When change was introduced:	V1R5 of the HLASM for MVS & VM & VSE product (5696-234), which is the same level as the HLASM base element in z/OS V1R6 and later.
Applies to migration from:	z/OS V1R5 without the V1R5 level of the HLASM product, and z/OS V1R4 without the V1R5 level of the HLASM product.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have any programs that are dependent on the associated data file format, and for which the ASMAXADR reformatting exit cannot be used.
Target system hardware requirements:	None.
Target system software requirements:	This change might have ISV debug product impacts.

Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Steps to take: If you use an ISV debug product, contact the vendor to ensure that the new ADATA format is compatible with that debug product.

If you need to revert back to the previous format for ADATA, investigate using user exit ASMAXADR. All sample user exits are shipped as members of data set ASM.SASMSAM1.

Reference information:
- For information about ADATA format changes, see "Appendix D" in *HLASM Programmer's Guide*.
- For information about user exits for ADATA, see "Appendix I" in *HLASM Programmer's Guide*.
- For a directory of ISV products that support z/OS, see the Global Solutions Directory at http://www.ibm.com/software/solutions/isv.

HLASM actions to perform after the first IPL of z/OS V1R7

None.

Chapter 13. ICKDSF migration actions

This chapter describes migration actions for base element ICKDSF.

ICKDSF actions to perform before installing z/OS V1R7

None.

ICKDSF actions to perform before the first IPL of z/OS V1R7

This section describes ICKDSF migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

Install ICKDSF R17 on systems that share DASD with a z9-109, z990, or z890 system

Description: All z/OS, z/VM, z/VSE, and VSE/ESA system images (regardless of server) that share DASD with any z/OS, z/VM, z/VSE, or VSE/ESA system images running on a z9-109, z990, or z890 server, need to have ICKDSF R17 installed. R17 is the same level of ICKDSF that is in z/OS as of the z/OS V1R4 z990 Compatibility Support feature. (In other words, R17 is the level in z/OS V1R7, z/OS V1R6, z/OS V1R5, z/OS V1R4 with the z/OS V1R4 z990 Exploitation Support feature, and z/OS V1R4 with the z/OS V1R4 Compatibility Support feature.)

Element or feature:	ICKDSF.
When change was introduced:	z/OS V1R4 with the z/OS V1R4 z990 Compatibility Support feature (and the z990 Compatibility for Selected Releases Web deliverable on earlier releases), which contains ICKDSF R17.
Applies to migration from:	z/OS V1R4 without the z/OS V1R4 z990 Compatibility Support feature or without the z/OS V1R4 z990 Exploitation Support feature, that is, z/OS V1R4 without ICKDSF R17.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if any z/OS, z/VM, z/VSE, or VSE/ESA system images share DASD with any z/OS, z/VM, z/VSE, or VSE/ESA system images running on a z9-109, z990, or z890 server, and ICKDSF R17 is not installed on all the images.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	See the "Description" above.

Restrictions:	None.
System impacts:	None.

Steps to take: Install ICKDSF R17 on all z/OS, z/VM, z/VSE, and VSE/ESA system images that require it, as explained in the "Description" above. IBM recommends that ICKDSF R17 be installed on all systems that share DASD before any z9-109, z990, or z890 server is brought into use in the sysplex.

Reference information: For information about installing the ICKDSF R17 product, see the program directory that accompanies it.

ICKDSF actions to perform after the first IPL of z/OS V1R7

None.

Chapter 14. Infoprint Server migration actions

This chapter describes migration actions for optional feature Infoprint Server.

Some Infoprint Server data sets have been added to z/OS. See "Add references to new data sets and paths" on page 53.

Infoprint Server actions to perform before installing z/OS V1R7

This section describes Infoprint Server migration actions that you can perform on your current (old) system. You don't need the z/OS V1R7 level of code to make these changes, and the changes don't require the z/OS V1R7 level of code to run once they are made.

Migrate the NetSpool and IP PrintWay features of PSF

Description: If you are migrating from the NetSpool™ or IP PrintWay™ features of Print Services Facility™ (PSF) V3R2, 5655-B17, you must migrate your IP PrintWay and NetSpool system data sets to the Infoprint Server Printer Inventory. Infoprint Server provides a migration program, **aopmig**, which can be used to migrate these data sets.

Element or feature:	Infoprint Server.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you use the NetSpool or IP PrintWay features of PSF V3R2.
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:

1. Run the **aopmig** migration program.

2. Use the output from the **aopmig** migration program as input to the Printer Inventory Definition Utility (PIDU) to load the Printer Inventory.

Reference information: For information about how to run the migration program and PIDU, see *Infoprint Server V1R2 – V1R4 Migration*.

Infoprint Server actions to perform before the first IPL of z/OS V1R7

This section describes Infoprint Server migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

Export the Printer Inventory and copy other files that were customized

Description: When migrating to z/OS V1R7 Infoprint Server, you must bring forward the Printer Inventory and customized data from your previous system.

Element or feature:	Infoprint Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

Steps to take:

- *Printer Inventory:* Use the Infoprint Server **pidu** command to export the Printer Inventory on the z/OS V1R6, V1R5, or V1R4 system. Then use the **pidu** command to restore the Printer Inventory on the z/OS V1R7 system. The restore step must be done after IPL of the z/OS V1R7 system and after you run the **aopsetup** shell script and start Infoprint Server on the z/OS V1R7 system. The format of the Printer Inventory has not changed; therefore, you can continue to use the same Printer Inventory that you used in z/OS V1R6, V1R5, or V1R4. 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.
- *Configuration file:* If you modified the Infoprint Server configuration file, copy the file to the z/OS V1R7 system. Its default location is `/etc/Printsrv/aopd.conf`. However, you might have specified a different location in environment variable AOPCONF.
- *aopstart EXEC:* If you're migrating from z/OS V1R4 and you modified the **aopstart** EXEC, make the same modifications to the z/OS V1R7 **aopstart** EXEC. The **aopstart** EXEC was modified in z/OS V1R5 to use additional environment variables.
- *IP PrintWay:* If you currently use the IP PrintWay component of Infoprint Server, copy to the z/OS V1R7 system any IP PrintWay exit routines you have written. You do not need to recompile the exit routines unless you want to use new functions in IP PrintWay extended mode.
- *NetSpool:* If you currently use the NetSpool component of Infoprint Server, copy to the z/OS V1R7 system any NetSpool exit routines you have written. You do not need to recompile the exit routines unless you want to use new functions.

- *Print Interface:* If you currently use the Print Interface component of Infoprint Server, take the following actions:
  - If you have written any data stream filters, copy them to the z/OS V1R7 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 V1R7 system. Its default location is `/etc/Printsrv/aopsapd.conf`. However, you might have specified a different location in environment variable AOPSAPD_CONF.
- *Infoprint Server Transforms:* If you currently use the Infoprint Server Transforms (5697-F51) product, take the following actions:
  - If you modified the default transform configuration file, copy the file to the z/OS V1R7 system. Its default location is `/etc/Printsrv/aopxfd.conf`. However, you might have specified a different location in environment variable AOPXFD_CONF.
  - If you modified the configuration files for the SAP to AFP™ transform, copy the directory that contains the files to the z/OS V1R7 system. The default directory is `/usr/lpp/Printsrv/sap2afp`. However, if you modified these files, the modified files are in the directory named in environment variable AOP_SAP2AFP_RESOURCES.
  - If you modified the `UserInit` or `preload.ps` configuration file for the PostScript to AFP transform, or added fonts for the transform, copy the directory that contains the modified files and fonts to the z/OS V1R7 system. This directory is named in environment variable AOP_RESOURCE_PATH, which is specified in the **ps2afp** transform entry in the transform configuration file, `aopxfd.conf`.
  - If you modified the multibyte conversion tables for the SAP to AFP transform, copy to the z/OS V1R7 system the directory that contains the files, `/usr/lib/nls/locale/uconvTable`.
  - If you modified the font-mapping table, AOXFONTS, used by the AFP to PCL, AFP to PDF, and AFP to PostScript transforms, apply user modifications to install the modified font-mapping table in each AFP transform. Sample usermods (AOX2PCLJ, AOX2PDFJ, and AOX2PSJ) to update AOXFONTS are provided in SYS1.SAMPLIB.
  - If you scaled 240-pel fonts to 300-pel fonts for use with the AFP to PCL, AFP to PDF, and AFP to PostScript transforms, copy the data set that contains the 300-pel fonts to the z/OS V1R7 system.

Reference information: *z/OS Infoprint Server Customization*.

Upgrade XML libraries for Infoprint Central

Description: The Infoprint Central component of Infoprint Server, which you can use to work with IP PrintWay extended mode print jobs and printers, now requires the IBM XML Toolkit V1.6 libraries.

Element or feature:	Infoprint Server.
When change was introduced:	z/OS V1R5 in PTF UA14959.
Applies to migration from:	z/OS V1R5 without PTF UA14959 installed and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.

Is the migration action required?	Yes, if you use Infoprint Central. You are using Infoprint Central if the start-daemons={ssid} attribute is specified in the Infoprint Server configuration file. The 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 XML Toolkit for z/OS and OS/390, C++ edition, *V1.6 level only*. The XML Toolkit V1.7 package contains the V1.6 libraries. • Infoprint Server PTF UA14959.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Steps to take:

- Install the IBM XML Toolkit V1.6 libraries.
- Make sure that Infoprint Server PTF UA14959 is installed.
- Change the following values in your z/OS IBM HTTP Server environment variables file (default location is `/etc/httpd.envvars`):
  - LIBPATH: change `/usr/lpp/ixm/IBM/xml4c-4_0/lib` to `/usr/lpp/ixm/IBM/xml4c-5_2/lib`.
  - LIBPATH: change `/usr/lpp/ixm/IBM/LotusXSL-C_1_3/lib` to `/usr/lpp/ixm/IBM/xslt4c-1_5/lib`.
  - ICU_DATA: change `/usr/lpp/ixm/IBM/xml4c-4_0/lib` to `/usr/lpp/ixm/IBM/xml4c-5_2/lib`.
- Restart the z/OS IBM HTTP Server to pick up the changes to the environment variables file.

Reference information: *z/OS Infoprint Server Customization*.

Upgrade Java support for the IPP server

Description: The Print Interface component of Infoprint Server provides an Internet Printing Protocol (IPP) server, which accepts print requests from any client that uses the IPP protocol. The IPP server no longer supports Java at SDK level 1.3. It now requires Java at SDK level 1.4.

Element or feature:	Infoprint Server.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.

Is the migration action required?	Yes, if you use the IPP server function in Infoprint Server. You're using this function if the start-daemons={ippd} attribute is specified in the Infoprint Server configuration file. The 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:	SDK for z/OS, Java 2 Technology Edition, V1R4 (5655-I56).
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Steps to take:

- Upgrade to Java at SDK level 1.4.
- APF-authorize the Java 1.4 libraries. You can run sample job AOPJAUTH to do this.
- If you did not install Java 1.4 in the default directories, specify the Java directory in the JAVA_HOME environment variable in the **aopstart** EXEC.

Reference information: *z/OS Infoprint Server Customization*.

Infoprint Server actions to perform after the first IPL of z/OS V1R7

This section describes Infoprint Server migration actions that you can perform only after you've IPLed z/OS V1R7. You need a running z/OS V1R7 system to perform these actions.

Run aopsetup

Description: When migrating to z/OS V1R7 Infoprint Server, you must run the **aopsetup** shell script to establish the correct file permissions for Infoprint Server directories and files.

Element or feature:	Infoprint Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
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.

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 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 the following 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 details about running **aopsetup**, see *z/OS Infoprint Server Customization*.

Replace the AOPADMIN profile with the AOP.ADMINISTRATOR profile

Description: Infoprint Server now lets you authorize users to read the Printer Inventory but not update it. To do this, you must define profile AOP.ADMINISTRATOR in the RACF PRINTSRV class. You can give users either READ or UPDATE access to this profile:

- READ access lets users read the Printer Inventory.
- UPDATE access lets users read and update the Printer Inventory.

The AOP.ADMINISTRATOR profile replaces the AOPADMIN profile in the FACILITY class. Infoprint Server continues to check the AOPADMIN profile until you define the AOP.ADMINISTRATOR profile.

Element or feature:	Infoprint Server.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended because it will become a requirement 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.

Steps to take:

1. Activate the PRINTSRV class in RACF, and define the AOP.ADMINISTRATOR profile in the PRINTSRV class.
2. Give all users and groups that currently have READ (or higher) access to the AOPADMIN profile UPDATE access to the AOP.ADMINISTRATOR profile. READ access to the AOPADMIN profile is equivalent to UPDATE access to the AOP.ADMINISTRATOR profile.
3. After all systems that share the RACF database have been migrated to z/OS V1R5 or later, delete the AOPADMIN profile from the FACILITY class.

Reference information: To find out how to activate the PRINTSRV class and define the AOP.ADMINISTRATOR profile, see *z/OS Infoprint Server Customization*.

Migrate from IP PrintWay basic mode to extended mode

Description: The IP PrintWay component of Infoprint Server can operate in a new mode called *IP PrintWay extended mode*. IP PrintWay extended mode uses the Sysout Application Programming Interface (SAPI) to obtain output data sets from the JES spool. IP PrintWay extended mode provides better performance, improved usability, and additional functions. For information about the enhancements and limitations in extended mode, see *z/OS Infoprint Server Customization*.

IP PrintWay basic mode is the name used for the original IP PrintWay mode of operation. You can continue to run IP PrintWay basic mode in z/OS V1R7. In future releases, IBM will make enhancements only to IP PrintWay extended mode.

You can run IP PrintWay basic mode and IP PrintWay extended mode at the same time only if you make sure that IP PrintWay basic mode and IP PrintWay extended mode select different print jobs from the JES spool to print. Otherwise, unpredictable results can occur.

Element or feature:	Infoprint Server.
When change was introduced:	Basic mode was stabilized in z/OS V1R5. Extended mode was introduced in z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended because it will become a requirement in a future release.
Target system hardware requirements:	None.

Target system software requirements:	• If you use the Transforms to AFP feature of Infoprint Server Transforms (5697-F51), PTF UA04288.
	• If you use Infoprint Central to work with IP PrintWay extended mode print jobs and printers:
	– z/OS HTTP Server.
	– IBM XML Toolkit for z/OS and OS/390, C++ edition, *V1.6 level only*. The XML Toolkit V1.7 package contains the V1.6 libraries. Ensure that PTF UA14959 is installed.
	– Microsoft Internet Explorer 5.5, Netscape Navigator 7.0, or IBM Home Page Reader 4.0.
	• To use IP PrintWay extended mode to print to VTAM-controlled printers, Infoprint Server PTF UA16412 and Infoprint Server Transforms PTF UA15500.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Steps to take:

1. Customize IP PrintWay extended mode as described in *z/OS Infoprint Server Customization*:

   - In the Infoprint Server configuration file, **aopd.conf**, specify the:
     - **outd** value in the **start-daemons** attribute to start IP PrintWay daemons.
     - **log-retention** attribute to specify how many days worth of messages to keep in the common message log.
     - **ebcdic-codepage** attribute to specify the default document code page. Specify the same code page that is currently specified in the Document code page field in the IP PrintWay basic mode FSS definition in the Printer Inventory.
   - Increase the space available to the /var/Printsrv directory if necessary.
   - Add an additional 50 to the current value of MAXPROCSYS in the BPXPRM*xx* parmlib member, which specifies the number of active z/OS UNIX processes that the system allows. Also, specify at least 70 for the MAXPROCUSER value, which specifies the number of processes that a single z/OS UNIX user ID can have concurrently active.
   - Create IP PrintWay job selection rules in the Printer Inventory. In the job selection rules, specify the same work-selection criteria that you currently specify for IP PrintWay basic mode functional subsystem applications (FSAs).
   - Give IP PrintWay extended mode RACF authorization to select output data sets from the JES spool.
   - Give IP PrintWay extended mode RACF authorization to write SMF type 6 records.
   - Edit the **aopstart** EXEC to set the _BPXK_SETIBMOPT_TRANSPORT, AOP_APPLID, STEPLIB, and AOPMAILER environment variables if

necessary. If you specify a step library in the STEPLIB variable, add the library to the STEPLIBLIST facility in the BPXPRM*xx* member of SYS1.PARMLIB. If you customized the **aopstart** EXEC in a previous release, you must copy your changes to the new **aopstart** EXEC.

- Recompile the IP PrintWay SMF exit. Also, review other IP PrintWay exits to see if changes are required.

2. Customize Infoprint Central and the z/OS HTTP Server as described in *z/OS Infoprint Server Customization*.

3. Restart the z/OS HTTP Server to pick up changes. For information about how to restart the HTTP Server, see *z/OS HTTP Server Planning, Installing, and Using*.

4. Change IP PrintWay printer definitions in the Printer Inventory if necessary. Because IP PrintWay extended mode and IP PrintWay basic mode share the same printer definitions, in most cases, no changes are required. However, you might need to change printer definitions that specify any of these fields: **Postscript header** (`Landscape`, `Always landscape`, or `Add` option), **Double-byte translate table**, **Response timeout**, **SOSI mode**, or **Translation dataset qualifier**.

   For information about how to change printer definitions for IP PrintWay extended mode, see *z/OS Infoprint Server Operation and Administration*.

5. If you currently specify a default font in the JES definitions for IP PrintWay basic mode FSAs and also use the AFP to PDF, AFP to PostScript, or AFP to PCL transform, specify the same default font in the printer definitions for the IP PrintWay printers. Or, if you want the default font to apply to all IP PrintWay printers, specify the font in the AOP_CHARS variable in the transform configuration file, `aopxfd.conf`. IP PrintWay extended mode does not use a default font supplied by JES like IP PrintWay basic mode does.

6. If you currently specify a default FCB in the JES definitions for IP PrintWay basic mode FSAs, ask job submitters to specify the same FCB in the FCB JCL parameter or **forms-control-buffer** job attribute to use this FCB. IP PrintWay extended mode does not use a default FCB supplied by JES like IP PrintWay basic mode does.

7. Review the SMF type 6 record for IP PrintWay extended mode to see if changes affect your accounting programs. See the description of the SMF type 6 record in *z/OS MVS System Management Facilities (SMF)*. For information about the differences between the records that IP PrintWay basic mode and extended mode write, see *z/OS Infoprint Server Operation and Administration*.

8. Change the manual and automatic procedures you use to search for IP PrintWay messages. IP PrintWay extended mode writes its messages only to the new Infoprint Server common message log. IP PrintWay extended mode messages have different IDs and message texts than IP PrintWay basic mode. The print administrator can use the new **aoplogu** command to retrieve messages from the common message log. Operators can use Infoprint Central to view all messages in the common message log for specific printers and print jobs. For information about the **aoplogu** command, see *z/OS Infoprint Server Operation and Administration*. For all Infoprint Server messages, see *z/OS Infoprint Server Messages and Diagnosis*.

9. Stop any IP PrintWay basic mode FSAs that select the same print jobs from the JES spool as IP PrintWay extended mode.

   Tip: The work-selection criteria for IP PrintWay basic mode FSAs determine which print jobs IP PrintWay basic mode selects. The job selection rules in the Printer Inventory determine which print jobs IP PrintWay extended mode selects.

10. Stop and restart all Infoprint Server daemons.

After you start IP PrintWay extended mode, submit print jobs that meet the criteria in the job selection rules. You can use Infoprint Central to work with print jobs, IP PrintWay printers, and IP PrintWay job selection rules, and to display the status of Infoprint Server daemons. For information about how to use Infoprint Central, see *z/OS Infoprint Server Operation and Administration*. For detailed usage information, see the Infoprint Central online help system.

To diagnose problems, use Infoprint Central to look at messages for selected print jobs and printers, or use the **aoplogu** command to view all messages in the common message log.

When you no longer want to run IP PrintWay basic mode, you can delete:
- All FSS and FSA definitions for IP PrintWay basic mode from the Printer Inventory.
- All JES initialization statements for IP PrintWay basic mode FSSs and FSAs.
- The IP PrintWay basic mode startup procedures.
- The IP PrintWay message data set (default name is ANF.MSGFILE) unless NetSpool writes messages to this data set.
- The IP PrintWay transmission queue data set (default name is ANF.QUEUE).
- The optional IP PrintWay Message (ANFUXMSG) and IP PrintWay Response Notification (ANFUXRSP) exits.

Reference information:
- *z/OS Infoprint Server Customization* describes the features and limitations of IP PrintWay extended mode and how to customize IP PrintWay extended mode. It also describes how to customize the common message log and Infoprint Central.
- *z/OS Infoprint Server Operation and Administration* describes how to log in to Infoprint Central and how to view messages in the common message log. It also describes how to modify printer definitions for IP PrintWay extended mode.
- *z/OS Infoprint Server User's Guide* describes considerations for submitting print jobs when you use IP PrintWay extended mode.
- *z/OS Infoprint Server Messages and Diagnosis* describes how to trace IP PrintWay extended mode.
- The Infoprint Central online help system describes how to use Infoprint Central.

Start the NetSpool daemon

Description: If you use the NetSpool component of Infoprint Server, you must edit the Infoprint Server configuration file to start the new NetSpool daemon, **aopnetd.**

Element or feature:	Infoprint Server.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use the NetSpool component of Infoprint Server.
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:

1. Add the **netd** value to the **start-daemons** attribute in the Infoprint Server configuration file, **aopd.conf**. For example:

   ```
   start-daemons = {lpd netd}
   ```

2. After you IPL the z/OS V1R7 system, start Infoprint Server using the AOPSTART JCL procedure or the z/OS UNIX `aopstart` command.

Reference information:

- For information about how to edit the Infoprint Server configuration file, see *z/OS Infoprint Server Customization*.
- For information about how to start Infoprint Server, see *z/OS Infoprint Server Operation and Administration*.

Chapter 15. Integrated Security Services migration actions

This chapter describes migration actions for base element Integrated Security Services. Integrated Security Services is made up of the following components: DCE Security Server, Enterprise Identity Mapping (EIM), Firewall Technologies, LDAP Server, Network Authentication Service, and Open Cryptographic Enhanced Plug-ins (OCEP).

Integrated Security Services is a new base element in z/OS V1R5, and EIM is a new component. The other components used to be in the Security Server optional feature. (RACF remains in Security Server.)

Some Integrated Security Services data sets have been removed from z/OS. See "Remove references to deleted data sets and paths" on page 40.

Integrated Security Services actions to perform before installing z/OS V1R7

This section describes Integrated Security Services migration actions that you can perform on your current (old) system. You don't need the z/OS V1R7 level of code to make these changes, and the changes don't require the z/OS V1R7 level of code to run once they are made.

Migrate from Firewall Technologies

Description: z/OS V1R7 is planned to be the last release to include the Firewall Technologies component of the Integrated Security Services base element. Many Firewall Technologies functions have been stabilized for some time and can be replaced using comparable or better functions provided by or planned for Communications Server, notably, IPSecurity. In addition, a functionally rich downloadable tool is planned to replace the IPSecurity and IP Filtering configuration GUI support.

Element or feature:	Integrated Security Services.
When change was introduced:	15 February 2005 in the z/OS V1R7 preview announcement.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	No, but recommended if you use any Firewall Technologies functions because the action is planned to become a requirement in the release following z/OS V1R7.

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: For the following functions, use the replacements indicated:

- *FTP proxy services:* No replacement.
- *Socks V4 services:* No replacement.
- *Network Address Translation (NAT):* No replacement.
- *RealAudio support:* No replacement.
- *HFS command line firewall configuration:* Use the tool z/OS Network Security Configuration Assistant, which can be downloaded from http://www.ibm.com/software/network/commserver/zos/.
- *Configuration server:* Use the tool z/OS Network Security Configuration Assistant, which can be downloaded from http://www.ibm.com/software/network/commserver/zos/.
- *Configuration GUI:* Use the tool z/OS Network Security Configuration Assistant, which can be downloaded from http://www.ibm.com/software/network/commserver/zos/.
- *IP packet filtering:* Use IP Security provided by Communications Server.
- *Manual VPN support:* Use IP Security provided by Communications Server.
- *Dynamic VPN support:* Use IP Security provided by Communications Server.

Reference information: For information about implementing the Communications Server functions referred to in "Steps to take", see:

- *z/OS Communications Server: New Function Summary*
- *z/OS Communications Server: IP Configuration Guide*
- *z/OS Communications Server: IP Configuration Reference*
- *z/OS Communications Server: IP System Administrator's Commands*
- *z/OS Communications Server: IP Diagnosis Guide*

Integrated Security Services actions to perform before the first IPL of z/OS V1R7

This section describes Integrated Security Services migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

LDAP Server: Make changes for LDAP enhancements

Description: New functions in z/OS V1R6 LDAP Server caused several behaviors to change. The behaviors are described in "Steps to take" below.

Element or feature:	Integrated Security Services.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.

Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if the behaviors described below in "Steps to take" are not desired.
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:

- Change logging has been extended to record changes to entries in the TDBM and GDBM backends, in addition to the RACF changes that were recorded in previous releases. If you are already creating change log records for RACF changes, changes to TDBM and GDBM entries will now automatically also cause change log records to be created.

  Action: If you do not want to create change log records for TDBM and GDBM changes, add the **changeLoggingParticipant no** option to the TDBM and GDBM backend sections of the LDAP server configuration file.

- If an asterisk (*) is specified as an attribute to be returned in a search directed to the SDBM backend, SDBM now returns all nonoperational attributes. In previous releases, the asterisk was treated as an attribute type, which never matched any returned attribute and thus resulted in no attributes being returned.

  Action: If your LDAP client application generates a search operation containing an asterisk, ensure that it can handle the extra output it now receives, or remove the asterisk from the search operation.

- The LDAP server now supports alias entries and dereferencing during a search operation. When an alias entry is encountered during a dereferenced search, search processing uses the entry pointed to by the alias instead of the alias entry itself. In previous releases, dereferencing was not supported and an alias entry was processed just like any other normal entry.

  Action: If you do not want to use dereferencing during search, ensure that your LDAP client application does not include dereferencing on search requests. Note that some LDAP clients (including the JNDI client) include dereferencing by default. The z/OS LDAP client defaults to no dereferencing. Also, if you already have alias entries in your directory, ensure that they conform to the alias entry rules enforced by z/OS LDAP Server.

- When modifying the TDBM schema with a modification that contains replace values, the LDAP server now uses the new replace-by-value behavior, which replaces individual values in the schema. The behavior in previous releases was to replace all values with the replace values.

  Action: If you want to continue to use the old behavior, either add the **SchemaReplaceByValue no** option to the TDBM backend section of the LDAP server configuration file, or modify your LDAP client application to include the **schemaReplaceByValueControl** with a value of FALSE in the schema modify request.

Reference information: *z/OS Integrated Security Services LDAP Server Administration and Use.*

LDAP Server: Update automation for return code and reason code changes in z/OS V1R6

Description: The return and reason code messages for several bind operations to the LDAP server have been updated for several error conditions. These changes were made to be consistent with the description of the bind response in LDAP RFC 2251 and also to deter hacking into the LDAP Server using information returned on a failed bind attempt.

Element or feature:	Integrated Security Services.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if automation of LDAP Server events is used and is based on return codes or reason codes.
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: The scenarios in which return codes and reason codes have been changed are listed below. Review and modify the use of these codes in the automation of LDAP Server events:

- *Scenario:* the authentication ID specified on a CRAM-MD5 or DIGEST-MD5 bind does not exist.

  z/OS V1R5 and V1R4: return code 48 (X'30'), reason code R007017 (entry not found in the database).

  z/OS V1R6 and later: return code 49 (X'31'), reason code R004062 (credentials are not valid) or reason code R007038 (credentials are not valid).

- *Scenario:* the authorization distinguished name specified on a CRAM-MD5 bind does not exist.

  z/OS V1R5 and V1R4: return code 48 (X'30').

  z/OS V1R6 and later: return code 49 (X'31').

- *Scenario:* the password specified on a CRAM-MD5 or DIGEST-MD5 bind is not correct.

  z/OS V1R5 and V1R4: return code 48 (X'30').

  z/OS V1R6 and later: return code 49 (X'31').

- *Scenario:* a CRAM-MD5 or DIGEST-MD5 bind is attempted with an entry that does not have a password.

  z/OS V1R5 and V1R4: reason code R004060 (entry does not contain a password).

  z/OS V1R6 and later: reason code R007038 (credentials are not valid).

- *Scenario:* a simple bind is attempted with an entry that does not have a password.

  z/OS V1R5 and V1R4: reason code R004060 (entry does not contain a password).

z/OS V1R6 and later: reason code R007038 (credentials are not valid).

Reference information: *z/OS Integrated Security Services LDAP Server Administration and Use.*

Integrated Security Services actions to perform after the first IPL of z/OS V1R7

This section describes Integrated Security Services migration actions that you can perform only after you've IPLed z/OS V1R7. You need a running z/OS V1R7 system to perform these actions.

EIM: Use RACF profiles instead of the APF authorization extended attribute for applications that access EIM APIs

Description: Before z/OS V1R7, the APF authorization extended attribute had to be turned on for each Enterprise Identity Mapping (EIM) application program accessing the EIM APIs. As of z/OS V1R7, the requirement to turn on the attribute has been removed. You might now need to define RACF profiles that give unauthorized applications the authority to access EIM configuration information stored in RACF profiles. IBM recommends that you turn off the APF authorization extended attribute, unless the application needs it for other reasons or the application is shared between two systems that are at different releases.

Element or feature:	Integrated Security Services.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have an application program that uses an API that retrieves configuration information from RACF profiles.
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:

1. Remove the APF authorization extended attribute for each EIM application program that accesses EIM APIs. Use the following command:

   extattr -a *filename*

   For example, if the filename were eimprog, the command would be:
   ```
   extattr -a eimprog
   ```

2. Decide which RACF profiles need to be created. To use an EIM service that interacts with EIM configuration information stored in RACF profiles, a user needs READ access to one or more of the following resources in the FACILITY class:

FACILITY class resource	Reason access is needed
IRR.RADMIN	The application modifies the EIM configuration settings in RACF profiles.
IRR.RADMIN IRR.RGETINFO.EIM	The application retrieves the EIM configuration settings in RACF profiles.
IRR.RGETINFO.EIM	The application uses EIM to locate mappings between user IDs and makes use of the local registry name stored in a RACF profile.
IRR.DCEKEY IRR.RGETINFO.EIM	The application uses the bind credentials for the EIM domain stored in a RACF profile. Note that in this case you also need to add the program control extended attribute to the application. The application can only run in a clean environment.

3. Create RACF profiles in either of the following ways:
   - Use the RACF RDEFINE command to create the profile that covers the resource, and give the user access by using the UACC keyword.
   - Define the profile and use the RACF PERMIT command to add the user, or a group to which the user belongs (recommended), to the profile's access list.

Reference information:
- For details about EIM and how to set up EIM applications, see *z/OS Integrated Security Services EIM Guide and Reference*.
- For details about the extattr command, see *z/OS UNIX System Services Command Reference*.
- For details about APF authorization, see *z/OS MVS Programming: Authorized Assembler Services Guide*.
- For details about RACF commands, see *z/OS Security Server RACF Command Language Reference*.

Chapter 16. ISPF migration actions

This chapter describes migration actions for base element ISPF.

ISPF actions to perform before installing z/OS V1R7

None.

ISPF actions to perform before the first IPL of z/OS V1R7

This section describes ISPF migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

Reassemble and relink SCLM project definitions

Description: In z/OS V1R5, the macros for the Software Configuration and Library Manager (SCLM) project definitions changed. Therefore, if you're migrating from z/OS V1R4 and don't have PTF UW89007 installed, you have to reassemble and relink-edit all of your SCLM project definitions using the macros provided with the new release.

Element or feature:	ISPF.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4 without PTF UW89007 installed.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use SCLM and have not installed PTF UW89007.
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: Reassemble and relink-edit all of your SCLM project definitions using the macros provided with z/OS V1R7.

If you have modified any of the SCLM-provided macros, you must reintegrate those changes with the new SCLM-provided macros. Failure to do this results in unpredictable results during SCLM execution.

Reference information: For more details about assembling and linking a project definition, see *z/OS ISPF Software Configuration and Library Manager Project Manager's and Developer's Guide*.

ISPF actions to perform after the first IPL of z/OS V1R7

None.

Chapter 17. JES2 migration actions

This chapter describes migration actions for base element JES2.

Some JES2 data sets have been removed from z/OS. See "Remove references to deleted data sets and paths" on page 40. Some JES2 data sets have been added to z/OS. See "Add references to new data sets and paths" on page 53.

JES2 actions to perform before installing z/OS V1R7

This section describes JES2 migration actions that you can perform on your current (old) system. You don't need the z/OS V1R7 level of code to make these changes, and the changes don't require the z/OS V1R7 level of code to run once they are made.

Migrate to z2 mode

Description: Before z/OS V1R7, JES2 could operate in either of two modes, as specified on the $ACTIVATE command: *compatibility (R4) mode* and *full function (z2) mode*. As of z/OS V1R7, JES2 can operate only in z2 mode; R4 mode is withdrawn. z2 mode enables larger limits for jobs, output elements, trackgroup space, and job number range, and improves trackgroup usage tracking. You must migrate to z2 mode before IPLing z/OS V1R7 JES2.

Element or feature:	JES2.
When change was introduced:	z2 mode was introduced in z/OS V1R2–V1R3 JES2. Removal of R4 mode was announced on 10 August 2004 as part of the z/OS V1R6 availability and z/OS V1R7 preview announcement.
Applies to migration from:	z/OS V1R5–V1R6 JES2 and z/OS V1R4 JES2.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you use R4 mode.

Target system hardware requirements:	None.
Target system software requirements:	Tivoli Operations Planning and Control (OPC) V2 (5697-OPC) is no longer service supported. But if you still use it, you will not be able to use JES2 in z2 mode. Use of z2 mode requires the follow-on Tivoli product, which is Tivoli Workload Scheduler for z/OS V8.1 (5697-WSZ).
Other system (coexistence or fallback) requirements:	• This function requires coexistence and fallback PTFs. See "Install coexistence and fallback PTFs" on page 4. • Do not activate z2 mode until all systems in the MAS are at z/OS V1R2 or later JES2.
Restrictions:	None.
System impacts:	None.

Steps to take: You must migrate to z2 mode before IPLing z/OS V1R7 JES2.

In preparing for your migration to JES2 z2 mode, analyze the following:

- Exit routines and unique code that would be affected by activating JES2 in z2 mode. If your exit routines use JQE or JOE chaining fields, or reference job number fields, then z2 mode changes require you to update the exit routines. Field names have been changed to help identify where logic changes are needed.

  You might want to enable your exit routines to support both R4 and z2 modes to facilitate migration. If your exit routines must support systems running in both modes, be aware that fields within control blocks such as the JQE are mode sensitive. For example in R4 mode, use JQEJOBNO_R4 for the job number in a real JQE; in z2 mode, use JQEJBNUM for the job number. However if you are referencing the job number in a JQA (artificial JQE), use JQEJBNUM.

- How your JES2 system processes the JOE, JQE, JQA, and JOT control blocks that are significantly changed in z2 mode.

- Control blocks and fields used to store job numbers (such as the $SJB, $JIB, $FSAXB, and $COMWORK).

- How you use the following JES2 macro services:

  - *$QJQE and $#JOE:* These macros process the JQE and JOE control block chains using proper chaining fields based on the current checkpoint processing mode (either R4 mode or z2 mode). Therefore, users of these macros do not have to be sensitive to which JES2 processing mode is currently being used. $#JOE is changed to process chains (such as the CHAR JOE chain). Both $QJQE and $#JOE have improved their loop control and have usability enhancements.

  - *$DOGJQE:* The JQA returned by $DOGJQE always reflects the z2 mode processing format. Code that processes an artificial JQE (JQA) need not examine the JES2 processing mode (z2 mode or R4 mode) to examine JQA fields.

  - *$JQEJNUM:* $JQEJNUM is a new macro used to obtain the binary job number for a particular JQE. This macro operates in z2 mode and R4 mode and processes the JQA or JQE that is passed.

– *$JBIDBLD:* This macro converts a binary job number to a printable job ID. $JBIDBLD is updated to accept a JQE (or JQA) as input and operates in z2 mode or R4 mode. $JBIDBLD formats the job ID, in the correct way, based on the current job number range.

- Your changes made to support JES2 in R4 mode, to ensure that they are compatible with z2 mode.

After your analysis is complete, perform the following tasks as appropriate for your installation:

- Convert any locally-developed code to use the new fields and field names.
- Process JOE and job queue element (JQE) control blocks as much as possible with the macros provided ($QJQE, $#JOE, $DOGJQE, $JQEJNUM, $JBIDBLD) instead of writing and using your own code.
- Ensure that all the field and control block changes identified with z/OS V1R2 JES2 are incorporated, including updates to the surrounding logic.

You can use the $ACTIVATE command ($ACTIVATE,LEVEL=R4) to revert to R4 mode from z2 mode. Before deactivating z2 mode, z/OS checks that no features exploiting z2 mode are active. If functions are exploiting z2 mode, the $ACTIVATE,LEVEL=R4 command fails with message HASP445. By default, JES2 restarts in the same mode (R4 or z2) 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 R4 mode, specify UNACT on PARM=.

Note: As of z/OS V1R7 JES2, the $ACTIVATE command has been deleted.

Reference information:

- For details about z2 mode support, see *z/OS JES2 Installation Exits*.
- For information about using the $ACTIVATE command, see *z/OS JES2 Commands*.

Review automation that handles message $HASP621

Description: Message $HASP621 displays the number of work elements in a class. Before z/OS V1R7 JES2, if the number exceeded 99999, an incorrect value was displayed. As of z/OS V1R7 JES2, if the number exceeds 99999, ***** is displayed. Be sure that your automation can handle the new display.

Element or feature:	JES2.
When change was introduced:	z/OS V1R7 JES2 (and APAR OA08768 on prior releases).
Applies to migration from:	z/OS V1R5–V1R6 JES2 without PTF UA14804 (for APAR OA08768) installed, and z/OS V1R4 JES2 without PTF UA14803 (for APAR OA08768) installed.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you have automation routines that examine message $HASP621.
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: Review automation routines that handle message $HASP621 to make sure they can handle ***** for the number of work elements, and update any routines that can't handle *****.

Reference information: For a description of message $HASP621, see *z/OS JES2 Messages*.

Update automation that displays certain characteristics of post-execution jobs

Description: Before z/OS V1R5, you could modify (using a $TJ command) or display (using a $DJ command) characteristics of a post-execution job even though those characteristics did not apply in a post-execution environment. As of z/OS V1R5, you cannot display SRVCLASS, SCHENV, SCHENV_AFF, and SECLABEL_AFF for jobs that are post-execution, because JES2 does not maintain these values for jobs once they complete execution.

Element or feature:	JES2.
When change was introduced:	z/OS V1R5–V1R6 JES2.
Applies to migration from:	z/OS V1R4 JES2.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you use automation to modify or display SRVCLASS, SCHENV, SCHENV_AFF, or SECLABEL_AFF for jobs that are post-execution.
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: It is possible that operators or automation scripts might attempt to issue a command to modify a range of jobs (or use some filter) that includes jobs that are already in post-execution processing. Educate your operations staff about this change and review and change automation scripts that issue $Djob and $Tjob commands that attempt to set SRVCLASS= or SCHENV= for post-execution jobs.

Reference information: For information about using the $Djob and $Tjob commands used by operators and automation scripts, see *z/OS JES2 Commands*.

JES2 actions to perform before the first IPL of z/OS V1R7

This section describes JES2 migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

Modify SAPI applications that set SSS2DUPJ

Description: SAPI applications that select sysout data sets by specific job name and set SSS2DUPJ now work differently. Before z/OS V1R7, without the PTF for APAR OA04747 installed, if two jobs in the system matched the name specified in SSS2JOBN and one of them had sysout data sets destined for another node, SSS2DUPJ was not set. As of z/OS V1R7, if two jobs in the system match the name specified in SSS2JOBN and one of them has sysout data sets destined for another node, SSS2DUPJ **is** set.

Element or feature:	JES2.
When change was introduced:	z/OS V1R7 JES2 (and APAR OA047475 on prior releases).
Applies to migration from:	z/OS V1R5–V1R6 JES2 without PTF UA09769 (for APAR OA047475) installed, and z/OS V1R4 JES2 without PTF UA09770 (for APAR OA047475) installed.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have SAPI applications that select sysout data sets by specific job name and set SSS2DUPJ.
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: Modify any applications that are affected by the change in processing.

Reference information: For details about writing JES2 applications, specifically SAPI applications that set SSS2DUPJ, see *z/OS MVS Using the Subsystem Interface*.

Remove the RELADDR= parameter from SPOOLDEF initialization statements

Description: In z/OS V1R2 (and rolled back to OS/390 V2R10 by an APAR), JES2 added initial support for large SPOOL volumes by allowing you to place a SPOOL data set anywhere on a volume, with the size of the SPOOL data set limited to 64K tracks. Also in z/OS V1R2, the keyword RELADDR= was added to the SPOOLDEF initialization statement to specify relative track addressing. Because older releases did not support relative track addressing, this keyword specified that relative addressing was allowed when a new SPOOL volume was started.

In z/OS V1R7, JES2 introduces support for SPOOL volumes greater than 64K tracks. Because of this larger SPOOL volume support and because compatibility with older releases is no longer an issue, the RELADDR= keyword is no longer supported and you should discontinue using it. All new SPOOL volumes started in z/OS V1R7 use relative track addressing.

Element or feature:	JES2.

When change was introduced:	z/OS V1R7 JES2.
Applies to migration from:	z/OS V1R5–V1R6 JES2 and z/OS V1R4 JES2.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if SPOOLDEF RELADDR= is set to NEVER.
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: Remove RELADDR= from the SPOOLDEF initialization statement in your z/OS V1R7 initialization deck. If you don't remove it, RELADDR=ALWAYS or RELADDR=ASNEEDED is ignored, but RELADDR=NEVER results in an invalid statement error and the entire SPOOLDEF statement is not processed.

Specify SPOOLDEF RELADDR=ALWAYS on pre-z/OS V1R7 members that share SPOOL with z/OS V1R7 by updating their initialization decks and by issuing the command $TSPOOLDEF,RELADDR=ALWAYS on one pre-z/OS V1R7 MAS member.

z/OS V1R7 JES2 continues to support existing SPOOL volumes that use absolute track addressing. No changes to your existing SPOOL volumes are needed. Only new volumes that are started by a z/OS V1R7 JES2 are affected by removal of support for the RELADDR= keyword.

Reference information: *z/OS JES2 Initialization and Tuning Reference*.

Update JES2 exit routines because of z/OS V1R7 structure changes

Description: In z/OS V1R7 JES2, some NJE and input service functions were moved from the JES2 address space to application address spaces. This was done to improve performance and reliability as well as reduce system outages. In particular, the new NJE over TCP/IP (NJE/TCP) function and existing internal reader (INTRDR) processing now occur outside the JES2 address space. This can break processing done by the following JES2 exit routines: 2, 3, 4, 7, 8, 13, 20, 36, 37, 39, 40, 46, 47, and 49.

The specific changes are:
- Exits 2, 3, 4, 7, 20, 39, 46, and 47 are not called for INTRDRs and NJE/TCP processing.
- Exit 8 is now called for INTRDR and NJE/TCP processing.
- Exits 36 and 37 now get control in a different address space for INTRDR and NJE/TCP processing.
- Exit 13 has been deleted.
- Exit 49 has new function and is being called for $S J commands.
- Exit 40 can now be used to control NJE mail notification (function that was in exit 13).
- The input to exits 2, 3, 4, 20, 46, and 47 has changed significantly.

If you are using any of these changed exits, examine your routines and modify them if necessary.

Element or feature:	JES2.
When change was introduced:	z/OS V1R7 JES2.
Applies to migration from:	z/OS V1R5–V1R6 JES2 and z/OS V1R4 JES2.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use any of the 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.

Steps to take: Modify your exit routines to take into account the changes in "Description" above. See *z/OS JES2 Installation Exits* for details about the functions and interfaces of the changed exits.

Some services have been added to z/OS V1R7 JES2 to help you rework your exit routines to support the new environment. The services are a new USER,ANY environment, local $JCT extensions, $BLDMSG and $SCAN support, table pair enhancements, and multiple exit 0s. These services are discussed in *z/OS JES2 Macros* and *z/OS JES2 Installation Exits*.

Reference information: For the reasons stated above, see *z/OS JES2 Installation Exits* and *z/OS JES2 Macros*.

Update automation and procedures because of changed input processing

Description: In z/OS V1R7 JES2, input processing was rewritten to support NJE over TCP/IP and internal reader changes. If any of your automation or procedures are affected by the changed processing, you have to modify them. The changes are:

* **JCL/JECL processing:** In previous releases, error messages for erroneous statements simply stated that the statement was incorrect (for example, `HASP112 jobname -- INVALID /*JOBPARM CARD`). In z/OS V1R7 JES2, these messages include details about the operand in error (for example, `HASP112 jobname -- INVALID /*JOBPARM CARD - VALUE OF CARDS= EXCEEDS 99999999`). You might need to update processing that examines error messages.

  In z/OS V1R7 JES2, the parsing of operands has been modified to conform to standard JCL rules. Some JCL that would result in errors in earlier releases now runs correctly. For example, SECLABEL='SYSHIGH' is allowed in z/OS V1R7 but is not processed correctly in previous releases. Pre-z/OS V1R7 JES2 code does not support the use of apostrophes with SECLABEL. Because of this, be careful when developing JCL in z/OS V1R7 JES2 that is to be run on previous releases. Test JCL on the target release to ensure that it is processed correctly.

* **SYSIN data processing:** In z/OS V1R7 JES2, the processing of SYSIN data sets has been updated to properly handle carriage control, variable record

formats, and SYSIN records up to 32 KB in length. Because of this, job streams that work in z/OS V1R7 might fail in prior releases of JES2. However, jobs submitted on z/OS V1R7 will run correctly on other MAS members, even if the member they run on is pre-z/OS V1R7.

- **Internal reader processing in requestor address space:** In z/OS V1R7 JES2, internal reader processing has been moved from the JES2 address space to the address space that allocated the internal reader. This was done to allow multiple job streams to be processed in parallel and to improve error isolation. However, because the processing is now in the owner address space, CPU and I/O activity that was previously associated with the JES2 address space is now associated with the owning address space. In addition, because the processing occurs in the address space that owns the internal reader, the processing occurs at the dispatching priority of the requestor instead of JES2's priority. Thus, in a busy system, low priority address spaces are not able to submit jobs as fast as higher priority address spaces.

- **Buffering of data in internal readers:** Before z/OS V1R7 JES2, jobs submitted to an internal reader were buffered in 8 KB buffers in a data space. The buffers were not processed until the internal reader was closed, an ENDREQ was issued, or a /*EOF or /*DEL card was processed. In z/OS V1R7 JES2, the cards are processed as soon as they are passed to the internal reader. There is no buffering of data and the internal reader data space no longer exists.

- **Internal reader messages in JOB log:** In z/OS V1R7 JES2, internal reader processing has been moved to the submitting address space. This causes input processing messages (such as $HASP100) to be issued in the submitting address space and to be placed in the JOB log (JESMSGLG) of the submitting address space. This is useful for verifying the status of jobs that are submitted. However, it can increase the size of the JOB log, especially for address spaces that submit a significant number of jobs. If the size of the JOB log becomes a concern, consider using the JESLOG JOB card parameter to spin or suppress the JOB log data set.

- **Internal reader processing when JES2 address space fails:** Before z/OS V1R7 JES2, JES2 discarded any job that was on an internal reader when the JES2 address space abnormally terminated. With z/OS V1R7 JES2, JES2 attempts to retain jobs that are active on an internal reader when JES2 terminates. However, in some cases, JES2 still discards a job because of lost checkpoint updates.

Element or feature:	JES2.
When change was introduced:	z/OS V1R7 JES2.
Applies to migration from:	z/OS V1R5–V1R6 JES2 and z/OS V1R4 JES2.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if any of the changes impact your automation or procedures.
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: Review your automation and procedures, and update them as needed based on the changes in "Description" above.

Reference information: *z/OS JES2 Initialization and Tuning Guide*.

Adjust debugging procedures because SVC 111 is no longer used for PUTs to an internal reader

Description: In z/OS V1R7, many uses of SVC 111 were converted to stacking Program Call (PC) instructions. As a result, when you debug problems related to internal readers, you must look for the JES2 PC trace entries rather than SVC 111 trace entries to understand what JES2 is doing.

Element or feature:	JES2.
When change was introduced:	z/OS V1R7 JES2.
Applies to migration from:	z/OS V1R5–V1R6 JES2 and z/OS V1R4 JES2.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you debug problems using system trace.
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: Evaluate your debugging procedures for the system trace impacts.

Reference information: For information about how to use system trace, see *z/OS MVS Diagnosis: Tools and Service Aids*.

Correctly process ENF58 records for SYSOUT checkpoints

Description: In releases before z/OS V1R5, JES2 generates an ENF 58 record as SYSOUT data sets allocated with a client token are processed. This allows an application to track the progress of a SYSOUT data set as it is processed. However, once a data set starts printing, there are no status updates until the printing has completed. There is no indication of progress (or lack of progress) while the data set is printing.

To address this deficiency in ability to track progress, JES2 is updated to generate an ENF 58 record whenever a SYSOUT data set is checkpointed. A new qualifier is used on this ENF record. The rate at which these ENF records are issued is determined by the checkpoint interval on the printer that is processing the SYSOUT data set.

Element or feature:	JES2.
When change was introduced:	z/OS V1R5–V1R6 JES2.
Applies to migration from:	z/OS V1R4 JES2.
Timing:	Before the first IPL of z/OS V1R7.

Is the migration action required?	Yes, if you have applications that process all ENF 58 records (with no qualifier).
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:

1. Review your frequency of checkpointing based on the addition of ENF58 record generation. You might find that updates to the PRT*nnnn* checkpoint parameters are appropriate for better system tuning. Frequent checkpoints can slow down printing and increase system overhead. A balance needs to be achieved between the overhead of printers taking a checkpoint and the currency of information displayed by applications listening to ENF 58.

2. If you have an application that listens for ENF 58 record generation, review that code and consider updating it to be certain to process this new qualifier correctly. Correctly structured code should not need updating; however, consider the following code scenario:

   a. There were 10 possible qualifiers for ENF58 when the exit was written.

   b. Code that listens to ENF58 tests for the first nine qualifiers explicitly.

   c. If not one of the first nine, the code assumes that the qualifier is the 10th.

   d. Now that a new qualifier is added (number 11 for "checkpoint issued"), this same code would mistakenly assume that qualifier 11 (not one of the nine explicitly tested) is qualifier 10 (the one not explicitly tested but assumed above).

   Your quick review of any ENF58 installation-provided processing code you now have might prove useful.

Reference information:

- For more details about affecting and tuning JES2 checkpoint record writing frequency, see *z/OS JES2 Initialization and Tuning Reference*.
- For more details about ENF58 records and client tokens, see *z/OS MVS Using the Subsystem Interface*.

Update exit 34 to support PSO unallocation flagging

Description: In JES2 exit 34 (subsystem interface data set unallocation), decimal offset 16 of register 1 contains the address of a peripheral data definition block (PDDB). Previously this address could be set to zero only if the data set type is a regular internal reader or an unknown data set type. It is now also set to zero if a PSO unallocation was performed after the job step TCB ended.

Element or feature:	JES2.
When change was introduced:	z/OS V1R5–V1R6 JES2.
Applies to migration from:	z/OS V1R4 JES2.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use JES2 exit 34

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: Examine your exit 34 code to ensure that the potential zero address for PSO unallocation can be processed correctly.

Reference information: For information about coding an exit 34 routine to affect subsystem interface data set unallocation, see *z/OS JES2 Installation Exits*.

Update exit routines to recognize null service class for WLM processing

Description: z/OS uses the default workload manager (WLM) policy when z/OS is started without a WLM couple data set or if there is a problem or error when accessing the current policy in the WLM couple data set. The default WLM policy assigns a null service class (SRVCLASS= on a $D*job* command) to all jobs. Previously, batch jobs in a WLM-managed job class that were assigned a null service class would not be selected for execution. Now these jobs are eligible for execution.

Element or feature:	JES2.
When change was introduced:	z/OS V1R5–V1R6 JES2.
Applies to migration from:	z/OS V1R4 JES2.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you are using WLM-managed initiators (that is, if you specify MODE=WLM on any JOBCLASS(x) statements).
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: Update exit routines and automation code to recognize a null service class as valid for jobs awaiting execution and in execution. This change implies that WLM-managed initiators will now select jobs with a null service class. This could impact data that is presented through SMF and information passed in various data areas. You should examine code that uses service classes to ensure that it properly handles a null or blank value.

Reference information:
- For information about using the $D*job* command used by operators and automation scripts, see *z/OS JES2 Commands*.
- For information about coding exit routines, see *z/OS JES2 Installation Exits*.

JES2 actions to perform after the first IPL of z/OS V1R7

This section describes JES2 migration actions that you can perform only after you've IPLed z/OS V1R7. You need a running z/OS V1R7 system to perform these actions.

Remove the RDINUM= parameter from INTRDR initialization statements

Description: In z/OS V1R7 JES2, internal reader processing was updated to move processing from the JES2 address space to the address space that allocates the internal reader. With this change, the table of internal readers that was maintained in ECSA is no longer required. The data areas that represent the internal reader are now in the private storage of the allocating address space. Because the table of internal readers no longer exists, you no longer need to specify the size of the table. As a result, the RDINUM= parameter, which specified the number of internal readers, has been removed from the INTRDR initialization statement. You should remove the obsolete RDINUM= parameter from your INTRDR initialization statements.

Element or feature:	JES2.
When change was introduced:	z/OS V1R7 JES2.
Applies to migration from:	z/OS V1R5–V1R6 JES2 and z/OS V1R4 JES2.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended to avoid confusion in the future.
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: Delete the RDINUM= parameter from the INTRDR statement in your initialization stream. If you don't delete it, it is ignored and no error message is generated. Nevertheless, deleting it can help avoid confusion by anyone who encounters it in the future and is unaware that it is no longer functional. Moreover, although the parameter is ignored now, it might not be ignored in a future release.

Reference information: *z/OS JES2 Initialization and Tuning Reference*.

Chapter 18. JES3 migration actions

This chapter describes migration actions for optional feature JES3.

JES3 actions to perform before installing z/OS V1R7

None.

JES3 actions to perform before the first IPL of z/OS V1R7

This section describes JES3 migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

Change OSEDBYCT to OSEDBYTE

Description: The data set byte count in the IATYOSE macro was changed to a 3-byte numeric field and the name of the field was changed to OSEDBYTE by APAR OA04281. OSEDBYCT, which mapped the low-order two bytes of this field, has been deleted.

Element or feature:	JES3.
When change was introduced:	z/OS V1R7 JES3.
Applies to migration from:	z/OS V1R5–V1R6 JES3 and z/OS V1R4 JES3.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use the IATYOSE macro.
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: Change any exit or modification code that refers to the field name OSEDBYCT to refer to OSEDBYTE instead, and to handle OSEDBYTE as a 3-byte field.

Reference information: None.

Update programs that obtain JES3 working set histogram data from SMF type 84 records

Description: Users of the JES3 monitoring facility (JMF) can produce a histogram of JES3 working set sizes. If requested, this data can be recorded in SMF type 84 records. These records contain plot table entries, in 100 KB increments (where KB equals 1024 bytes), starting with the smallest working set value that is found and ending with the largest one found. Each entry was two words: word 1 contains the working set size in KB and word 2 contains the number of times the working set size was at this KB value.

Before z/OS V1R7 JES3, entries in which word 2 was 0 were included in the SMF data. Starting with z/OS V1R7 JES3, entries in which word 2 is 0 are no longer included. If the histogram data is being used to generate a report and the 0-count entries are needed, the program generating the report has to create them.

Element or feature:	JES3.
When change was introduced:	z/OS V1R7 JES3.
Applies to migration from:	z/OS V1R5–V1R6 JES3 and z/OS V1R4 JES3.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if the SMF type 84 working set size data is used for report generation.
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: Before the first time that SMF data will be used to create a working set size report, update the report generating program to supply 0-count entries. One way to determine the number of 0-count entries to include is to process the first entry (call this entry *x*), subtract the size of entry *x* (in KB) from the size of entry *x*+1, and divide the result by 100. The result, minus 1, is the number of 0-count entries that need to be generated before processing entry *x*+1. Then make entry *x*+1 the *x* entry and repeat this process until the high count value is processed. Note that the incremental value can be obtained from field R84WSINC in the SMF type 84 record.

Reference information:

- For details about SMF record type 84, see *z/OS MVS System Management Facilities (SMF)*.
- For information about starting JMF, see *z/OS JES3 Commands*.

Change exits and modifications to use IATXDATX

Description: The DATCC prefix size in the IATYDAT macro increased in z/OS V1R5. If you have any exits or modifications that use the length of DATCC or reference DATXMLEN (which depends on the prefix size), or use the field SVTMUBLN in the IATYSVT macro or the field TVTMUBLN in the IATYTVT macro (both of which depend on the prefix size) to determine the amount of room left in a buffer, you must change this code to use the IATXDATX macro.

Element or feature:	JES3.
When change was introduced:	z/OS V1R5–V1R6 JES3 and rolled back to z/OS V1R4 JES3 and z/OS V1R2–V1R3 JES3 by APAR OW57535.
Applies to migration from:	z/OS V1R4 JES3.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have any user exits or modifications that use the DATCC value to advance from the DAT prefix to the data within spooled records.
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: Recode any user exits or modifications that use the DATCC value to advance from the DAT prefix to the data in spooled records to instead use the IATXDATX macro.

Reference information: For details about using the IATXDATX utility, see *z/OS JES3 Customization*

Update the BFSIZ parameter on the NJERMT statement

Description: Starting in z/OS V1R5, JES3 spool records have an additional two bytes in the prefix. Because of this, the maximum buffer size for an NJERMT statement (BFSIZ parameter) is now the maximum buffer size on the BUFFER BUFSIZE parameter minus 46, instead of minus 44.

Element or feature:	JES3.
When change was introduced:	z/OS V1R5–V1R6 JES3.
Applies to migration from:	z/OS V1R4 JES3.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have any directly connected BSC NJE nodes and do not allow the buffer size to take the default.
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: If you have any NJERMT statements that specify a BFSIZ parameter that is larger than BUFFER,BUFSIZE minus 45, recode the BFSIZ parameter on the NJERMT statement to be BUFFER,BUFSIZE minus 46 instead of BUFFER,BUFSIZE minus 44.

Reference information: For details about using the NJERMT statement, see *z/OS JES3 Initialization and Tuning Reference*.

JES3 actions to perform after the first IPL of z/OS V1R7

None.

Chapter 19. Language Environment migration actions

This chapter describes migration actions for base element Language Environment.

Some Language Environment data sets have been removed from z/OS. See
"Remove references to deleted data sets and paths" on page 40.

Language Environment actions to perform before installing z/OS V1R7

This section describes Language Environment migration actions that you can
perform on your current (old) system. You don't need the z/OS V1R7 level of code
to make these changes, and the changes don't require the z/OS V1R7 level of code
to run once they are made.

Migrate from use of RTLS

Description: Effective with z/OS V1R6, Language Environment's use of run-time
library services (RTLS) is discontinued. z/OS V1R5 is the last release that included
the support. This function has been used primarily in run-time migration. Given the
stability and the upward compatibility being provided by the Language Environment
run-time library in recent releases of OS/390 and z/OS, this functionality is no
longer required.

Element or feature:	Language Environment.
When change was introduced:	The removal of Language Environment support for RTLS was announced in May 2003. z/OS V1R5 is the last release in which the function was available.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you use RTLS with Language Environment or if you have any CEEUOPT or CEEROPT modules that contain RTLS, VERSION, or LIBRARY run-time options.
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: Remove any references that your applications make to the LIBRARY, RTLS, and VERSION run-time options. All references to these run-time options are removed from the CEEDOPT, CEECOPT, CEEROPT, and CEEUOPT modules, and from all options reports.

Note that existing CEEUOPT and CEEROPT modules might contain RTLS, VERSION, or LIBRARY options. If so, you can use them unchanged on z/OS V1R7. Informational message CEE3611I is issued to indicate that the run-time options are ignored. To eliminate the message, modify the CEEUOPT or CEEROPT module.

Reference information: For information about use of RTLS with Language Environment, see the following documents for the release from which you're migrating: *z/OS Language Environment Customization* and *z/OS Language Environment Programming Reference*.

Migrate from use of the DLL Rename Utility

Description: Effective with z/OS V1R6, IBM has removed the Dynamic Link Library (DLL) Rename Utility, which was in Language Environment. z/OS V1R5 was the last release that included the utility. This utility was used to package and redistribute IBM-supplied DLLs with applications. Since OS/390 V1R3, the C/C++ DLLs have been licensed with the OS/390 and z/OS base operating systems. Therefore, the DLL Rename Utility is no longer required.

Element or feature:	Language Environment.
When change was introduced:	The removal of the DLL Rename Utility was announced in October 2003. z/OS V1R5 was the last release in which the utility was available.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you use the DLL Rename Utility.
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: Stop using the DLL Rename Utility if you have not already done so.

Reference information: For information about building and using DLLs, see *z/OS XL C/C++ Programming Guide*.

Language Environment actions to perform before the first IPL of z/OS V1R7

This section describes Language Environment migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't 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 member CEECCSD and, if using CICS Transaction Server (TS) for z/OS V3 (5655-M15), in member CEECCSDX.

For example, in z/OS V1R2, the CLER CICS transaction was added to display run-time options under CICS and alter a subset of options. Therefore, you must define the CLER transaction in the CICS CSD. The CEECCSD sample job in the *hlq*.SCEESAMP data set has been updated to include the CSD entries for the CLER transaction.

Element or feature:	Language Environment.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes.
Target system hardware requirements:	None.
Target system software requirements:	CICS
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Steps to take: Update the CSD file using the program definitions in member CEECCSD (and member CEECCSDX if using CICS TS V3) found in the *hlq*.SCEESAMP data set.

Note: The group containing the Language Environment run-time routines must be in the group list used during CICS startup.

Reference information: *z/OS Language Environment Run-Time 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's still suitable.

Element or feature:	Language Environment.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

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 PROG*xx* member of SYS1.PARMLIB that includes all Language Environment CEE-prefixed run-time 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 run-time support.
- *EDCWLPA:* This is a sample of a PROG*xx* member of SYS1.PARMLIB that includes all Language Environment EDC-prefixed and CEH-prefixed run-time modules eligible for the LPA (that is, all XL C/C++ component modules) except locales and code page converters.
- *IBMALLP2 (or IBMPLPA1 for VisualAge® PL/I):* 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 highly recommends that you place the SCEELPA data set in the LPA list (LPALST*xx*). 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: 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*, Appendix D. The tables 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 the impact of changes to default run-time options

Description: Periodically, Language Environment introduces new run-time options, adds new suboptions to existing run-time options, and changes the defaults of run-time options. Before migrating to a new release of z/OS, you should review the run-time option values for the new release.

In z/OS V1R7, a new parmlib member, CEEPRM*xx*, was added for Language Environment. You can use it to specify Language Environment run-time options for the system. Operator commands are also provided to allow you to query and update the active run-time options for the system. This simplifies the management of Language Environment options, particularly in multisystem environments, and makes it possible to move Language Environment customization out of assembler language modules maintained using SMP/E usermods. However, specifying Language Environment options using CEEDOPT, CEECOPT and CELQDOPT modules continues to be supported.

In z/OS V1R7 and z/OS V1R6, there were no changes to Language Environment run-time options.

In z/OS V1R5, the following changes were made to Language Environment run-time options:

- HEAPCHK now has a pool depth suboption.
- HEAPPOOLS has several new suboptions that allow you to define six additional pools.

Element or feature:	Language Environment.
When change was introduced:	z/OS V1R7 and z/OS V1R5.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you updated the installation-wide run-time options CSECT (CEEDOPT or CEECOPT) in a previous release.
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:

- Consider using CEEPRM*xx*, the new parmlib member added in z/OS V1R7.
- Compare your existing source for the installation-wide run-time options CSECT, CEEDOPT (non-CICS environment) or CEECOPT (CICS environment), with the

new samples in *hlq*.SCEESAMP to determine whether you need to change your defaults. If changes are necessary, you must make them and apply the corresponding usermods.

If you don't update your previous CEEDOPT or CEECOPT with the new HEAPCHK and HEAPPOOLS suboptions, the assembly of the previous usermods will fail. If you don't install any usermods whatsoever, Language Environment uses the default values.

Reference information:

- For details about using the new suboptions, changing CEEDOPT and CEECOPT, and specifying CEEPRM*xx*, see *z/OS Language Environment Customization*.
- For CEEDOPT and CEECOPT samples, see the *hlq*.SCEESAMP data set.

Update applications that do not use standard interfaces to process a utmpx database

Description: The `/etc/utmpx` file contains a user accounting database. In z/OS V1R6, the format of the utmpx records is extended to support longer remote host names (`ut_host`) of up to 1024 bytes. The new format also supports the natural growth of the 64-bit `timeval` structure, providing a separate `ut_tv` element for applications compiled as 64-bit. Finally, an internal element, `ut_version`, replaces space formerly taken up for alignment and is used by the library to distinguish the utmpx record format.

Existing applications (compiled before z/OS V1R6) that use the standard interfaces to process a utmpx database will continue to run as before, with the same mappings. The offsets of existing elements in the old format have not changed. Applications will simply not "see" beyond the first 32 bytes of `ut_host`. (Of course, if you want your applications to reference any of the new elements, you will have to modify and recompile the applications.)

Existing applications that *do not* use the standard interfaces to process a utmpx database must be rewritten for use on a z/OS V1R7 system.

Element or feature:	Language Environment.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have applications that do not use the standard interfaces to process a utmpx database.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	Install PTF UQ85892 on z/OS V1R5 or UQ85891 on z/OS V1R4, unless you already installed them as part of "Install coexistence and fallback PTFs" on page 4.
Restrictions:	A single utmpx database cannot contain records in both old and new record formats.
System impacts:	None.

Steps to take: Rewrite applications that use nonstandard interfaces to process a utmpx database. For details, see the utmpx.h header shipped with z/OS V1R7.

If possible, convert to use of standard interfaces so that future changes do not impact you. The standard interfaces include the following C functions: setutxent(), getutxent(), getutxid(), getutxline(), pututxline(), and endutxent().

Reference information: For details about using utmpx, see *z/OS XL C/C++ Run-Time Library Reference*.

Language Environment actions to perform after the first IPL of z/OS V1R7

This section describes Language Environment migration actions that you can perform only after you've IPLed z/OS V1R7. You need a running z/OS V1R7 system to perform these actions.

Accept the new putenv() default

Description: The XL C/C++ function `putenv()` has changed to place the string passed to `putenv()` directly into the array of environment variables. This behavior assures compliance with the POSIX standard.

Before the change, the storage used to define the environment variable passed to `putenv()` was not added to the array of environment variables. Instead, the system copied the string into system allocated storage. You can still achieve this prior behavior, if desired, by using the environment variable *_EDC_PUTENV_COPY*.

Element or feature:	Language Environment.
When change was introduced:	z/OS V1R5 and rolled back to z/OS V1R4, z/OS V1R3, and z/OS V1R2 by APAR PQ61928.
Applies to migration from:	z/OS V1R4 without APAR PQ61928 installed.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended in order to be POSIX compliant.
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 the new, POSIX-compliant behavior of `putenv()`, do nothing; it's now the default condition.

To restore the previous behavior of `putenv()`, which is not POSIX compliant, follow these steps:

1. Be sure the environment variable *_EDC_PUTENV_COPY* is available on your z/OS V1R7 system.
2. Set the environment variable to *_EDC_PUTENV_COPY=YES*.

Reference information: For details about using `putenv()` and *_EDC_PUTENV_COPY*, see *z/OS XL C/C++ Run-Time Library Reference* and *z/OS XL C/C++ Programming Guide*.

Chapter 20. Library Server migration actions

This chapter describes migration actions for base element Library Server.

Before z/OS V1R5, this element was named BookManager BookServer.

Some Library Server data sets have been added to z/OS. See "Add references to new data sets and paths" on page 53.

Library Server actions to perform before installing z/OS V1R7

None.

Library Server actions to perform before the first IPL of z/OS V1R7

This section describes Library Server migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't 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 MVS data sets and the names of the HFS directories that Library Server reads and writes during execution. The information in `booksrv.80` includes the HFS directory names of book collections, shelves, and bookcases. 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.)

Element or feature:	Library Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

Steps to take: Copy your current (customized) configuration files, `bookmgr.80` and `booksrv.80`, to your new system. 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 a complete description of each parameter of the Library Server configuration files, see *z/OS Program Directory*.

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.

Element or feature:	Library Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

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 complete description of each parameter of the Library Server configuration files, see *z/OS Program Directory*.

Library Server actions to perform after the first IPL of z/OS V1R7

None.

Chapter 21. NFS migration actions

This chapter describes migration actions for base element Network File System (NFS).

NFS actions to perform before installing z/OS V1R7

None.

NFS actions to perform before the first IPL of z/OS V1R7

This section describes NFS migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

Install the PTF for APAR OA13792 to avoid message GFSC729W

Description: In z/OS V1R7, the z/OS NFS client socket requirement increased, which can cause the issuance of message GFSC729W (z/OS NFS CLIENT IS UNABLE TO RESERVE *d_digit* SOCKETS, CURRENT MAXFILEPROC IS *d_digit*). Installing the PTF for APAR OA13792 on z/OS V1R7 allows NFS to reserve a higher limit for its network sockets and eliminates the warning message when the NFS client is started.

Element or feature:	NFS.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended to prevent message GFSC729W from being issued.
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: Install the PTF for APAR OA13792.

Reference information: For details about message GFSC729W, see the client messages in the message chapter of *z/OS Network File System Guide and Reference.*

Define new NFS site attributes for starting NLM and NSM

Description: Before z/OS V1R7, the Network Lock Manager (NLM) and Network Status Monitor (NSM) components of NFS had to be started with a series of commands issued in the correct sequence. As of z/OS V1R7, the startup procedure is simplified. Instead of the series of commands (which is no longer supported), the site attributes file contains a new parameter, NLM or NONLM, which indicates whether NLM and NSM are to be started along with NFS. Use this new parameter to indicate how NLM and NSM should be started.

Element or feature:	NFS.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use NLM.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	If NONLM is specified, the NLM cannot be started after NFS has been initialized. See "Steps to take" below for more information.

Steps to take: In the NFS site attributes file, code the NLM or NONLM parameter to indicate whether NLM and NSM are to be started with NFS:

NLM
Specifies that the initialization of the z/OS NFS server should include starting the NLM and NSM daemons.

NONLM
Specifies that the initialization of the z/OS NFS server should not include starting the NLM and NSM daemons. The system will run without lockd and statd. Specifying NONLM does not affect the availability of byte range locking and share reservation support for NFS version 4 protocol access. NONLM is the default.

Note: If NONLM is specified, the NLM cannot be started after NFS has been initialized. If NLM is desired, you must stop and restart NFS after specifying the NLM site attribute. The only way to stop NLM is to shut down the NFS server.

The lock data sets must always be allocated, even if NONLM is specified in the site attributes.

The NLM and NSM startup procedures are not shipped in z/OS V1R7 because they are obsolete. Do not use old copies from previous releases on V1R7.

Because the NLM and NSM startup procedures are no longer used, it is no longer necessary to define them to a z/OS UNIX segment to RACF as UID(0). As cleanup in your security definitions, remove the UID(0) definition in the z/OS UNIX segment of the startup procedures.

Reference information: For details about allocating the NFS lock data sets, see *z/OS Network File System Guide and Reference*.

Convert NFS lock data sets from HFS files to VSAM data sets

Description: Before z/OS V1R7, lock data sets for NFS were HFS files that had to be rewritten in their entirety to remove any entries, and they contained only client host names, which provided no coherency checking after a server restart. To solve these problems, in z/OS V1R7 the lock data sets are VSAM key-sequenced data sets that record the client host IP address and, for NFS V4, the NFS client ID as well as the client host name. Following a server outage, the NFS server reads the new lock data sets during initialization to determine which clients can reclaim locks.

When the z/OS V1R7 NFS server is started, you need to allocate the new lock data sets.

Element or feature:	NFS.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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:	When the z/OS NFS V1R7 server is started for the first time, it will not read the old HFS lock files. Therefore, if there were client applications that held locks when the z/OS system was brought down before migrating to z/OS V1R7, the first NFS grace period will not allow any lock reclaims.

Steps to take: Allocate two lock data sets for NFS using the sample JCL provided in the GFSAMHDJ member of SYS1.SAMPLIB. The two lock data sets should be allocated on separate DASD volumes to reduce the possibility that a single failure would result in the loss of both data sets. The lock data sets must be allocated and pointed to by the LDBASE DD statement and LDBASE2 DD statement in the MVSNFS procedure, even if NONLM is specified in the site attributes.

The following files are obsolete as of z/OS V1R7. If they are present in the /etc directory, delete them:

    statd.sm
    statd.sm@bak
    statd.state
    d.sm
    d.sm@bak

d.state
lockd.logfile

Reference information: For details about allocating the NFS lock data sets, see the section "Lock data sets" in the Customization chapter of *z/OS Network File System Guide and Reference*.

Reallocate NFS mount handle data sets with larger record lengths

Description: The z/OS NFS server uses two mount handle data sets to record clients' active mounts of server resources and to allow clients to maintain mounts when the server is shut down and restarted. Before z/OS V1R7, the mount handle data sets had to be allocated with a maximum record length of 1600 bytes and an average record length of 400 bytes. In z/OS V1R7, some fields in the records are expanded to allow for larger IP addresses and other changes. Therefore, the mount handle data sets must be reallocated with larger record lengths. After the data sets are reallocated, copy records from the previous mount handle data sets into the new data sets. The NFS server must be started with the default *nodhcp* site attribute value, to support static client addresses in the existing records.

Note: Because of changes in file system type used by z/OS UNIX, some NFS mount handle database records might not be usable when the z/OS NFS server is brought up in z/OS V1R7. Object file IDs that are changed will not match file IDs saved in mount handle records, so the file handle can no longer locate the object it is intended for. Such unusable records will eventually be deleted from nonuse.

Element or feature:	NFS.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use NFS.
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:

- Before the z/OS V1R7 NFS server is started, reallocate the two mount handle data sets with a maximum record length of 2000 bytes and an average record length of 1700 bytes. Use the sample JCL provided in the GFSAMHDJ member of SYS1.SAMPLIB, specifying a record size parameter of *RECSIZE(1700 2000)*.

- After the mount handle data sets are reallocated, copy records from the previous data sets into the new ones, using a method such as the IDCAMS REPRO command.

- Start the NFS server with the site attribute value of *nodhcp*, specifying that the dynamic host configuration protocol not be used. It is important to use *nodhcp* because previous mount handle database records will not contain client host names, and when the NFS Server is run in *dhcp* mode, records missing host names are skipped. The first time the z/OS NFS V1R7 Server is shut down, it will

update the MHDB with client host names. Therefore, after this, if the server is started with DHCP mode, the records will not be skipped.

- If you want the server to accept dynamic IP addresses for the NFS client, using the dynamic host configuration protocol, shut down the server and restart it with the *dhcp* site attribute specified.

Reference information: For details about allocating the NFS mount handle data sets, see the sections "Mount handle data sets" and "Using dynamic client IP addressing" in the customization chapter of *z/OS Network File System Guide and Reference*. See also the descriptions of the *dhcp* and *nodhcp* site attributes in the chapter "Initialization attributes for the z/OS NFS Server".

Add new component trace member CTINFS00 to parmlib

Description: Beginning in z/OS V1R7, diagnostic information for the z/OS NFS server can be recorded in z/OS component trace buffers. This function involves the use of a new default parmlib member, CTINFS00. This new parmlib member must be copied to parmlib from the sample parmlib shipped with z/OS V1R7.

Element or feature:	NFS.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you plan to use the z/OS NFS server.
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: Copy sample CTRACE member CTINFS00 to parmlib and, if desired, customize it.

Reference information: For details about using component trace for the z/OS NFS server, see the diagnosis chapter in *z/OS Network File System Guide and Reference*.

Update the NFS client procedure

Description: Beginning in z/OS V1R7, NFS exploits new binder capabilities that eliminate the prelink process. The result is that APARs will only ship modified parts, making PTFs much smaller. As a part of this packaging restructure, SYS1.NFSLIB is now shipped as a PDSE, SYS1.NFSLIBE.

Element or feature:	NFS.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you plan to use the z/OS NFS client.
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: Update the STEPLIB statement in the NFS client procedure to point to the new DSN=&SYSNFS..NFSLIBE library.

Reference information: None.

Update the NFS server procedure

Description: Beginning in z/OS V1R7, NFS exploits new binder capabilities that eliminate the prelink process. The result is that APARs will only ship modified parts, making PTFs much smaller. As a part of this packaging restructure, SYS1.NFSLIB is now shipped as a PDSE, SYS1.NFSLIBE.

Beginning in z/OS V1R7, the NFS server also requires that the NFS lock data sets be allocated and defined.

Element or feature:	NFS.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you plan to use the z/OS NFS server.
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: Update the STEPLIB statement in the NFS server procedure to point to the new DSN=&SYSNFS..NFSLIBE library. Update the LDBASE DD statement and LDBASE2 DD statement in the MVSNFS procedure to point to the new lock data sets.

Reference information: None.

NFS actions to perform after the first IPL of z/OS V1R7

This section describes NFS migration actions that you can perform only after you've IPLed z/OS V1R7. You need a running z/OS V1R7 system to perform these actions.

Authorize the z/OS NFS server for component trace

Description: Beginning in z/OS V1R7, diagnostic information for the z/OS NFS server can be recorded in z/OS component trace buffers. This function involves the use of a new default parmlib member, CTINFS00. The z/OS NFS server task must be authorized to read the PARMLIB DD data set concatenation to determine

whether the member exists, and if so, to read it. If the NFS server task is not authorized to read that concatenation, an access failure might occur during NFS server initialization.

Element or feature:	NFS.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you plan to use the z/OS NFS server.
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: Before initializing the z/OS NFS server, authorize the NFS server task to read the PARMLIB DD data set concatenation.

Reference information: For details about using component trace for the z/OS NFS server, see the Diagnosis chapter in *z/OS Network File System Guide and Reference*.

Chapter 22. OSA/SF migration actions

This chapter describes migration actions for base element Open Systems Adapter/Support Facility (OSA/SF).

Some OSA/SF data sets have been removed from z/OS. See "Remove references to deleted data sets and paths" on page 40. Some OSA/SF data sets have been added to z/OS. See "Add references to new data sets and paths" on page 53.

OSA/SF actions to perform before installing z/OS V1R7

None.

OSA/SF actions to perform before the first IPL of z/OS V1R7

This section describes OSA/SF migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

Migrate to the Java-based OSA/SF GUI

Description: Effective with the z/OS V1R4 z990 Compatibility Support feature (and in the z990 Compatibility for Selected Releases Web deliverable), OSA/SF has changed the graphical user interface (GUI). It is now a Java application. The earlier versions of the OSA/SF GUI cannot share files with the Java-based OSA/SF GUI, and any configuration that you have created with earlier versions of the OSA/SF GUI are not accessible to the Java-based OSA/SF GUI.

Element or feature:	OSA/SF.
When change was introduced:	z/OS V1R4 with the z/OS V1R4 z990 Compatibility Support feature (and the z990 Compatibility for Selected Releases Web deliverable on earlier releases).
Applies to migration from:	z/OS V1R4 without the z/OS V1R4 z990 Compatibility Support feature or z/OS V1R4 z990 Exploitation Support feature.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you are using the OSA/SF GUI.
Target system hardware requirements:	None.
Target system software requirements:	Java 1.1.2 help files and Java 1.4 run-time library loaded on the workstation.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Steps to take:

1. Set up the Java environment and the OSA/SF GUI on the workstation on which you wish to use the GUI. For details about installing Java and GUI files, see *zSeries OSA-Express Customer's Guide and Reference*.

2. To read and save a configuration for a currently installed OSA, perform the following steps from the Java-based GUI:

    a. Start the GUI and from **CHPID View** open a configuration window for the CHPID whose data you want to save.

    b. From the menu bar, select **File > Get current configuration**. The configuration data for the OSA is loaded into the configuration window.

    c. Give the OSA configuration a name. From the menu bar, select **Save configuration**. The OSA configuration data is saved to the host list.

Reference information: *zSeries OSA-Express Customer's Guide and Reference*.

Use the new message log name

Description: The name of the OSA/SF message log has changed. Formerly, the name was IOADSN.LP*xx*, where *xx* was the image on which OSA/SF was running. Now, the name is IOADSN.I*xy,* where *x* is the logical channel subsystem and *y* is the image number on which OSA/SF is running. You should update any diagnostic procedures that use this name.

Element or feature:	OSA/SF.
When change was introduced:	z/OS V1R4 with the z/OS V1R4 z990 Compatibility Support feature (and the z990 Compatibility for Selected Releases Web deliverable on earlier releases).
Applies to migration from:	z/OS V1R4 without the z/OS V1R4 z990 Compatibility Support feature or z/OS V1R4 z990 Exploitation Support feature.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if this change impacts diagnostic procedures.
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: Update local procedures related to this change. The recommended way to look at the OSA/SF message log is to use the GET DEBUG command with the MESSAGE LOG parameter, which allows you to retrieve information without having to know a data set name.

Reference information: *zSeries OSA-Express Customer's Guide and Reference*.

OSA/SF actions to perform after the first IPL of z/OS V1R7

None.

Chapter 23. RMF migration actions

This chapter describes migration actions for optional feature Resource Measurement Facility (RMF).

RMF actions to perform before installing z/OS V1R7

None.

RMF actions to perform before the first IPL of z/OS V1R7

This section describes RMF migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

Specify NOZFS to suppress the gathering of zFS data

Description: Before z/OS V1R7, RMF did not gather data about zFS activity. As of z/OS V1R7, RMF gathers data about zFS activity, and it does so by default. You can suppress the gathering of zFS data by specifying the new Monitor III gatherer option NOZFS.

Element or feature:	RMF.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you do not want to gather data about zFS activity.
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 suppress the gathering of data about zFS activity, specify the Monitor III gatherer option NOZFS. You can set this option using msys for Setup for RMF. However, if you want to gather data about zFS activity, simply accept the default.

Control access to RMF data

Description: Before z/OS V1R5, RMF did not perform access checks for Monitor II data and Monitor III set-of-samples data. RMF only performed access checks for SMF data in the RMF Sysplex Data Server's SMF buffers. You could enable these access checks by using either of the following methods:

- Authorizing users to the discrete RACF resource profile of class FACILITY called ERBSDS.SMFDATA
- Authorizing users to the generic RACF resource profile of class FACILITY called ERBSDS.*

As of z/OS V1R5, RMF offers optional access checks for Monitor II data and Monitor III set-of-samples data, using profiles ERBSDS.MON3DATA and ERBSDS.MON2DATA.

Element or feature:	RMF.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if all of the following are true: (1) you are currently using generic profile ERBSDS.*, (2) you have generic profile checking active, and (3) you do not want to protect Monitor II and Monitor III data.
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:

- If you do not want to protect Monitor II data and Monitor III set-of-samples data (that is, if you want z/OS V1R7 to work like z/OS V1R4), consider these two cases:
  - If, in z/OS V1R4, users used discrete profile ERBSDS.SMFDATA, no migration steps are necessary.
  - If, in z/OS V1R4, users used generic profile ERBSDS.* and generic profile checking was active, change the generic profile ERBSDS.* to the discrete profile ERBSDS.SMFDATA.
- If you now want to exploit the new function (that is, you want to protect Monitor II data and Monitor III set-of-samples data), consider these two cases:
  - If the same group of users will access Monitor II data and Monitor III set-of-samples data (newly protected) as well as SMF data in the RMF Sysplex Data Server's SMF buffers (already protected in z/OS V1R4), then the easiest method is to work with the generic profile ERBSDS.* with generic profile checking active. Authorize all users of the group to this profile. Nothing else needs to be done because the generic profile protects all data.

– If different users will access Monitor II data and Monitor III set-of-samples data (newly protected) as well as SMF data in the RMF Sysplex Data Server's SMF buffers (already protected in z/OS V1R4):

- If, in z/OS V1R4, users used generic profile ERBSDS.* and generic profile checking was active, you might need to authorize additional user IDs to now protect Monitor II and Monitor III data.
- If, in z/OS V1R4, users used discrete profile ERBSDS.SMFDATA, users who want to access Monitor II and Monitor III data now need to be authorized to profiles ERBSDS.MON3DATA and ERBSDS.MON2DATA.

Reference information: For more details, see *z/OS RMF User's Guide*.

RMF actions to perform after the first IPL of z/OS V1R7

This section describes RMF migration actions that you can perform only after you've IPLed z/OS V1R7. You need a running z/OS V1R7 system to perform these actions.

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 V1R7 for data collected with an RMF gatherer from z/OS V1R4, 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.

Element or feature:	RMF.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you had planned to use a back-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" below.
Restrictions:	None.
System impacts:	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.

Reference information: *z/OS RMF User's Guide.*

Migrate Working Sets to the new Spreadsheet Reporter format

Description: With z/OS V1R5 RMF, a new version of the Spreadsheet Reporter is implemented in Java. You can migrate Working Sets produced with previous Spreadsheet Reporter versions using batch procedures that are delivered with the new RMF Spreadsheet Reporter.

Element or feature:	RMF.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you want to process Working Sets produced with previous Spreadsheet Reporter versions.
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 migrate Working Sets from earlier releases, the Spreadsheet Reporter provides the following procedures that you invoke from a command line:

- **MigrateOvwWorkSet.bat:** to migrate an existing Working Set created from Overview records
- **MigrateReportWorkSet.bat:** to migrate an existing Working Set created from a Report Listing

Both procedures have the same invocation interface. You must provide the following parameters:

- `wsdir:` existing Working Set directory
- `wsname:` new Working Set name

For example, to migrate a Working Set created from a report listing in directory d:\Rmfpp\r051203a and to make it known to the new Spreadsheet Reporter under the name of "My New Working Set", you invoke the procedure as follows:

```
MigrateReportWorkSet d:\Rmfpp\r051203a "My New Working Set"
```

Reference information: For more details, see:

- *z/OS RMF User's Guide*
- The RMF Spreadsheet Reporter online help

Remove WKLD suboptions for Monitor I gathering

Description: Starting with z/OS V1R3, WLM supports goal mode only and no longer supports compatibility mode. In RMF, the WKLD option with all its suboptions

(PERIOD, GROUP, and so on) controlled real time reporting with Monitor I in WLM compatibility mode. So starting with z/OS V1R5 RMF, there is only the option WKLD or NOWKLD to specify whether the system workload is to be measured. All suboptions are ignored.

Element or feature:	RMF.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended so that you can avoid receiving message ERB325I, which tells you that you have old WKLD gatherer suboptions.
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: Remove suboptions from Monitor I option WKLD so that you don't receive message ERB325I, which tells you that you have old WKLD gatherer suboptions. WKLD can be in the parm field of the START command that starts the Monitor I session, the PARM field of the EXEC statement in the RMF cataloged procedure, or in RMF Monitor I parmlib member ERBRMF00.

If you want to measure the system workload, you can still do so; just specify WKLD without any suboptions. For example, in RMF Monitor I parmlib member ERBRMF00 you would specify:

```
WKLD                     /* WORKLOAD MANAGER DATA                   */
```

Reference information: For more details, see *z/OS RMF User's Guide*.

Chapter 24. SDSF migration actions

This chapter describes migration actions for optional feature SDSF.

Some data sets have been added to SDSF. See "Add references to new data sets and paths" on page 53.

SDSF actions to perform before installing z/OS V1R7

None.

SDSF actions to perform before the first IPL of z/OS V1R7

This section describes SDSF migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

Reassemble user exit routines

Description: If you have written user exit routines, review them to ensure they are still appropriate for the current environment. All user exit routines must be reassembled with the z/OS V1R7 level of the SDSF macro library.

Element or feature:	SDSF.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

Steps to take: Reassemble user exit routines with the z/OS V1R7 level of the SDSF macro library.

Reference information: *z/OS SDSF Operation and Customization.*

Reassemble customized ISFPARMS

Description: If you have customized ISFPARMS and it is in assembler macro format, you must reassemble it to use it with z/OS V1R7.

Element or feature:	SDSF.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you want to use a customized ISFPARMS that is in assembler macro format rather than the dynamic statement format. Converting your ISFPARMS to the dynamic statement format allows you to avoid this migration action in the future.
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: Before reassembling ISFPARMS, you might want to update it for new function.

Notes:

1. If you convert your ISFPARMS to the dynamic statement format, you will no longer need to reassemble ISFPARMS when you make changes.
2. If you have the JESDATA and NSPBUF keywords in your ISFPARMS, you may remove them. They are syntax-checked but ignored beginning with z/OS V1R7.

Reference information: *z/OS SDSF Operation and Customization*.

SDSF actions to perform after the first IPL of z/OS V1R7

This section describes SDSF migration actions that you can perform only after you've IPLed z/OS V1R7. You need a running z/OS V1R7 system to perform these actions.

Update discrete profiles that protect ENC and PS panels

Description: The SAF resources that protect the ENC and PS commands have been changed to be consistent with similar resources. A system value has been added as the last qualifier. With this change, the resources are:

- ISFCMD.ODSP.ENCLAVE.system
- ISFCMD.ODSP.PROCESS.system

These resources are in the SDSF class.

Element or feature:	SDSF.
When change was introduced:	z/OS V1R7.

Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if the ENC and PS commands are protected with discrete profiles. If the commands are protected with generic profiles (for example, ISFCMD.ODSP.**), no action is necessary.
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:

1. Define new profiles that include a value for the final qualifier, for example ISFCMD.ODSP.ENCLAVE.*, with the RACF RDEFINE command.

2. Copy the access lists from the original profiles to the new profiles with the RACF PERMIT command. If the RACF data set is not shared with any lower-level systems, you might want to delete the original profiles with the RACF RDELETE command.

Reference information:

- For details about the resources in the SDSF class, see *z/OS SDSF Operation and Customization*.

- For details about the RACF commands, see *z/OS Security Server RACF Command Language Reference*.

Implement an exit routine if you want to allow sharing a console across address spaces

Description: SDSF has changed the conditions under which you can share a console, that is, use an already active EMCS console rather than activating a new one. SDSF uses a console to issue system commands. When a console is shared, SDSF issues commands using the console ID of the shared console. However, responses to the commands are visible only in the SDSF session that activated the console.

Before z/OS V1R7, SDSF allowed you to share a console that had been activated with the same name. With z/OS V1R7, SDSF allows you to share a console only if the console was activated by SDSF in your address space, for example, when you split the screen with ISPF. You can use the SDSF initialization exit routine to restore the pre-z/OS V1R7 behavior for console sharing.

Element or feature:	SDSF.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you want to allow a console to be shared across users and address spaces.

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: Use the SDSF initialization exit routine to restore the pre-z/OS V1R7 behavior for console sharing. Implement the initialization exit point in ISFUSER. In the exit routine, turn on compatibility flag UPRSFLG5.UPRS5CSX. This flag tells SDSF that the console can be shared if activation of the console fails because the console is in use.

Reference information: For details about SDSF exit routines, see *z/OS SDSF Operation and Customization*, SA22-7670.

Chapter 25. Security Server migration actions

This chapter describes migration actions for optional feature Security Server.

As of z/OS V1R5, Security Server has a single component, RACF. Its other six components moved:

- The Cryptographic Services base element received the PKI Services component.
- The Integrated Security Services base element received the remaining five components, which are DCE Security Server, Firewall Technologies, LDAP Server, Network Authentication Service, and Open Cryptographic Enhanced Plug-ins (OCEP).

Security Server actions to perform before installing z/OS V1R7

This section describes Security Server migration actions that you can perform on your current (old) system. You don't need the z/OS V1R7 level of code to make these changes, and the changes don't require the z/OS V1R7 level of code to run once they are made.

Adjust settings because of an increase in audit records

Description: Before z/OS V1R7, the branch-entered PassTicket generation service did not generate audit records. Starting in z/OS V1R7, it does. This could result in an increase in the number of audit records created by RACF. You can use the AUDIT and GLOBALAUDIT settings on individual profiles in the PTKTDATA class, as well as the SETROPTS LOGOPTIONS setting for the PTKTDATA class, to control the generation of audit records.

Before z/OS V1R7, password changes made with RACF commands were audited based on the SETR AUDIT setting for the USER class, but those made at logon were not. Starting in z/OS V1R7, RACROUTE REQUEST=VERIFY also audits password changes when SETR AUDIT(USER) is set. This causes additional audit records to be written when users change their passwords at logon or signon.

Element or feature:	Security Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	No, but recommended to avoid extra audit records.
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: Examine and update the following to ensure that the level of auditing is acceptable:

- AUDIT and GLOBALAUDIT information specified in profiles in the PTKTDATA class
- The SETR LOGOPTIONS setting for the PTKTDATA class
- The SETR AUDIT setting for the USER class

Reference information: For details about changing audit settings, see:

- *z/OS Security Server RACF Auditor's Guide*
- *z/OS Security Server RACF Callable Services*
- *z/OS Security Server RACF Macros and Interfaces*
- *z/OS Security Server RACF Security Administrator's Guide*

Add RACF profiles in the DSNR class to protect all DB2 subsystems

Description: If you use RACF to protect connections to DB2 subsystems, you must have the DSNR class active and you might have to create additional RACF profiles in the DSNR class. Otherwise, connections to some DB2 subsystems might fail.

Element or feature:	Security Server.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you use RACF to protect connections to DB2 subsystems.
Target system hardware requirements:	None.
Target system software requirements:	Any release of DB2.
Other system (coexistence or fallback) requirements:	None.
Restrictions:	None.
System impacts:	None.

Steps to take:

1. **Activate the DSNR class to activate RACF protection for DB2 connections.**

If you already have the DSNR class active, you can skip this step. To see if you have the DSNR class active, issue the SETROPTS LIST command and look for DSNR after the heading "ACTIVE CLASSES =".

If you wish to use RACF to protect connections to DB2, you must have the DSNR class active. Starting with z/OS V1R6, if the DSNR class is inactive, connections are *allowed* to all DB2 subsystems from all environments.

When the DSNR class is active, the profiles in the DSNR class determine whether a connection to a DB2 subsystem is allowed. To activate the DSNR class, issue the following RACF command:

```
SETROPTS CLASSACT(DSNR)
```

Before z/OS V1R6, if you had the DSNR class inactive, a connection to DB2 could be allowed or denied, depending on whether the DB2 subsystem was defined in the RACF router table. Starting with z/OS V1R6, the entry in the RACF router table is no longer required. If the DSNR class is inactive, connections are *allowed* to all DB2 subsystems from all environments. If the DSNR class is active, the profiles in the DSNR class determine whether the connection is allowed.

2. **Create additional RACF profiles in the DSNR class to protect all DB2 subsystems.**

   If you have the DSNR class active and you have *all* DB2 subsystems defined in the RACF router table (ICHRFR01) with an entry containing ACTION=RACF on a z/OS system before V1R6, you can skip this step.

   If your DB2 installation already uses DSNR protection to control access to some DB2 subsystems, you need to ensure there are RACF profiles in the DSNR class to control access to all DB2 subsystems. In releases before z/OS V1R6, if you did not have an entry in the RACF router table (ICHRFR01) for a subsystem, RACF authorization checking was bypassed for that subsystem; any user who tried to access that DB2 subsystem from any environment was allowed. Starting with z/OS V1R6, the router table entry is no longer required, so any user who tries to access that DB2 subsystem might or might not be allowed, depending on which RACF profiles are defined in the DSNR class. If you depended on the missing router table entry to allow access, starting with z/OS V1R6 you must create appropriate profiles in the DSNR class to allow access.

   For example, if you had no entry in the router table for subsystem DSND and have no profiles defined in the DSNR class that begin with "DSND", starting with z/OS V1R6 you might receive error messages at DB2 startup when the DSNDSPAS address space attempts to connect with DB2, such as the following:

```
IEF403I DSNDSPAS -STARTED -TIME=15.31.42
DSNX980E DSNX9STP ATTEMPT TO PERFORM CALL
ATTACH FUNCTION CONNECT 047
FAILED WITH DB2 SUBSYSTEM DSND.
RETURN CODE =00000008 REASON CODE
=00F30013
+DSNX965I DSNX9STP THE
DB2-ESTABLISHED STORED
PROCEDURES ADDRESS 048
SPACE FOR SUBSYSTEM DSND
IS STOPPING
```

   Also, a user might receive an error message when trying to connect to the DSND DB2 subsystem, such as the following:

```
DSNE102I YOU ARE NOT AUTHORIZED TO USE DB2 SUBSYSTEM DSND
```

   Note that you will not see any RACF ICH408I messages.

In this example, if you want to allow all connections to the DSND subsystem from any environment, you can create a generic profile in the DSNR class by issuing the following commands:

```
SETROPTS GENERIC(DSNR)
RDEFINE DSNR DSND.** UACC(READ)
```

If you had many subsystems with no router table entries defined before z/OS V1R6, the simplest way to ensure that all subsystems are protected by a RACF profile is to create a generic profile in the DSNR class named **. If you have other profiles in the DSNR class, but not a profile named ** or *, you can do this by issuing the following commands:

```
SETROPTS GENERIC(DSNR)
RDEFINE DSNR ** UACC(READ)
```

This allows all users to connect to all DB2 subsystems from any environment, unless another more specific RACF profile in the DSNR class disallows the access.

Reference information:

- For details about updating the RACF router table in ICHRFR01, see *z/OS Security Server RACF System Programmer's Guide*.
- For details about using RACF to control access to DB2 subsystems, see *z/OS Security Server RACF Security Administrator's Guide* and *DB2 Administration Guide.*

Change code that checks for RACROUTE return code 4/0/0

Description: In releases before z/OS V1R6, if no matching entry was found in the RACF router table for a specific class, REQSTOR, and SUBSYS keyword combination on a RACROUTE request, the result was SAF return code 4, RACF return code 0, and RACF reason code 0 (4/0/0). Starting with z/OS V1R6, an entry is no longer required in the RACF router table, so this may result in a different return code for some RACROUTE requests.

Element or feature:	Security Server.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you have applications that use any of the following RACROUTE macros: RACROUTE REQUEST=AUDIT RACROUTE REQUEST=AUTH RACROUTE REQUEST=DEFINE RACROUTE REQUEST=EXTRACT RACROUTE REQUEST=FASTAUTH RACROUTE REQUEST=LIST RACROUTE REQUEST=STAT
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: You might need to change code that uses any of the RACROUTE macros listed in "Required action" above and that expects the following return code combination:

```
SAF Return code (Register 15) = 4
RACF Return code (SAFPRRET field in ICHSAFP) = 0
RACF Reason code (SAFPRREA field in ICHSAFP) = 0
```

This return code combination of 4/0/0 can be issued for several reasons. One reason might be that a RACROUTE request specified a combination of request, resource, and subsystem (in the CLASS, REQSTOR, and SUBSYS parameters) that could not be found in the RACF router table. This means that the matching combination of CLASS=, REQSTOR=, and SUBSYS= specified on a RACROUTE request could not be located in the RACF router table. If you have code that depends on this return code combination for this reason, you might need to change your code, or you might need to provide documentation on creating RACF profiles.

You do not have to change code if either of the following cases is true:
- Your RACROUTE macros reference only IBM classes (they do not reference installation-defined classes), and either
    - Do not specify the REQSTOR= or SUBSYS= keywords, or
    - Specify REQSTOR= and SUBSYS= but use a combination of CLASS, REQSTOR, and SUBSYS shipped in RACF before z/OS V1R6.
- Your RACROUTE macros specify DECOUPL=YES and they do not specify a RELEASE= value higher than the level of the system on which the macros are running.

Reference information: For details about the RACF router table, see:
- *z/OS Security Server RACROUTE Macro Reference*
- *z/OS Security Server RACF System Programmer's Guide*

Add entries to the RACF router table if you do not want RACF called on RACROUTE requests

Description: In releases before z/OS V1R6, if no matching entry was found in the RACF router table for a specific class, REQSTOR, and SUBSYS keyword combination on a RACROUTE request, RACF was not called. Starting with z/OS V1R6, the default is changed so that RACF is called even if a matching entry is not found in the RACF router table.

If you do *not* want RACF to be called on RACROUTE requests for a specific class, REQSTOR, and SUBSYS keyword combination, you must add an entry in the RACF router table (ICHRFR01) to specify ACTION=NONE.

Element or feature:	Security Server.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you do not want RACF to be called for RACROUTE requests with a specific class, REQSTOR, and SUBSYS keyword combination.
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:

1. If you do not want RACF to be called on RACROUTE requests for a specific class, REQSTOR, and SUBSYS keyword combination, you must add an entry in the RACF router table (ICHRFR01) to specify ACTION=NONE. If you update the entries in ICHRFR01, assemble and link edit the module, then IPL your system.

   If you already have entries in ICHRFR01 that specify ACTION=NONE, no change is required to those entries.

2. Optionally, if you have entries in the RACF router table (ICHRFR01) that specify ACTION=RACF, you may remove those entries. Starting with z/OS V1R6, ACTION=RACF is the default action for the RACF router, regardless of whether an entry exists in the RACF router table for a specific class, REQSTOR, and SUBSYS keyword combination.

   If all of the entries in your installation-defined RACF router table (ICHRFR01) contain the ACTION=RACF keyword, you no longer need ICHRFR01 at all. You can remove the ICHRFR01 module from SYS1.LINKLIB (or any other APF-authorized link list library).

   If some of the entries in ICHRFR01 specify ACTION=NONE, then those entries should remain. You may remove any router table entries that specify ACTION=RACF, or you may leave them. If you update the entries in ICHRFR01, assemble and link-edit the module, then IPL your system.

Reference information:

- For details about updating the RACF router table in ICHRFR01, see *z/OS Security Server RACF System Programmer's Guide*.
- For details about the ICHRFRTB macro, and the ACTION=RACF and ACTION=NONE keywords, see *z/OS Security Server RACF Macros and Interfaces*.

Make changes for multilevel security support

Description: Multilevel security support introduced in z/OS V1R5 builds on the existing multilevel security features that enabled MVS/SP™ V3R1.3 and RACF 1.9 to previously obtain an evaluation under the Trusted Computer Systems Evaluation Criteria.

This support extends mandatory access checking to the z/OS UNIX environment and allows networking in a more secure environment. It also adds additional security features, such as limiting the ability of users to see the names of data sets and files if they do not have READ access.

Element or feature:	Security Server.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before installing z/OS V1R7.
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.

Steps to take:

1. If you have defined a security label named SYSMULTI on your system, you must delete the security label and define a new one with a different name, and update every profile that uses the SYSMULTI security label to specify its new name.

2. If you currently have the SETR MLACTIVE option active, analyze and prepare your systems to prevent migration problems. Profiles in the following classes will require security labels if MLACTIVE is set:
   > APPL
   > DSNADM
   > DSNR
   > MDSNCL
   > MDSNDB
   > MDSNJR
   > MDSNPN
   > MDSNSC
   > MDSNSG
   > MDSNSM
   > MDSNSP
   > MDSNTB
   > MDSNTS
   > MDSNUF
   > SERVAUTH
   > SERVER
   > TERMINAL

3. If you have the SECLABEL class active, the security labels assigned to SERVAUTH profiles representing IP addresses may be used in the determination of which security label you run with when you enter the system through that IP address. For other SERVAUTH profiles, a SYSNONE or SYSMULTI security label might be appropriate.

4. A number of classes are being changed to EQUALMAC classes (checked for equality rather than dominance), which could require you to change existing security labels in the profiles of these classes. The classes being changed to EQUALMAC classes are TERMINAL, MQCONN, APPL, DSNR, JESINPUT, SERVER and SERVAUTH.

Reference information: For details about multilevel security, see:
- *z/OS Planning for Multilevel Security and the Common Criteria*
- *z/OS Communications Server: IP Configuration Guide*

Security Server actions to perform before the first IPL of z/OS V1R7

This section describes Security Server migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't 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 router table and 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*.

Element or feature:	Security Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
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.

Steps to take: If you have duplicate class names, you will receive the following error messages when the system is IPLed:

- For a duplicate router table entry, RACF issues the following message and continues processing:

```
ICH527I RACF DETECTED AN ERROR IN THE INSTALLATION ROUTER TABLE,
ENTRY class_name, ERROR CODE 1
```

- For a duplicate CDT entry, 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: *z/OS Security Server RACF System Programmer's Guide*.

Review auditing options for SECLABEL profiles

Description: The SETROPTS SECLABELAUDIT option has been expanded to allow logging of all access attempts to z/OS UNIX resources that have security labels, and logging of all access attempts by user IDs that have security labels. If you have SETROPTS SECLABELAUDIT active, the number of type 80 SMF records could increase, resulting in poor performance.

Element or feature:	Security Server.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.

Is the migration action required?	Yes, if you have SETROPTS SECLABELAUDIT active.
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: Check the audit values specified for your SECLABEL profiles and adjust them appropriately to prevent excessive TYPE 80 SMF records.

Reference information: For details about the SECLABELAUDIT option of the SETROPTS command, see *z/OS Security Server RACF Command Language Reference*.

Modify POSIT values that were documented incorrectly in an IMS redbook

Description: In z/OS V1R6, four new RACF security classes were added as predefined default IBM classes for IMS V9 (5655-J38):

- IIMS — Program specification block (PSB)
- JIMS — Grouping class for PSB
- LIMS — Logical terminal (LTERM)
- MIMS — Grouping class for LTERM

These four classes are required when converting IMS/SMU security to RACF with IMS V9. z/OS V1R5 and z/OS V1R4 also support IMS V9 but they do not have these four predefined RACF security classes. However, you can add them to your installation-defined class descriptor table. (Macro ICHERCDE is used to define a new class. The procedure for adding classes to this table is described in "Adding installation-defined classes" in *z/OS Security Server RACF System Programmer's Guide*.)

If your z/OS V1R7 system will use a RACF database that was created or used by IMS V9 on a z/OS V1R5 or z/OS V1R4 system, and you added the classes IIMS, JIMS, LIMS, and MIMS to your class descriptor table on any of the earlier systems, check the POSIT values you used for the classes. The redbook *IMS Version 9 Implementation Guide* contained an error suggesting POSIT values 19 and 20 for these classes, but the values shipped with RACF in z/OS V1R6 and later are 575 and 576. If you used the values 575 and 576, no action is needed. But if you used the values 19 and 20, as documented in the redbook, the classes will not activate properly on z/OS V1R7.

Element or feature:	Security Server.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.

Is the migration action required?	Yes, if all of the following are true:
	• Your z/OS V1R7 system will use a RACF database that was created or used by IMS V9 (5655-J38) on a z/OS V1R5 or z/OS V1R4 system.
	• You added the classes IIMS, JIMS, LIMS, and MIMS to your class descriptor table on any of the z/OS V1R5 or z/OS V1R4 systems.
	• You used POSIT values 19 and 20 for these classes (as documented by the redbook *IMS Version 9 Implementation Guide*).
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: Issue a SETROPTS LIST command on the z/OS V1R5 or z/OS V1R4 system to see which options were used for the IIMS, JIMS, LIMS, and MIMS classes. Then issue a SETROPTS command on the z/OS V1R7 system to activate the classes and set the same options that you had, except that the SETROPTS RACLIST option is not allowed on z/OS V1R6 and later. It is best to change the POSIT value to be the same on all systems. This requires an all-systems IPL, but if you do not change the POSIT value, there might be some situations where changes to SETROPTS options do not take effect on systems using a different POSIT value, and you will need to reissue the command from the system where it did not take effect. Note that use of POSIT values 575 and 576 for these classes gives a warning MNOTE about specifying a nonrecommended POSIT value, which you can safely ignore.

Reference information: For more information about changing POSIT values, see *z/OS Security Server RACF System Programmer's Guide* and *z/OS Security Server RACF Security Administrator's Guide*.

Enforce PASSCHK=NO on RACROUTE

Description: RACF supports the use of the *BYPASS* user ID to create accessor environment elements (ACEEs) for functions that require an ACEE, such as RACROUTE REQUEST=EXTRACT. When user ID *BYPASS* is passed to RACROUTE REQUEST=VERIFY or REQUEST=VERIFYX, no password is needed. With z/OS V1R5, the PASSCHK=NO parameter must also be specified to indicate this. If PASSCHK=NO is not specified, the request will fail with existing abend codes: ABEND283 for REQUEST=VERIFY and ABEND9C7 for REQUEST=VERIFYX.

Element or feature:	Security Server.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.

Is the migration action required?	Yes, if you have written applications that use RACROUTE REQUEST=VERIFY or VERIFYX.
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: If you have written applications that use RACROUTE REQUEST=VERIFY or VERIFYX, check the applications to see whether they use *BYPASS*. If they do, be sure to specify PASSCHK=NO.

Reference information: *z/OS Security Server RACROUTE Macro Reference*.

Security Server actions to perform after the first IPL of z/OS V1R7

This section describes Security Server migration actions that you can perform only after you've IPLed z/OS V1R7. You need a running z/OS V1R7 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.

Element or feature:	Security Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
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.

Steps to take: To install the database template updates, run the IRRMIN00 utility with PARM=UPDATE.

Reference information:
- *z/OS Program Directory*
- *ServerPac: Installing Your Order*
- *z/OS Security Server RACF System Programmer's Guide*

Run dynamic parse

Description: When new keywords are added to RACF commands, the dynamic parse table (IRRDPSDS) is also updated. After IPLing your system to use the updated RACF database, you should also issue the IRRDPI00 command to start dynamic parsing and to start using the updated parse table.

Element or feature:	Security Server.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
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.

Steps to take: Issue the IRRDPI00 command to start dynamic parsing and to start using the updated parse table.

Reference information: *z/OS Security Server RACF System Programmer's Guide*.

Update programs and procedures that use ALTUSER, LISTUSER, or LISTGRP

Description: Before z/OS V1R7, a newly created RACF user ID would not be revoked for inactivity if the user ID was never used. As of z/OS V1R7, when a new user is created, the LJDATE field is set to the creation date, allowing new users to be revoked because of inactivity. When a user is revoked, revoke and resume dates are no longer cleared from the user profile as they were in prior releases. New NOREVOKE and NORESUME keywords on the ALTUSER command are provided to clear the dates. Revoke and resume dates are shown in LISTUSER and LISTGRP output even if they are in the past, and LISTGRP shows the date the group was created. Programs that examine the LJDATE field or LISTUSER or LISTGRP output might need to be changed, and procedures updated.

Element or feature:	Security Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have programs or procedures that depend on what has changed.
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:
- Check programs that examine the LJDATE field in the user profile, or at the LISTUSER or LISTGRP output (including programs that use R_admin to retrieve the information), to see if they are impacted by the change to the date fields.
- Update procedures for resuming users who are revoked by date. Users who are resumed with ALTUSER RESUME will be revoked again if they try to log on.

Reference information: For details about updating programs that use LISTUSER or LISTGRP, see:
- *z/OS Security Server RACF Command Language Reference*
- *z/OS Security Server RACF Security Administrator's Guide*

Update automation that uses RVARY

Description: Before z/OS V1R7, a device error on the DASD unit where the primary RACF data set resides resulted in a flood of RACF error messages indicating an I/O error. To resume normal RACF activity, an RVARY command had to be issued to switch to the backup RACF data set. As of z/OS V1R7, an automatic RVARY switch occurs if there is an active unboxed backup RACF data set and the RACF manager detects that the DASD unit where the primary RACF data set resides is boxed. Boxing can occur when hardware detects an error or when the RVARY command is issued. Also, the output of RVARY LIST has changed; information has been added, and headings and spacing have been changed. You might need to modify procedures and automation to accommodate these changes.

Note: The RVARY SWITCH command is still the recommended way to switch RACF primaries and backups.

Element or feature:	Security Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended to avoid having an extra RVARY issued, which could be confusing but wouldn't cause system problems.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence) requirements:	None.
Restrictions:	None.
System impacts:	None.

Steps to take:
- Change recovery processes, including automation, to note that if the hardware boxes the DASD on which a primary RACF data set resides, a fully automated RVARY SWITCH will have already occurred.

- Check any automation that relies on the RVARY LIST output to ensure that it is compatible with the new format, and correct as needed.

Reference information: For details about using the RVARY command, see:
- *z/OS Security Server RACF System Programmer's Guide*
- *z/OS Security Server RACF Command Language Reference*

Rename sample fields

Description: In z/OS V1R7, two Enterprise Identity Mapping (EIM) fields in the SMF DB2 samples have been renamed. Field SETR_UTK_REMOVE has been renamed SETR_UTK_REMOTE, and field RVAR_UTK_REMOVE has been renamed RVAR_UTK_REMOTE.

Element or feature:	Security Server.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you intend to use the IRRADUTB and IRRADULD samples supplied by IBM.
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: Rename the fields in your copy of the IRRADUTB and IRRADULD samples, as stated in the "Description" above. This might require you to make a similar change to field names in your DB2 database.

Reference information: For details about renaming EIM sample fields, see *z/OS Integrated Security Services EIM Guide and Reference*.

Update applications that scan the RACF class descriptor table

Description: In releases before z/OS V1R6, you could use the RCVTCDTP pointer in the RCVT data area when scanning the RACF class descriptor table (CDT) for the purpose of finding all RACF classes. Starting with z/OS V1R6, dynamic classes cannot be found using the RCVTCDTP pointer. You have to use the RACROUTE REQUEST=STAT macro instead of the RCVTCDTP pointer.

Element or feature:	Security Server.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have an application that uses the RCVTCDTP pointer in the RCVT data area to scan the RACF CDT.
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: Examine any applications that scan all classes in the RACF CDT. Look for the use of the RCVTCDTP pointer in the RCVT data area. If you find any such uses, update your applications to use the RACROUTE REQUEST=STAT macro instead of the RCVTCDTP pointer. You can use the NEXT= keyword on the RACROUTE REQUEST=STAT macro to scan all classes in the RACF CDT, including dynamic classes.

Reference information:
- For details about RACROUTE REQUEST=STAT, see *z/OS Security Server RACROUTE Macro Reference*.
- For details about using dynamic RACF classes, see *z/OS Security Server RACF Security Administrator's Guide*.

Chapter 26. SMP/E migration actions

This chapter describes migration actions for base element SMP/E.

Note: SMP/E is a driving system element and, as such, is fully usable from your driving system by accessing the installed SMP/E target libraries before an IPL. For this reason, SMP/E migration actions are presented in two categories rather than the three categories used in the rest of this document. The two categories are:

- SMP/E actions to perform after installing SMP/E V3R4 (z/OS V1R7 SMP/E) but before starting to use it
- SMP/E actions to perform after starting to use SMP/E V3R4 (z/OS V1R7 SMP/E)

SMP/E actions to perform after installing SMP/E V3R4 (z/OS V1R7 SMP/E) but before starting to use it

This section describes SMP/E migration actions that you can perform after installing SMP/E V3R4 (which is in z/OS V1R7) but before you start to use it.

Modify firewall commands for the FTP client

Description: In SMP/E V3R3 (which is in z/OS V1R6), the RECEIVE FROMNETWORK command was enhanced to use the Communications Server FTP client. Because of the way in which the FTP client and local firewalls prompt for a user ID and password, this enhancement requires changes to the <FIRECMD> tags used to navigate through a local firewall. The <FIRECMD> tags are specified in the CLIENT data set for the RECEIVE FROMNETWORK command and the SMPCLNT data set for the new GIMGTPKG service routine

Element or feature:	SMP/E.
When change was introduced:	SMP/E V3R3 (which is in z/OS V1R6).
Applies to migration from:	SMP/E V3R2 (which is in z/OS V1R5) and SMP/E V3R1 (which is in z/OS V1R4).
Timing:	After installing SMP/E V3R4 (which is in z/OS V1R7) but before starting to use it.
Is the migration action required?	Yes, if you use the SMP/E RECEIVE FROMNETWORK command and specify client firewall commands.
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: Before SMP/E V3R3 (which is in z/OS V1R6), you might have specified the following <FIRECMD> tags:

```
<FIRECMD> USER &USER; </FIRECMD>
<FIRECMD> PASS &PW; </FIRECMD>
```

Starting with SMP/E V3R3, if your local firewall or the FTP client prompts for a user ID, do not specify the USER subcommand on the <FIRECMD> tag. Specify only the user ID or the appropriate substitution variable on the <FIRECMD> tag, as follows:

```
<FIRECMD> &USER; </FIRECMD>>
```

If your local firewall or the FTP client prompts for a password, do not specify the PASS subcommand on the <FIRECMD> tag. Specify only the password or the appropriate substitution variable on the <FIRECMD> tag, as follows:

```
<FIRECMD> &PW; </FIRECMD>>
```

With SMP/E V3R3, you might need to add two additional <FIRECMD> tags if, once connected to your local firewall, you are not yet connected to the remote server. To connect to the remote server, add the following <FIRECMD> tags:

```
<FIRECMD> &USER &REMOTE_USER; </FIRECMD>>
```

The commands you specify in the <FIRECMD> tags should be the same as those you use with the Communications Server FTP client. Because the behavior of various firewalls differs, the best way to determine the necessary <FIRECMD> tags is to perform an FTP operation using the FTP client in a job and then specify the same commands that were needed in that operation in the <FIRECMD> tags in the CLIENT or SMPCLNT data set (or both). For example:

```
//job JOB job parameters...
//FTP EXEC PGM=FTP
//OUTPUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//INPUT DD *
firewall_host
firewall_userid
SITE remote_host
; USER remote_userid
; remote_password
DIR
QUIT
```

Reference information: *SMP/E Reference*.

Migrate from CLIENT to FTP.DATA for local site parameters

Description: SMP/E now uses the FTP.DATA configuration data set to allow the client to specify local site parameters. Two of the parameters specified in the FTP.DATA data set are FWFriendly and FTPKEEPALIVE. These parameters correspond to the pasv and keepalive attributes in the CLIENT data set. Therefore, no longer specify the pasv and keepalive attributes in the CLIENT data set. Rather, specify the FWFriendly and FTPKEEPALIVE parameters in the FTP.DATA data set.

Element or feature:	SMP/E.

When change was introduced:	SMP/E V3R3 (which is in z/OS V1R6).
Applies to migration from:	SMP/E V3R2 (which is in z/OS V1R5) and SMP/E V3R1 (which is in z/OS V1R4).
Timing:	After installing SMP/E V3R4 (which is in z/OS V1R7) but before starting to use it.
Is the migration action required?	Yes, if you use the pasv and keepalive attributes in the CLIENT data set.
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: Remove any pasv and keepalive attributes from the CLIENT data set. Replace them with FWFriendly and FTPKEEPALIVE parameters in the FTP.DATA data set.

Any pasv and keepalive attributes that remain in the CLIENT data set are ignored. However, removing them now can help avoid confusion in the future by anyone who encounters them and is unaware that they are no longer functional.

Reference information: For more information about the statements that can be coded in the FTP.DATA data set, see *z/OS Communications Server: IP User's Guide and Commands*.

Specify which utility programs SMP/E can call

Description: In prior SMP/E releases, you had to modify module GIMUTTBL to specify which utility programs SMP/E was allowed to call. Module GIMUTTBL and load module GIMUTTBL are no longer supplied as part of SMP/E. Macro GIMDFUT, which was used to replace the IBM-supplied copy of GIMUTTBL, is also no longer supplied.

Element or feature:	SMP/E.
When change was introduced:	SMP/E V3R2 (which is in z/OS V1R5).
Applies to migration from:	SMP/E V3R1 (which is in z/OS V1R4).
Timing:	After installing SMP/E V3R4 (which is in z/OS V1R7) but before starting to use it.
Is the migration action required?	Yes, if you have modified module GIMUTTBL and want to retain the options specified there.
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: You can specify which utility programs SMP/E can call by using z/OS Security Server (RACF) to create a profile for the utility program in the PROGRAM general resource class.

Reference information: For information about using z/OS Security Server, refer to *z/OS Security Server RACF Security Administrator's Guide*.

Specify SMP/E dialog customization options

Description: A new option, Option 0, has been added to the SMP/E Primary Option Menu GIM@PRIM to implement the current SMP/E customization options. This new option allows you to enter or change the values for the customization options that were previously found in panel GIM@UPRM. When you select option 0 from the GIM@PRIM panel, the panel GIM@PARM will appear. The options you then specify are saved permanently in the ISPF profile pool for later use by other SMP/E dialog processes.

Element or feature:	SMP/E.
When change was introduced:	SMP/E V3R2 (which is in z/OS V1R5).
Applies to migration from:	SMP/E V3R1 (which is in z/OS V1R4).
Timing:	After installing SMP/E V3R4 (which is in z/OS V1R7) but before starting to use it.
Is the migration action required?	Yes, if you have modified panel GIM@UPRM and want to keep the options specified there.
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: Use the new Option 0 on the SMP/E Primary Option Menu GIM@PRIM to specify the desired SMP/E dialog customization options. The options you specify will be saved.

Reference information: For more information about SMP/E dialog customization, refer to the tutorial panels that accompany the SMP/E dialogs.

Use the LINK LMODS command instead of REPORT CALLLIBS

Description: The REPORT CALLLIBS command has been removed from SMP/E V3R2. It has been replaced by the LINK LMODS command.

Element or feature:	SMP/E.
When change was introduced:	SMP/E V3R2 (which is in z/OS V1R5).
Applies to migration from:	SMP/E V3R1 (which is in z/OS V1R4).
Timing:	After installing SMP/E V3R4 (which is in z/OS V1R7) but before starting to use it.
Is the migration action required?	Yes, if you have system programming procedures or jobs that use the REPORT CALLLIBS command.
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: Use the LINK LMODS command instead of REPORT CALLLIBS.

Reference information: information about using the LINK LMODS command, refer to *SMP/E Commands.*

SMP/E actions to perform after starting to use SMP/E V3R4 (z/OS V1R7 SMP/E)

This section describes SMP/E migration actions that you can perform after you've started to use SMP/E V3R4 (which is in z/OS V1R7).

Upgrade SMP/E zones

Description: New releases of SMP/E must sometimes make changes to SMP/E data sets that cannot be properly processed by prior SMP/E releases. SMP/E usually makes incompatible changes only when necessary to provide new and improved capabilities. For example, a new type of SMP/E element would require a new entry type in SMPCSI data sets, and new entry types are typically not understood or processed correctly by SMP/E levels that have not been specifically updated to do so.

The UPGRADE command allows you to specify when SMP/E is permitted to make incompatible changes to SMP/E data sets. This, in turn, allows you to make the trade-off between exploiting new SMP/E functions and preserving compatibility with prior SMP/E releases.

Element or feature:	SMP/E.
When change was introduced:	SMP/E V3R3 (which is in z/OS V1R6) and SMP/E V3R2 (which is in z/OS V1R5).
Applies to migration from:	SMP/E V3R2 (which is in z/OS V1R5) and SMP/E V3R1 (which is in z/OS V1R4).
Timing:	After starting to use SMP/E V3R4 (which is in z/OS V1R7).
Is the migration action required?	Yes, if you wish to use new SMP/E functions that make incompatible changes to SMP/E zones.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	Any SMP/E zone updated by the UPGRADE command can no longer be maintained by prior SMP/E releases. Also, SMP/E coexistence PTFs are required; see "Install coexistence and fallback PTFs" on page 4.
Restrictions:	None.
System impacts:	None.

Steps to take: Once you have decided that you will no longer maintain a particular SMP/E zone with SMP/E releases before SMP/E V3R2, run the UPGRADE command for that zone. This enables you to exploit all the new functions of the latest SMP/E for that zone. But remember, once you run UPGRADE for a zone using a particular release level of SMP/E, you must continue to use that release level to process that zone.

Reference information: For information about using the UPGRADE command, see *SMP/E Commands*.

Chapter 27. TSO/E migration actions

This chapter describes migration actions for base element Time Sharing Option/Extensions (TSO/E).

TSO/E actions to perform before installing z/OS V1R7

None.

TSO/E actions to perform before the first IPL of z/OS V1R7

This section describes TSO/E migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

Review your specification of the maximum number of REXX environments

Description: The maximum number of concurrent REXX environments that the system can initialize in an address space is defined in an environment table called IRXANCHR. To change the number of environment table entries, you must create a new IRXANCHR load module. TSO/E provides a SYS1.SAMPLIB member called IRXTSMPE, which is an SMP/E usermod, to change the maximum number of language processor environments in an address space.

Before z/OS V1R6, the default number of environments specified in IRXANCHR was 40. As of z/OS V1R6, the default number of environments is 401.

Element or feature:	TSO/E.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have a usermod that changes the number of environments in IRXANCHR and the new value of 401 is acceptable 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.

Steps to take: Review the number of environments you have specified for IRXANCHR in your usermod. If the default value of 401 is acceptable to you, then you may eliminate this usermod. If the default value of 401 is not acceptable, then you must continue to use the usermod to specify your desired IRXANCHR value.

Reference information: For information about changing the maximum number of REXX environments, see *z/OS TSO/E REXX Reference*.

Accommodate TEST output command changes for subcommands LIST I and LISTPSW

Description: As of z/OS V1R6, the TSO/E TEST command supports 64-bit (z/Architecture) programs that do not exploit 64-bit addressing mode and programs that contain IEEE floating-point instructions. As a result, the output from the TEST command when using subcommands LIST I and LISTPSW has changed.

Element or feature:	TSO/E.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have a dependency on the output of the LIST I or LISTPSW subcommand of the TEST command.
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: Change any dependency you have on the output of TEST LIST I or TEST LISTPSW. The output has changed as follows:

- TEST LIST I subcommand output is in a more readable format. General purpose registers are now designated by "R*n*" instead of just "*n*". Index register 0 is no longer displayed when it is in the index register position of an instruction. This is an example of TEST LIST I output:

Old format	New format
| ```
TEST
list +38 length(50) i
        +38    SLL    15,8(0)
        +3C    ICM    15,13,52(12)
        +40    SR     1,1
        +42    SVC    120
        +44    LR     11,1
        +46    ST     13,4(0,11)
        +4A    ST     11,8(0,13)
        +4E    LM     15,1,16(13)
        +52    LR     13,11
        +54    L      2,20(0,1)
        +58    L      3,0(0,2)
        +5C    LTR    3,3
        +5E    BC     8,112(0,12)
        +62    L      3,8(0,2)
        +66    LA     0,2(0,0)
TEST
``` | ```
TEST
list +38 length(50) i
        +38    SLL    R15,8
        +3C    ICM    R15,13,52(R12)
        +40    SR     R1,R1
        +42    SVC    120
        +44    LR     R11,R1
        +46    ST     R13,4(,R11)
        +4A    ST     R11,8(,R13)
        +4E    LM     R15,R1,16(R13)
        +52    LR     R13,R11
        +54    L      R2,20(,R1)
        +58    L      R3,0(,R2)
        +5C    LTR    R3,R3
        +5E    BC     8,112(,R12)
        +62    L      R3,8(,R2)
        +66    LA     R0,2
TEST
``` |

- The TEST LISTPSW subcommand is enhanced to display the z/Architecture program status word (PSW). If bit 12 of the PSW is off, the PSW is the z/Architecture PSW and the entire 64-bit instruction address is shown. The extended addressability (EA) bit is now displayed along with the basic addressability (BA) bit. For example, this is TEST LISTPSW output for a 31-bit (ESA/390) PSW:

```
PSW LOCATED AT 7F3B28
  XRXXXTIE   KEY  XMWP  AS CC  PROGMASK  EA BA   INSTR ADDR
  00000111    8   1101  00 01    0000     0  0   00022FF8
```

This is TEST LISTPSW output for a 64-bit (z/Architecture) PSW:

```
PSW LOCATED AT 01E0
  XRXXXTIE   KEY  XMWP  AS CC  PROGMASK  EA BA   INSTR ADDR
  00000000    0   0000  00 00    0000     0  1   00000000_074B9968
```

- New messages are associated with this new support in the TSO/E TEST command.

Reference information:
- For details about using the TEST command, see *z/OS TSO/E Command Reference*.
- For new messages associated with this change, see *z/OS TSO/E Messages*.

TSO/E actions to perform after the first IPL of z/OS V1R7

None.

Chapter 28. XL C/C++ migration actions

This chapter describes migration actions for base element Run-Time Library
Extensions and optional feature C/C++ without Debug Tool.

Note: As of z/OS V1R7, the C/C++ compiler has been rebranded to XL C/C++.
However, the name of the optional feature that contains the XL C/C++
compiler remains C/C++ without Debug Tool.

Optional feature C/C++ *with* Debug Tool is no longer included in this chapter
because it is removed from the system as of z/OS V1R5. See "Find alternatives to
removed elements and features" on page 23.

Some XL C/C++ data sets have been removed from z/OS. See "Remove references
to deleted data sets and paths" on page 40. Some XL C/C++ data sets have been
added to z/OS. See "Add references to new data sets and paths" on page 53.

XL C/C++ actions to perform before installing z/OS V1R7

This section describes XL C/C++ migration actions that you can perform on your
current (old) system. You don't need the z/OS V1R7 level of code to make these
changes, and the changes don't require the z/OS V1R7 level of code to run once
they are made.

Review the XL C/C++ Migration Guide for the Application Programmer

Description: The publication *z/OS XL C/C++ Compiler and Run-Time Migration
Guide for the Application Programmer* is written for application programmers,
whereas this publication (*z/OS Migration*) is written for system programmers.
However, in some customer locations, job scope could 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. Therefore, you ought to review the
XL C/C++ publication if you use XL C/C++.

Element or feature:	C/C++ without Debug Tool.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
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.

Steps to take: Look through *z/OS XL C/C++ Compiler and Run-Time Migration Guide for the Application Programmer* for migration information that's relevant to your installation.

Reference information: *z/OS XL C/C++ Compiler and Run-Time Migration Guide for the Application Programmer.*

Remove your dependency on the OS/390 V2R10 level of the C/C++ compilers

Description: Starting with z/OS V1R2, the OS/390 V2R10 C/C++ compiler was shipped in addition to the strategic ISO XL C/C++ compiler that is provided with the z/OS optional feature C/C++ without Debug Tool. As of z/OS V1R7, the OS/390 V2R10 C/C++ compiler is removed from the C/C++ without Debug Tool feature, leaving only the ISO C/C++ compiler.

Element or feature:	C/C++ without Debug Tool.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you are currently using the OS/390 V2R10 C/C++ compiler to compile your programs.
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: The ISO C++ Standard (also known as ISO/C++98 or ANSI/C++98) introduces new features to the C++ language. Semantics are changed, keywords are added, and new facilities are added to the Standard Library. See *z/OS XL C/C++ Compiler and Run-Time Migration Guide for the Application Programmer* for discussions about changes due to the new standard. Highlights are:
- The **for**-loop scoping rule is changed.
- Implicit **int** is no longer supported.
- The semantics of **friend** class declaration is changed.
- The semantics of the **throw** operator is changed.
- Exception handling is added to the **new** and **delete** operators.

The following keywords are added to the compiler. If your existing code uses any of these keywords as identifiers, the recommended practice is to change your code. If that is not possible or not practical, use the NOKEYWORD(*keyword*) option to disable the individual keyword.

- bool
- explicit
- export
- false
- mutable
- namespace
- true
- typename
- using

Use the LANGLVL option, which controls the language level of the compilers, to help in your migration:

- LANGLVL(COMPAT92). This option group instructs the z/OS XL C/C++ compiler to follow the OS/390 V2R10 compiler's semantics whenever possible. Use this as a tactical transition if your code compiles with OS/390 V2R10 and you want to move quickly to the new compiler with minimal immediate changes.
- LANGLVL(STRICT98) or LANGLVL(ANSI). These two are identical; they instruct the z/OS XL C/C++ compiler to follow the ISO/C++98 standard.
- LANGLVL(EXTENDED). This is the extended language level; it includes all IBM extensions on top of ISO/C++98.

Replace the following OS/390 V2R10 compiler options, which are not supported with the newer compilers:

- DECK. The replacement for the DECK functionality that routes output to DD:SYSPUNCH is OBJECT(DD:SYSPUNCH).
- GENPCH.
- HWOPTS. The replacement for HWOPTS is ARCHITECTURE.
- LANGLVL(COMPAT).
- OMVS. The replacement for OMVS is OE.
- SRCMSG.
- SYSLIB. The replacement for SYSLIB is SEARCH.
- SYSPATH. The replacement for SYSPATH is SEARCH.
- USEPCH.
- USERLIB. The replacement for USERLIB is LSEARCH.
- USERPATH. The replacement for USERPATH is LSEARCH.

Note that GENPCH and USEPCH served as a tactical initiative to reduce compile times. IBM is concentrating instead on improving compile times by building the compilers with successively higher levels of optimization from release to release, exploiting the ongoing optimization improvements made in the compilers.

Note: If you are not yet able to migrate to the ISO XL C/C++ compiler, you can copy the OS/390 V2R10 C/C++ compiler (which is not shipped with z/OS V1R7) from your old z/OS system for use on z/OS V1R7, with limitations. See informational APAR PK05324 for details.

Reference information:

- For more information about the compiler changes that were made between OS/390 V2R10 and z/OS V1R2, and about migrating from the older to the newer level, see *z/OS XL C/C++ Compiler and Run-Time Migration Guide for the Application Programmer*.

- The new language standard is described in publications from the International Standards Organization (ISO) and the American National Standards Institute (ANSI). The publications are available for purchase on the Internet at http://www.iso.ch and at http://www.ansi.org.
- For information about the compiler options, see *z/OS XL C/C++ Compiler and Run-Time Migration Guide for the Application Programmer* and *z/OS XL C/C++ User's Guide*.
- See also "Remove your dependency on the C/C++ IBM Open Class Library."

Migrate from use of the C/C++ ISPF panels

Description: Effective with z/OS V1R6, the C/C++ ISPF panels were removed from z/OS. z/OS V1R5 was the last release that included the panels. These panels were shipped with the C/C++ without Debug Tool feature and included panels for C/C++ foreground compiles, C/C++ background compiles, and help panels for these compiles.

Element or feature:	C/C++ without Debug Tool.
When change was introduced:	The removal of the C/C++ ISPF panels was announced in May 2003. z/OS V1R5 was the last release in which the panels were available.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you use the C/C++ ISPF panels.
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: Instead of using the ISPF panels, you can continue to invoke the XL C/C++ compiler by using z/OS UNIX commands, by using JCL, and under TSO/E.

Reference information: *z/OS XL C/C++ User's Guide*.

Remove your dependency on the C/C++ IBM Open Class Library

Description: As of z/OS V1R5, development with the C/C++ IBM Open Class Library is not supported. The Application Support Class and Collection Class libraries have been removed. Run-time support is provided for existing applications, but this support will be removed in a future release.

The data sets and paths that are affected are:
- The path for the header file is changed from `/usr/lpp/ioclib` to `/usr/lpp/cbclib`.
- The IBM Open Class (IOC) samples are removed from `/usr/lpp/ioclib/sample`.
- The Application Support and Collection Class Library headers are removed from `/usr/lpp/ioclib/include`.
- The Application Support and Collection Class Library static nonxplink/xplink objects are removed from CBC.SCLBCPP2.

- The Application Support and Collection Class Library static objects are removed from CBC.SCLBCPP.
- The Application Support and Collection files are removed from CBC.SCLBH.C.
- The Application Support Class Library files are removed from CBC.SCLBH.HPP.
- The Collection Class Library files are removed from CBC.SCLBH.INL.
- The Application Support and Collection Class Library side decks are removed from CBC.SCLBSID.

Element or feature:	C/C++ without Debug Tool.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you use the C/C++ IBM Open Class Library.
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: For new application development that needs C++ library support, use the C++ Standard Library, shipped with z/OS base element Language Environment, instead of the C/C++ IBM Open Class Library.

You can no longer compile and link applications that use IOC classes. This includes all the classes, templates, and facilities that are described in *IBM Open Class Library Reference* with the two exceptions noted below. Run-time support is provided for existing applications that use IOC, but this support will be removed in a future release.

The following classes are still supported for application development. The name of the base element that provides this application development support has changed from C/C++ IBM Open Class Library to Run-Time Library Extensions:
- UNIX System Laboratories (USL) I/O Stream Library
- USL Complex Mathematics Library

Although support for these two classes is not being removed at this time, it is recommended that you migrate to the Standard C++ iostream and complex classes. This is especially important if you are migrating other IOC streaming classes to Standard C++ Library streaming classes, because combining USL and Standard C++ Library streams in one application is not recommended.

Reference information:
- For more information about the USL I/O Stream Library and the USL Complex Mathematics Library, see *C/C++ Legacy Class Libraries Reference*.
- For information about migrating away from the C/C++ IBM Open Class Library, see *IBM Open Class Library Transition Guide*.

- For information about class library changes, see *z/OS XL C/C++ Compiler and Run-Time Migration Guide for the Application Programmer* and *z/OS XL C/C++ User's Guide*.

XL C/C++ actions to perform before the first IPL of z/OS V1R7

This section describes XL C/C++ migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

Accommodate the change to the euro as the default currency

Description: Before z/OS V1R6, the default currency for European Union countries was set to the local currency in the LC_MONETARY category of the locale. If you wanted to set the euro as the currency, you would set the @euro locales using setlocale().

As of z/OS V1R6, the LC_MONETARY information in the base locale is set to use the euro. If you set the base locale, the euro is now the default currency.

If you want your applications to continue using the old (local) currency, you must now issue setlocale() with the new @preeuro locale as the parameter.

Behavior of the @euro locales has not changed.

Element or feature:	C/C++ without Debug Tool.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if your applications use the default currency and need to use the local currency (that is, not the euro currency symbol).
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 set the euro as the currency, do nothing. But if you want to restore the prior situation, which is to use the local currency as the default, use the setlocale() function to do so.

Reference information: For information about customizing locale source files, see *z/OS XL C/C++ Programming Guide*.

XL C/C++ actions to perform after the first IPL of z/OS V1R7

This section describes XL C/C++ migration actions that you can perform only after you've IPLed z/OS V1R7. You need a running z/OS V1R7 system to perform these actions.

Add CEE.SCEERUN2 to user-written compiler procedures

Description: Before z/OS V1R5, the IBM-supplied procedures for invoking the C/C++ compiler specified the CEE.SCEERUN data set, which is a PDS that contains the run-time library routines needed during execution of applications written in C/C++, COBOL, PL/I, and FORTRAN. As of z/OS V1R5, CEE.SCEERUN2 was added; it is a PDSE that contains the run-time library routines needed during execution of applications written in XL C/C++ and COBOL. If, before z/OS V1R5, you wrote JCL that uses a STEPLIB DD statement to override an IBM-supplied compiler procedure, be sure to add a reference to CEE.SCEERUN2 in your JCL.

Element or feature:	C/C++ without Debug Tool.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you modified any IBM-supplied procedures that reference the CEE.SCEERUN2 data set.
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: Add a reference to CEE.SCEERUN2 wherever you have a reference to CEE.SCEERUN in user-written JCL. If you have the current z/OS level of CEE.SCEERUN, CEE.SCEERUN2, CBC.SCCNCMP, CBC.SCLBDLLL, and CBC.SCLBDLL2 in your system's link list, there is no need to have a STEPLIB DD statement specified in your XL C/C++ compiler procedures.

Reference information: For details about specifying CEE.SCEERUN and CEE.SCEERUN2 in JCL, see *z/OS XL C/C++ User's Guide*.

Chapter 29. z/OS UNIX migration actions

This chapter describes migration actions for base element z/OS UNIX System Services (z/OS UNIX).

Some z/OS UNIX data sets have been removed from z/OS. See "Remove references to deleted data sets and paths" on page 40. Some z/OS UNIX data sets have been added to z/OS. See "Add references to new data sets and paths" on page 53.

z/OS UNIX actions to perform before installing z/OS V1R7

This section describes z/OS UNIX migration actions that you can perform on your current (old) system. You don't need the z/OS V1R7 level of code to make these changes, and the changes don't require the z/OS V1R7 level of code to run once they are made.

Modify BPXPRMxx because SET OMVS=xxx now executes MOUNT, FILESYSTYPE, and NETWORK statements

Description: Before z/OS V1R7, the SET OMVS=*xx* operator command did not execute the MOUNT, FILESYSTYPE, and NETWORK statements from the BPXPRMxx parmlib member. As of z/OS V1R7, SET OMVS=*xx* executes MOUNT, FILESYSTYPE, and NETWORK statements from BPXPRM*xx*.

Element or feature:	z/OS UNIX.
When change was introduced:	z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	Yes, if you have MOUNT, FILESYSTYPE, or NETWORK statements in your BPXPRM*xx* parmlib member and you do not want these statements to be executed when the SET OMVS=*xx* operator command is issued.
Target system hardware requirements:	None.

Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	If BPXPRM*xx* is used in a sysplex, the MOUNT, FILESYSTYPE, and NETWORK statements are ignored on pre-z/OS V1R7 systems but executed on z/OS V1R7 systems.
Restrictions:	None.
System impacts:	None.

Steps to take: If you do not want SET OMVS=*xx* to execute the BPXPRM*xx* MOUNT, FILESYSTYPE, or NETWORK statements, then edit your BPXPRM*xx* parmlib member to remove these statements and copy them into another BPXPRM*xx* parmlib member. If you want to use that new BPXPRM*xx* parmlib member for your next IPL, add it to your OMVS= list in IEASYS*xx*. If you want SET OMVS=*xx* to execute the BPXPRM*xx* MOUNT, FILESYSTYPE, or NETWORK statements, then do nothing.

Reference information: For a complete description of the MOUNT, FILESYSTYPE, and NETWORK statements, see *z/OS MVS Initialization and Tuning Reference*.

Remove settings of _MAKE_BI=YES

Description: Support for the _MAKE_BI shell variable is removed. Before z/OS V1R5, when set to YES, the z/OS UNIX shell used built-in **make**, **c89**, **cc**, and **c++** commands, rather than the separate executables. The intended performance benefits for large application builds were not realized in most cases. This support is disabled in z/OS V1R5 in favor of internal changes to the compiler commands. The **make**, **c89**, **cc**, and **c++** commands are no longer built into the z/OS UNIX shell.

Element or feature:	z/OS UNIX.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before installing z/OS V1R7.
Is the migration action required?	No, but recommended to avoid confusion in the future.
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: Delete any settings of _MAKE_BI=YES. If any remain, they are ignored.

Reference information: None.

z/OS UNIX actions to perform before the first IPL of z/OS V1R7

This section describes z/OS UNIX migration actions that you can perform after you've installed z/OS V1R7 but before the first time you IPL. These actions might require the z/OS V1R7 level of code to be installed but don't require it to be active.

Update /etc configuration files

Description: Some utilities provided by z/OS UNIX 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 `/samples` directory. Before the first use of any of these utilities, you must 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/rc` file by copying the sample file from `/samples/rc` to `/etc/rc` 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.

Element or feature:	z/OS UNIX.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you have customized a configuration file (listed in Table 21) 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.

Steps to take: If you added installation-dependent customization to any of the IBM-provided configuration files listed in Table 21, 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 21. Changed z/OS UNIX configuration files

Utility	IBM-provided sample file	File to which you copy the sample	What changed and when
OHELP	/samples/ohelp.ENU	/etc/ohelp.ENU	Every release, bookshelf and book data set names are updated. See "Install books and a bookshelf for the OHELP command" on page 333.

Reference information:

- For more details about configuration files, see *z/OS UNIX System Services Planning*.

- For more information about utilities, see *z/OS UNIX System Services Command Reference*.

Use the changed cp and mv defaults for files with different source and target tags

Description: In z/OS V1R7 (and prior releases with the appropriate PTF for APAR OA10314 installed), the **cp** and **mv** commands have new default behaviors when copying or moving files with different source and target tags.

For a UNIX-to-UNIX copy or move of files to a target file system that does not support setting file tags (such as NFS):
- The previous default behaviors (in z/OS V1R6 without PTF UA17740 installed, in z/OS V1R5 without PTF UA17739 installed, and in z/OS V1R4 without PTF UA17738 installed) are:
  - Automatic conversion is disabled for both the source and target files.
  - When the target file has a different tag than the source file, the target file is tagged the same as the source file.
- The new default behaviors (in z/OS V1R7, in z/OS V1R6 with PTF UA17740 installed, in z/OS V1R5 with PTF UA17739 installed, and in z/OS V1R4 with PTF UA17738 installed) are:
  - Automatic conversion is enabled for both the source and target files.
  - Existing target tags are not changed or a new target file is created with a tag according to file system attributes. (The MOUNT parameter can specify TAG.)

For an MVS-to-UNIX copy or move of files to a target file system that does not support setting file tags (such as NFS), if the MVS source file contains text data:
- The previous default behaviors (in z/OS V1R6 without PTF UA17740 installed, in z/OS V1R5 without PTF UA17739 installed, and in z/OS V1R4 without PTF UA17738 installed) are:
  - Automatic conversion is disabled for the target file.
  - An existing tagged target file is untagged.
- The new default behaviors (in z/OS V1R7, in z/OS V1R6 with PTF UA17740 installed, in z/OS V1R5 with PTF UA17739 installed, and in z/OS V1R4 with PTF UA17738 installed) are:
  - Automatic conversion is enabled for the target file.
  - Existing target tags are not changed or a new target file is created with a tag according to file system attributes. (The MOUNT parameter can specify TAG.)

If you use the **cp** or **mv** command in any of the situations described above, the new default behaviors occur. There is no way to return to the prior default behaviors.

Element or feature:	z/OS UNIX.
When change was introduced:	z/OS V1R7 and rolled back to prior releases by APAR OA10314 (PTF UA17740 on z/OS V1R6, PTF UA17739 on z/OS V1R5, and PTF UA17738 on z/OS V1R4).
Applies to migration from:	z/OS V1R6 without PTF UA17740 installed, z/OS V1R5 without PTF UA17739 installed, and z/OS V1R4 without PTF UA17738 installed.
Timing:	Before the first IPL of z/OS V1R7.

Is the migration action required?	Yes, if you use the **cp** or **mv** command for files with different source and target tags.
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: Notify users of the **cp** and **mv** commands about the new default behaviors.

Reference information: For details about using the **cp** and **mv** commands, see *z/OS UNIX System Services Command Reference*.

Change NOAUTOMOVE to AUTOMOVE for sysplex-aware file systems

Description: Previously, you could set either NOAUTOMOVE or an automove system list (SYSLIST) for both sysplex-aware and sysplex-unaware file systems. However, they would be ignored for sysplex-aware file systems during dead system recovery. Now you cannot set NOAUTOMOVE or SYSLIST for sysplex-aware file systems. If you do, AUTOMOVE is used instead and you will get an informational message telling you of the change.

What are sysplex-aware file systems? The owner of a file system is the first system that processes the mount. This system always accesses the file system locally, that is, the system does not access the file system through a remote system. Other nonowning systems in the sysplex access the file system either locally or through the remote owning system, depending on the physical file system (PFS) and the mount mode. If a PFS allows a file system to be locally accessed on all systems in a sysplex for a particular mode, the PFS is *sysplex-aware* for that mode. If a PFS requires that a file system be accessed through the remote owning system from all other systems in a sysplex for a particular mode, then the PFS is *sysplex-unaware* for that mode.

To find out if the file system is sysplex-aware, you can use the D OMVS,F command to display each mounted file system. Those file systems for which this system is not the owner, and for which it says `Client=N`, are sysplex-aware (they are not clients and are locally-mounted to the PFS). Those file systems for which this system is not the owner, and for which it says `Client=Y`, are sysplex-unaware.

Element or feature:	z/OS UNIX.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended to avoid confusion in the future.
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: For sysplex-aware file systems, replace NOAUTOMOVE in the BPXPRM*xx* parmlib member with AUTOMOVE. Also, when mounting file systems, do not use a SYSLIST. On MOUNT statements in BPXPRM*xx*, we recommend that you use either AUTOMOVE or UNMOUNT for sysplex-aware file systems.

Reference information: For information about AUTOMOVE and automove system lists, see *z/OS UNIX System Services Planning*.

Migrate from central BRLM support

Description: Before z/OS V1R6, central byte range lock manager (BRLM) was the default and distributed BRLM was an option. Now, central BRLM is no longer supported once all systems in a sysplex are at the z/OS V1R6 or later level. Distributed BRLM is the only supported byte range locking method when all systems in a sysplex are at the z/OS V1R6 or later level. With distributed BRLM, the lock manager is initialized on every system in the sysplex.

Element or feature:	z/OS UNIX.
When change was introduced:	z/OS V1R6.
Applies to migration from:	z/OS V1R5 and z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use central BRLM support.
Target system hardware requirements:	None.
Target system software requirements:	None.
Other system (coexistence or fallback) requirements:	If you migrate to z/OS V1R7 by running mixed levels in a sysplex, you must enable distributed BRLM before IPLing the z/OS V1R7 system because a z/OS V1R7 system may attempt to activate distributed BRLM when the central BRLM server leaves the sysplex, regardless of the setting in the z/OS UNIX couple data set. The inconsistency between distributed BRLM being active and central BRLM being defined in the couple data set can cause an EC6-BadOmvsCds abend on downlevel systems. It is a notification-only abend indicating that the CDS should be updated. z/OS UNIX will still operate normally, and distributed BRLM will be active in the sysplex.
Restrictions:	None.
System impacts:	None.

Steps to take: If you are already running with a z/OS UNIX couple data set that enables distributed BRLM, there is no change required to activate distributed BRLM for z/OS V1R7. Likewise, if your sysplex only has systems at the z/OS V1R7 level, there is no change required because distributed BRLM is the default. z/OS V1R7 systems ignore the DISTBRLM setting in the couple data set.

If you run the IXCL1DSU utility to create a z/OS UNIX couple data set, distributed BRLM is set up as the default.

To enable distributed BRLM if you are running mixed levels in a sysplex, follow these steps before bringing the first z/OS V1R7 system into the sysplex:

1. Use the IXCL1DSU utility to update the BPXCMDS data set.
   - DISTBRLM NUMBER(0) is no longer supported; NUMBER(1) is the default
   - DISTBRLM NUMBER is ignored in a sysplex that consists of all z/OS V1R7 systems; NUMBER(1) is recommended if you are running mixed levels in a sysplex.

   Example:

   ```
   DEFINEDS SYSPLEX(PLEX1) ...
                DATA TYPE(BPXMCDS)
                     ITEM NAME(DISTBRLM) NUMBER(1)  /*default */
   ```

2. Activate the BPXCMDS data set.

Reference information:

- For details about distributed BRLM, see *z/OS UNIX System Services Planning*.
- For more information about the IXCL1DSU utility and the BPXCMDS data set, see *z/OS MVS Setting Up a Sysplex*.

Choose an appropriate GID value for the TFS root directory

Description: Previously, when a GID for the root of a temporary file system (TFS) was assigned, its value was that of the default group for the user ID under which the TFS was running. Now, the GID for a TFS root directory is the value of what you specify when you mount the TFS; if you do not specify a value, the default of 0 is used.

Element or feature:	z/OS UNIX.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use TFS but the following are not appropriate for your environment: a GID of 0, permissions of 0777, and a 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.

Steps to take: On the mount, set the GID for the TFS root. Mount users must have UID(0) or at least READ access to the BPX.SUPERUSER resource in the FACILITY class. If the only privilege the user needs is the ability to mount, then you should define the profile SUPERUSER.FILESYS.MOUNT in the UNIXPRIV class and give that user at least READ authority.

Example: To set the GID to 1 for the TFS root:

```
MOUNT FILESYSTEM('/tmp')                    /* TFS for /tmp directory              */
      MOUNTPOINT('/tmp')
      TYPE(TFS)                             /* Filesystem type TFS                 */
      MODE(RDWR)                            /* Mounted for read/write              */
      PARM('-g 1 -p 1777 -u 999 -s 20') /* change the GID from 0 (default) to 1
                                             change permissions from 0777 (default)
                                             to 1777, which sets the sticky bit.   */
                                             change UID from 0 (default) to 999
                                             set size to 20 MB                     */
```

Notes:

1. Global access is allowed by default.

2. If you do not specify a size on a TFS mount, the default of 1 MB is used.

Guideline: Set the sticky bit on for /tmp and other public directories. If the sticky bit is on, only the owner of a file (or superuser) can remove files in that directory. On a public directory such as /tmp, if the sticky bit is not set, anyone could remove files.

Reference information: For details about the TFS, see *z/OS UNIX System Services Planning*.

Specify enough storage above the bar if you are mounting a TFS in a colony address space

Description: If you plan to mount a temporary file system (TFS) in a colony address space, you need to specify enough storage above the 2 GB bar to accommodate the mount request, or choose to have the TFS mounted below the bar.

Element or feature:	z/OS UNIX.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	Before the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use a TFS in a colony address space and do not have enough storage specified above the 2 GB bar.
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: When a TFS is mounted in a colony address space, storage for the mount is obtained (by default) above the 2 GB bar. Therefore, make sure that enough storage is available above the bar. The amount of storage required depends on the size of the TFS.

If you wish to have the TFS mount obtain storage below the bar, specify PARM('-s 60 -3') in the MOUNT statement in the BPXPRM*xx* parmlib member to force the storage to be obtained below the bar.

Reference information:

z/OS UNIX actions to perform after the first IPL of z/OS V1R7

This section describes z/OS UNIX migration actions that you can perform only after you've IPLed z/OS V1R7. You need a running z/OS V1R7 system to perform these actions.

Install books and a bookshelf for the OHELP command

Description: The TSO/E OHELP command uses the BookManager READ base element to display online reference information about shell commands, TSO/E commands, C functions, callable services, and messages issued by the shell and dbx. Before this online help facility can be used, you must set it up by installing books and a bookshelf.

Element or feature:	z/OS UNIX.
When change was introduced:	General migration action not tied to a specific release.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if you use the OHELP command.
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: The IBM-supplied `/samples/ohelp.ENU` file contains the book and bookshelf names. These BOOK files and the BKSHELF file are shipped on the *z/OS Collection*. Copy `/samples/ohelp.ENU` to `/etc/ohelp.ENU`. If you do not want to use the IBM-supplied default file, you can create your own file called `/etc/ohelp.language_id`, where *language_id* is the TSO/E user's primary language code.

Guideline: Keep the default association of the number 1 with the *z/OS UNIX Command Reference* book. The book associated with 1 is the book that is searched if a user issues the OHELP command but does not specify a number. For example, if a user types:

```
OHELP ls
```

then OHELP opens the book associated with the number 1.

You can add any book name to the list of publications that are supported. The only time multiple books are searched is when the reference number is specified as an

asterisk. When a search is performed, only the books in the bookshelf are searched. To add book names, edit the file and install the books. For example:

```
25 'IBMBOOKS.EZ239104.EUVAP002.BOOK'    DCE Application Prog Reference
```

There is no limit to the number of books that you can include. Each book must have a unique number by which the help facility recognizes it, so it might be difficult for users to relate the books to the numbers if the total number of books is very large. Also, searches on a bookshelf that contains a large number of books can be slow.

For consistency from system to system, the following naming conventions are suggested for books available with OHELP:

Element or feature	OHELP numbers
z/OS UNIX	1–19
z/OS DCE	20–39
C/C++ for z/OS and Language Environment	40–49
z/OS	50–99
The RACF component of optional feature Security Server	100–119
TSO/E	120–139

The descriptive text that identifies each book can take up more than one line in the file, although the file is more readable if each record is on a single line. The text following the data set name can be used in messages, so it should be descriptive.

The books do not need to be from the *z/OS Collection*. You can include any BookManager BOOK file.

Reference information: For more information about the OHELP 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.

Element or feature:	z/OS UNIX.
When change was introduced:	zFS became the strategic file system as of z/OS V1R7.
Applies to migration from:	z/OS V1R6, z/OS V1R5, and z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	No, but recommended because the action is planned to become a requirement 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.

Steps to take: Before beginning the migration, follow these steps:

1. Establish backout procedures.
2. Decide on naming conventions.
3. Decide on unavailability.
4. Perform the conversion from an HFS to zFS file system.

   Tip: Use the BPXWH2Z tool to perform the conversion. It is an ISPF-based tool that migrates HFS file systems to zFS file systems. It has a panel interface that enables you to 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.
   - Have the migration run in TSO foreground or UNIX background.

   BPXWH2Z is located in partitioned data set SBPXEXEC (usually called SYS1.SBPXEXEC). When you run the BPXWH2Z tool on your z/OS V1R7 system, it uses the z/OS V1R7 level of the **pax** command. This level has been enhanced 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. When doing that, the z/OS V1R7 level of the **pax** command is recommended. However, you would need to allocate and format the target zFS file systems.

5. Change policies and scripts, and so forth, to reflect the change from the HFS file system to zFS file system.

   Tip: Use the RMF Monitor III option to report on zFS activity.

Reference information:

- For more information about the HFS and zFS file systems, see *z/OS UNIX System Services Planning*.
- To read about setting up zFS, see *z/OS Distributed File Service zSeries File System Administration*.
- For information about the **pax** enhancements that were added in z/OS V1R7, see *z/OS UNIX System Services Command Reference*.

Evaluate the need for chmod and chtag to follow symbolic links

Description: The **chmod** and **chtag** commands are updated to follow symbolic links, for compatibility with non-z/OS UNIX platforms. Shell scripts that depend on the original behavior of the **chmod** and **chtag** commands might fail. For example, the command:

```
chmod -R 777 dir
```

where the `dir` tree contains external links, will now generate errors for the external links.

You can use the **-h** option, which is unchanged, to specify that symbolic links are not followed.

Element or feature:	z/OS UNIX.
When change was introduced:	z/OS V1R5.
Applies to migration from:	z/OS V1R4.
Timing:	After the first IPL of z/OS V1R7.
Is the migration action required?	Yes, if **chmod** or **chtag** commands are not intended to follow symbolic links.
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: Evaluate any failing shell scripts. Typically, you can fix them by adding the **-h** option. For example:

```
chmod -hR 777 dir
```

Reference information: *z/OS UNIX System Services Command Reference.*

Appendix. Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in z/OS enable users to:

- Use assistive technologies such as screen readers and screen magnifier software
- Operate specific or equivalent features using only the keyboard
- Customize display attributes such as color, contrast, and font size

Using assistive technologies

Assistive technology products, such as screen-readers, function with the user interfaces found in z/OS. Consult the assistive technology documentation for specific information when using it to access z/OS interfaces.

Keyboard navigation of the user interface

Users can access z/OS user interfaces using TSO/E or ISPF. Refer to *z/OS TSO/E Primer*, *z/OS TSO/E User's Guide*, and *z/OS ISPF User's Guide Vol I* for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

Additional accessibility features may be included as part of the user interface of a particular z/OS element. Check the individual element's documentation for any additional information about accessibility.

z/OS Information

z/OS information is accessible using screen readers with the BookServer/Library Server versions of z/OS books in the Internet library at:

http://www.ibm.com/eserver/zseries/zos/bkserv/

Accessibility

Notices

This information was developed for products and services offered in the U.S.A. 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
USA

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, 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.

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:

IBM Corporation
Mail Station P300
2455 South Road
Poughkeepsie, NY 12601-5400
USA

339

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.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States, other countries, or both:
- AFP
- AIX
- AnyNet
- BookManager
- CICS
- DB2
- DB2 Universal Database
- DFSMSdfp
- DFSMSdss
- DFSMShsm
- DFSMSrmm
- DFSORT
- Encina
- ESCON
- @server
- FICON
- HiperSockets
- IBM
- IBMLink
- IMS
- Infoprint
- Language Environment
- Multiprise
- MVS
- MVS/ESA
- MVS/SP
- NetSpool
- NetView
- Open Class
- OS/390
- Parallel Sysplex
- PR/SM
- Print Services Facility
- PrintWay
- RACF
- Resource Link
- RMF
- S/390
- S/390 Parallel Enterprise Server
- Sysplex Timer
- SystemPac

- System z9
- Tivoli
- TotalStorage
- VisualAge
- VSE/ESA
- VTAM
- WebSphere
- z/Architecture
- z/OS
- z/VM
- zSeries

Java is a registered trademark of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Pentium is a registered trademark of Intel Corporation in the United States, other countries, or both. (For a complete list of Intel trademarks, see http://www.intel.com/sites/corporate/tradmarx.htm.)

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Index

Special characters

_MAKE_BI shell variable removal 326
/etc directory
  migrating files in 32
/var directory
  migrating files in 32
$HASP621, JES2 247

Numerics

1-byte console IDs, removal of 93
255 media types 201
3270 PC File Transfer Program
  no migration actions for 2
3800 Printing Subsystem, preparing to use 195
3900 Printing Subsystem, preparing to use 195
64-bit support
  migrating to 62
  restrictions 67

A

accessibility 337
Accommodation, z/OS Bimodal Migration 63
ACDS (active control data set)
  ensuring data integrity 204
actions to perform, meaning of
  after first IPL xviii
  before first IPL xvii
  before installing xvii
active control data set (ACDS)
  ensuring data integrity 204
adding VSAM alternate indexes
  PKI Services 185
address space, TN3270E Telnet server 177
address spaces, new 58
ADRUFO parameter list 203
after first IPL, migration actions
  BCP 111
  Communications Server 175
  Cryptographic Services 186
  DFSMS 204
  DFSORT 208
  HCD 216
  Infoprint Server 229
  Integrated Security Services 241
  JES2 256
  Language Environment 267
  NFS 276
  RMF 283
  SDSF 288
  Security Server 301
  sysplex 89
  XL C/C++ 322
  z/OS UNIX 333
ALLCMPID default change 164
ALTER security parameters, IDCAMS 193

alternate VSAM indexes for PKI Services, adding 185
ALTUSER command 302
AMDSADDD utility 104
AnyNet 138
AOP.ADMINISTRATOR profile, Infoprint Server 230
aopd.conf update required 234
aopsetup, running 229
APF authorization for EIM APIs 241
Application Support Class library removal 320
APPN search diagnostics 168
ARCHLVL parameter 64
  removing 68
ASSORTEDPARMS statement
  removed from IP Services 132
attributes, DFSMShsm journal 191
authorizing the z/OS NFS server for component
  trace 277
AUTOREJOIN/NOAUTOREJOIN 175

B

base elements
  removed from z/OS 23
BATCH_IODF_NAME_CHECK keyword 215
BCP migration actions
  after first IPL 111
  before first IPL 98
  before installing 91
BDT
  no migration actions for 2
BDT File-to-File
  no migration actions for 2
BDT SNA NJE
  no migration actions for 2
before first IPL, migration actions
  BCP 98
  Communications Server 139
  Cryptographic Services 183
  DFSMS 193
  DFSORT 208
  Distributed File Service 212
  general 29
  HCD 215
  HLASM 219
  ICKDSF 223
  Infoprint Server 226
  Integrated Security Services 238
  ISPF 243
  JES2 248
  JES3 257
  Language Environment 262
  Library Server 269
  NFS 271
  OSA/SF 279
  RMF 281
  SDSF 287
  Security Server 297
  sysplex 89

343

G

GDDM
   no migration actions for   2
GDDM-PGF
   no migration actions for   2
GDDM-REXX
   no migration actions for   2
general migration actions
   before first IPL   29
   before installing   3
GENPCH option no longer supported, C/C++   319
GetAddrinfo   148
gethostname() and gethostid() calls   162
GFSC729W, NFS message   271
GIM@PARM (SMP/E Dialog Settings)   310
GIM@UPRM
   removal of   310
GIMDFUT macro no longer supplied   309
GIMUTTBL module no longer supplied   309
global resource serialization with synchronous reserve
   default   96
GLOBALCONFIG MLSCHKTERMINATE   178
GRSCNFxx parmlib member
   SYNCHRES=YES default   96
GTTERM macro, TSO/VTAM   171
guest subcapacity reporting change, z/VM   107
GUI, Java-based OSA/SF   279

H

hardware migration actions   69
HASP621, JES2   247
HCD migration actions
   after first IPL   216
   before first IPL   215
HCD profile keywords   215, 216
HCM
   no migration actions for   2
Health Checker for z/OS, IBM
   HZSPROC address space   58
   using   103
HFS file systems
   migrating to zFS   334
HLASM migration actions
   before first IPL   219
HLASM Toolkit
   no migration actions for   2
HMC microcode, upgrading   75
how this document is organized   xv
how to use this document   xv
HQUERY command
   format change   199
   replacement for QUERY   201
HWOPTS option no longer supported, C/C++   319
HZSPROC address space   58

I

IATXDATX macro, JES3   258

IBM Health Checker for z/OS
   HZSPROC address space   58
   using   103
IBM HTTP Server
   no migration actions for   2
IBM HTTP Server NA Secure
   no migration actions for   2
IBM License Manager (ILM)
   removed from z/OS   23
   removing   27
IBM Open Class Library removal   320
ICE000I DFSORT message changed   208
ICEMAC macro default changes, DFSORT   208
ICKDSF migration actions
   before first IPL   223
ICSF migration actions
   after first IPL   186
   before installing   181
IDCAMS ALTER security parameters   193
IEASYSxx parmlib member
   ILMMODE parameter   28
IEFUSI exit routine   67
IHAPSA macro   66
IHAPSAE macro   66
IKTCASX1 exit parameter   172
ILM (IBM License Manager)
   removed from z/OS   23
   removing   27
ILMMODE parameter in parmlib   28
IMBED attribute for VSAM data sets, removal of   187
Infoprint Server
   migrating from NetSpool and IP PrintWay features of
      PSF   225
   NetSpool daemon start required   234
Infoprint Server migration actions
   after first IPL   229
   before first IPL   226
   before installing   225
installation steps   1
Integrated Security Services migration actions
   after first IPL   241
   before first IPL   238
   before installing   237
Internet address
   for ANSI publications   320
   for Bimodal Migration Accommodation   63
   for CFCC levels and processors   72
   for CFSIZER tool   72, 110
   for flashes   40
   for ISO publications   320
   for ISV support of z/Architecture   64
   for ISVs   37
   for migration to z9101   74
   for overview of IBM JSSE   183
   for reader comments   ii
   for Resource Link   78
   for SCRT User's Guide   109
   for ShopzSeries   23
   for SoftCap   19
   for software pricing   29
   for Text Search download   25

Readers' Comments — We'd Like to Hear from You

z/OS
Migration
Version 1 Release 7

Publication No. GA22-7499-08

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you?   ☐ Yes   ☐ No

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

Name _____   Address _____

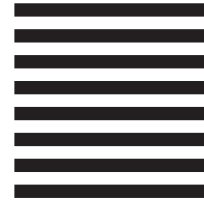Company or Organization _____

Phone No. _____

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL   PERMIT NO. 40   ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Department 55JA, Mail Station P384
2455 South Road
Poughkeepsie, NY 12601-5400

IBM ®

Program Number: 5694-A01

Printed in USA