## Contents

### Figures .............. vii

### Tables ............... ix

### About this document ........ xi
- Who should use this document : xi
- Where to find more information : xi
- The z/OS Basic Skills Information Center : xi
- z/OSMF home page : xii
- How to send your comments to IBM : xii
  - If you have a technical problem : xii

### Summary of Changes ........ xiii
- For z/OSMF Version 1 Release 13, SA38-0652-06 : xii
- For z/OSMF Version 1 Release 13, SA38-0652-05 : xiv
- For z/OSMF Version 1 Release 12, SA38-0652-04 : xv
- Information applicable to all releases : xvi

### Part 1. Planning ......... 1

#### Chapter 1. Overview of z/OSMF .. 3
- z/OSMF and related system components .. 4
- Software delivery options for z/OSMF .. 5
- What setup is needed for z/OSMF? .. 6
- Getting started with z/OSMF .. 6
- Overview of the z/OSMF administration tasks .. 8
- Overview of z/OSMF system management tasks .. 9
  - Capacity Provisioning task overview .. 9
  - Configuration Assistant task overview .. 11
  - Deployment task .. 12
  - Incident Log task overview .. 13
  - ISPF task overview .. 15
  - Resource Monitoring task overview .. 16
  - System Status task overview .. 18
  - Workload Management task overview .. 19
- Online help in z/OSMF .. 21
- Troubleshooting problems in z/OSMF .. 21

### Chapter 2. Planning for the z/OSMF configuration process ......... 23
- Choosing which plug-ins to configure .. 23
- System prerequisites for the z/OSMF plug-ins .. 24
  - System prerequisites for the Capacity Provisioning plug-in .. 24
  - System prerequisites for the Configuration Assistant plug-in .. 25
  - System prerequisites for the Incident Log plug-in .. 25
  - System prerequisites for the ISPF plug-in .. 27
  - System prerequisites for the Resource Monitoring plug-in .. 29
  - System prerequisites for the Software Deployment plug-in .. 30
- System prerequisites for the Workload Management plug-in .. 31
- The configuration process .. 32
- Authorizations needed during the configuration process .. 33
- Using an override file .. 34
- Choosing a script mode: Interactive or fastpath .. 34
- Planning worksheets for z/OSMF .. 35
  - Input for the core functions .. 36
  - Planning your plug-in selections .. 40
  - Input for the Capacity Provisioning task .. 41
  - Input for the Incident Log task .. 41
  - Input for the Workload Management task .. 44
- Reviewing the z/OSMF advanced settings .. 45
- Preparing your workstation for z/OSMF .. 46
- Planning a remote instance of z/OSMF .. 47
- Planning a backup instance of z/OSMF .. 47
- Planning service updates for z/OSMF .. 47

### Chapter 3. Planning security for z/OSMF .. 49
- Security concepts in z/OSMF .. 49
- Authorization modes for z/OSMF .. 50
  - Choosing an authorization mode .. 51
  - Managing guest user access in z/OSMF .. 52
  - Setting up security in SAF Authorization Mode .. 52
    - Security setup for plug-ins in SAF Authorization Mode .. 55
    - Managing security for links in SAF Authorization Mode .. 55
  - Setting up security in Repository Authorization Mode .. 56
    - Roles in z/OSMF .. 57
    - Managing security for links in Repository Authorization Mode .. 58

### Part 2. Configuration ......... 59

#### Chapter 4. Configuring z/OSMF .. 61
- Users of this information .. 61
  - Before you begin .. 61
  - How to access and run the script .. 61
    - Setting the z/OSMF environment variables for your shell session .. 62
    - Ensuring that your user ID has enough storage .. 64
    - Removing command aliases .. 64
    - Refreshing session status (for OMVS users) .. 65
  - Step 1: Create the initial configuration .. 65
  - Step 2: Run the security commands .. 69
  - Step 3: Verify the RACF security setup .. 72
  - Step 4: Prime the z/OSMF data file system .. 73
  - Step 5: Complete the setup .. 75
  - Step 6: Access the z/OSMF Welcome task .. 77
- Logging into z/OSMF .. 78
## Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>z/OSMF login page</td>
</tr>
<tr>
<td>2.</td>
<td>z/OSMF and related system components</td>
</tr>
<tr>
<td>3.</td>
<td>z/OSMF Welcome task (after user login)</td>
</tr>
<tr>
<td>4.</td>
<td>Capacity Provisioning task: Main page</td>
</tr>
<tr>
<td>5.</td>
<td>Configuration Assistant task main page</td>
</tr>
<tr>
<td>6.</td>
<td>Deployment page</td>
</tr>
<tr>
<td>7.</td>
<td>Incident Log task</td>
</tr>
<tr>
<td>8.</td>
<td>ISPF task main page</td>
</tr>
<tr>
<td>9.</td>
<td>Resource Monitoring main page</td>
</tr>
<tr>
<td>10.</td>
<td>System Status page</td>
</tr>
<tr>
<td>11.</td>
<td>Workload Management task main page</td>
</tr>
<tr>
<td>12.</td>
<td>User authorizations in z/OSMF</td>
</tr>
<tr>
<td>13.</td>
<td>SAF authorizations in z/OSMF</td>
</tr>
<tr>
<td>14.</td>
<td>SAF authorizations in z/OSMF: The default setup</td>
</tr>
<tr>
<td>15.</td>
<td>Example: Defining a link resource name and permitting a group to it</td>
</tr>
<tr>
<td>16.</td>
<td>Contents of the izu_env.sh file</td>
</tr>
<tr>
<td>17.</td>
<td>Format of the RACF ALTUSER command</td>
</tr>
<tr>
<td>18.</td>
<td>Override file updated for SAF Authorization Mode</td>
</tr>
<tr>
<td>19.</td>
<td>Override file entries for converting to Repository Authorization Mode</td>
</tr>
<tr>
<td>20.</td>
<td>izusetup.sh syntax</td>
</tr>
<tr>
<td>21.</td>
<td>Sample override file</td>
</tr>
<tr>
<td>22.</td>
<td>Sample override file</td>
</tr>
<tr>
<td>23.</td>
<td>Customizable areas of the z/OSMF Welcome page</td>
</tr>
<tr>
<td>24.</td>
<td>Content of the Welcome page properties file</td>
</tr>
<tr>
<td>25.</td>
<td>Example of a Welcome page properties file</td>
</tr>
<tr>
<td>26.</td>
<td>Content of the link properties file</td>
</tr>
<tr>
<td>27.</td>
<td>Example of a link definition</td>
</tr>
<tr>
<td>28.</td>
<td>Syntax for adding a link to z/OSMF</td>
</tr>
<tr>
<td>29.</td>
<td>Key components in the application linking process</td>
</tr>
<tr>
<td>30.</td>
<td>z/OSMF Administration tasks for Repository Authorization Mode</td>
</tr>
<tr>
<td>31.</td>
<td>Roles task main page</td>
</tr>
<tr>
<td>32.</td>
<td>Users task main page</td>
</tr>
<tr>
<td>33.</td>
<td>Sample results from the MODIFY DISPLAY, TRACE operator command</td>
</tr>
<tr>
<td>34.</td>
<td>Example of the &quot;garbage characters&quot; problem</td>
</tr>
<tr>
<td>35.</td>
<td>Invoking the Incident Log IVP as a batch job</td>
</tr>
<tr>
<td>36.</td>
<td>Checking the sysplex dump directory—sample job for creating an IPCS report</td>
</tr>
<tr>
<td>37.</td>
<td>Specifying a larger time interval for error log snapshots</td>
</tr>
<tr>
<td>38.</td>
<td>Determining which files systems are mounted</td>
</tr>
<tr>
<td>39.</td>
<td>Connection failure message in Firefox Version 3</td>
</tr>
<tr>
<td>40.</td>
<td>Connection failure message in Firefox Version 3</td>
</tr>
<tr>
<td>41.</td>
<td>Digital ring information for the controller user ID</td>
</tr>
<tr>
<td>42.</td>
<td>Format of resource URLs for z/OS jobs REST interface</td>
</tr>
<tr>
<td>43.</td>
<td>Example: Returned job status</td>
</tr>
<tr>
<td>44.</td>
<td>Example: Returned list of the jobs for an owner and job ID prefix</td>
</tr>
<tr>
<td>45.</td>
<td>Example: Returned list of spool files</td>
</tr>
<tr>
<td>46.</td>
<td>Example: Returned spool file content</td>
</tr>
<tr>
<td>47.</td>
<td>Example: Returned spool file content (a range of records)</td>
</tr>
<tr>
<td>48.</td>
<td>Example: Returned results of a job submission</td>
</tr>
<tr>
<td>49.</td>
<td>Example: Returned results of a job cancellation</td>
</tr>
<tr>
<td>50.</td>
<td>Example: Returned results of a job cancellation</td>
</tr>
<tr>
<td>51.</td>
<td>Example: Results of a job purge request</td>
</tr>
<tr>
<td>52.</td>
<td>Format of resource URLs for Application Linking Manager interface</td>
</tr>
<tr>
<td>53.</td>
<td>Registering an event type: request content</td>
</tr>
<tr>
<td>54.</td>
<td>Example: Registering an event type</td>
</tr>
<tr>
<td>55.</td>
<td>Example: Returned results of a successful event registration</td>
</tr>
<tr>
<td>56.</td>
<td>Example: Returned results of an unsuccessful event registration</td>
</tr>
<tr>
<td>57.</td>
<td>Example: Registering an event handler</td>
</tr>
<tr>
<td>58.</td>
<td>Example: Returned results of a successful list handlers request</td>
</tr>
<tr>
<td>59.</td>
<td>z/OS components used in Incident Log task processing</td>
</tr>
<tr>
<td>60.</td>
<td>Expected results from the D XCF,Couple,TYPE=LOGR operator command</td>
</tr>
<tr>
<td>61.</td>
<td>Expected results from the D C,HC operator command</td>
</tr>
<tr>
<td>62.</td>
<td>Expected results from the D LOGREC operator command</td>
</tr>
<tr>
<td>63.</td>
<td>Expected results from the D LOGGER operator command</td>
</tr>
<tr>
<td>64.</td>
<td>RACF commands to enable CEA to access SYSLOG</td>
</tr>
<tr>
<td>65.</td>
<td>Expected results from the D A,CEA operator command</td>
</tr>
<tr>
<td>66.</td>
<td>Expected results from the D A,AXR operator command</td>
</tr>
<tr>
<td>67.</td>
<td>Sample JCL to rename SVC dumps in the sysplex dump directory</td>
</tr>
<tr>
<td>68.</td>
<td>Expected results from the D PROG operator command</td>
</tr>
<tr>
<td>69.</td>
<td>izusetup.sh syntax</td>
</tr>
<tr>
<td>70.</td>
<td>Default override file</td>
</tr>
<tr>
<td>71.</td>
<td>Sample results from the izuupdate.sh -display script invocation</td>
</tr>
<tr>
<td>72.</td>
<td>Settings that are processed through the izuupdate.sh script</td>
</tr>
<tr>
<td>73.</td>
<td>Syntax for the izuupdate.sh script</td>
</tr>
<tr>
<td>74.</td>
<td>Portion of a z/OSMF server side log data</td>
</tr>
</tbody>
</table>
# Tables

1. Plug-ins and associated tasks in z/OSMF V1R13 .............................................. 23
2. z/OS setup actions for the Incident Log task ....................................................... 25
3. z/OS setup actions for the Resource Monitoring and System Status tasks .................. 29
4. z/OS setup actions for the Workload Management task ......................................... 31
5. Authorizations needed for configuring z/OSMF on your z/OS system .......................... 33
6. Modes for running the izusetup.sh script ................................................................ 35
7. Worksheet for the core functions variables ................................................................ 36
8. Worksheet for planning your plug-in selections ......................................................... 40
9. Worksheet for the Capacity Provisioning task variables ............................................. 41
10. Worksheet for the Incident Log task variables ......................................................... 42
11. Worksheet for the Workload Management task variable .......................................... 44
12. z/OSMF advanced settings ..................................................................................... 45
13. Decision points: Choosing a z/OSMF authorization mode ....................................... 51
14. Worksheet for the z/OSMF environment variables ................................................... 62
15. Which commands exec to use ................................................................................. 70
16. Sample MOUNT commands for z/OSMF file systems ............................................ 82
17. Actions users can take against global zones by access authority ................................ 88
18. Actions users can take against software instances by access authority ...................... 89
19. Actions users can take against deployments by access authority ............................... 90
20. Actions users can take against categories by access authority .................................. 91
21. WebSphere response file values ............................................................................. 93
22. Workload Management task authorizations when z/OSMF is running in Repository Authorization Mode ................................................................. 96
23. Workload Management task authorizations when z/OSMF is running in SAF Authorization Mode .............................................................................................. 97
24. Authorities needed after z/OSMF has been configured ............................................. 119
25. Script options for verification .................................................................................. 123
26. Summary of tools and information for troubleshooting problems with z/OSMF ......... 143
27. Columns in the environment checker tool results page .......................................... 145
28. Recommended settings for Firefox .......................................................................... 146
29. Recommended settings for Internet Explorer ........................................................... 148
30. Authorizing the z/OSMF administrator for operator commands ............................... 158
31. Responding to system setup errors indicated in the izuincidentlogverify.report file .... 162
32. Operations provided through the z/OS jobs REST interface services ....................... 184
33. Contents of the JSON Job document ..................................................................... 202
34. Contents of the JSON JobFile document .................................................................. 203
35. Contents of the JSON ErrorReport document ......................................................... 204
36. Error categories for z/OS jobs REST interface operations ....................................... 205
37. Category 1 errors .................................................................................................... 205
38. Category 2 errors ................................................................................................... 206
39. Category 3 errors ................................................................................................... 206
40. Category 4 errors ................................................................................................... 206
41. Category 5 errors ................................................................................................... 206
42. Category 6 errors ................................................................................................... 208
43. Category 7 errors ................................................................................................... 208
44. Category 8 errors ................................................................................................... 208
45. Category 9 errors ................................................................................................... 209
46. Operations provided through the Application Linking Manager interface services .... 214
47. Default profiles, resource names, and group assignments for z/OSMF in SAF Authorization Mode ................................................................. 228
48. CEA security profiles ......................................................................................... 229
49. Default configuration file ..................................................................................... 255
50. WebSphere response file values ............................................................................. 261
51. z/OSMF advanced settings ..................................................................................... 263
52. CEA reason codes related to Incident Log task processing ................................. 270
53. CEA reason codes related to ISPF task processing ................................................. 274
54. Keyboard shortcuts for panes ............................................................................... 297
55. Keyboard shortcuts for tabs ................................................................................... 298
56. Keyboard shortcuts for trees ................................................................................... 298
57. Keyboard shortcuts for tables ............................................................................... 298
58. Keyboard shortcuts for other interface controls ..................................................... 299
About this document

This document provides information for configuring IBM® z/OS® Management Facility (z/OSMF). This document also provides information for troubleshooting problems related to the use of z/OSMF.

Who should use this document

This document provides information for the system programmer responsible for configuring z/OSMF and diagnosing problems with the product. This document assumes that you are familiar with the z/OS operating system and its accompanying products.

The planning and configuration information in this document is intended for installations that install z/OSMF from a Custom-Built Product Delivery Option (CBPDO) software delivery package. If you receive z/OSMF as part of a ServerPac order, this configuration work is performed for you as part of a ServerPac post-install step. If you are using ServerPac, use the jobs and documentation supplied with your order. That documentation might refer you to specific sections of this document as required.

Where to find more information

Where necessary, this document references information about other elements and features of z/OS that is documented in z/OS publications. For complete titles and order numbers for all z/OS publications, see [z/OS Information Roadmap](http://publib.boulder.ibm.com/infocenter/zos/sicm/index.jsp), GC28-1727.

The z/OS library is available in the z/OS Collection Kit, SK2T-6700. This softcopy collection contains a set of z/OS and related unlicensed product documents. The CD-ROM collection includes the IBM Library Reader, a program that enables you to read the softcopy documents.

You can also visit the [z/OS Internet Library](http://publib.boulder.ibm.com/infocenter/zos/sicm/index.jsp).

The z/OS Basic Skills Information Center

The z/OS Basic Skills Information Center is a web-based information resource intended to help users learn the basic concepts of z/OS, the operating system that runs most of the IBM mainframe computers in use today. The Information Center is designed to introduce a new generation of Information Technology professionals to basic concepts and help them prepare for a career as a z/OS professional, such as a z/OS system programmer.

Specifically, the z/OS Basic Skills Information Center is intended to achieve the following objectives:

- Provide basic education and information about z/OS without charge
- Shorten the time it takes for people to become productive on the mainframe
- Make it easier for new people to learn z/OS.

To access the z/OS Basic Skills Information Center, open your web browser to the following web site, which is available to all users (no login required):

**z/OSMF home page**


**How to send your comments to IBM**

We appreciate your input on this publication. Feel free to comment on the clarity, accuracy, and completeness of the information or give us any other feedback that you might have.

Use one of the following methods to send us your comments:

1. Send an email to mhvrcfs@us.ibm.com
3. Mail the comments to the following address:
   IBM Corporation
   Attention: MHVRCFS Reader Comments
   Department H6MA, Building 707
   2455 South Road
   Poughkeepsie, NY 12601-5400
   U.S.A
4. Fax the comments to us, as follows:
   From the United States and Canada: 1+845+432-9405
   From all other countries: Your international access code +1+845+432-9405

Include the following information:
- Your name and address
- Your email address
- Your telephone or fax number
- The publication title and order number:
  IBM z/OSMF Configuration Guide
  SA38-0652-06
- The topic and page number related to your comment
- The text of your comment.

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.

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

**If you have a technical problem**

Do not use the feedback methods listed above. Instead, do one of the following:
- Contact your IBM service representative
- Call IBM technical support
Summary of Changes

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.

For z/OSMF Version 1 Release 13, SA38-0652-06

This document contains information previously presented in IBM z/OS Management Facility Configuration Guide, SA38-0652-05, which supports IBM z/OS Management Facility Version 1 Release 13.

This edition of the document removes all references to the WebSphere administrative console and replaces the references, as appropriate, with alternate information.

Script izuupdate.sh is new. This script is provided to assist you in querying and, if necessary, modifying certain environmental or advanced settings that control the behavior of z/OSMF. Use this script only at the direction of IBM Support. For more information, see Appendix F, "Modifying advanced settings for the z/OSMF configuration," on page 263.

This document contains updated information in support of the following APARs:
• OA36507
• PM40764
• PM43882
• PM45287
• PM47232
• PM50651
• PM54745
• PM56165.

Technical changes are indicated by a vertical line to the left of the change.

With the application of APAR PM56165, the DASD Management task is removed as a configuration option for z/OSMF V1R13. For details, see Software Announcement 211-252 (RFA56143). This publication is thus revised to describe the process of configuring z/OSMF without the DASD Management task as an available plug-in.

New troubleshooting actions are added for the ISPF task; see "Problems when using the ISPF task" on page 175.
For z/OSMF Version 1 Release 13, SA38-0652-05

This document contains information previously presented in *IBM z/OS Management Facility Configuration Guide*, SA38-0652-04, which supports IBM z/OS Management Facility Version 1 Release 12.

**New information**

The following categories are new in this release:

- **Software.** Tools for deploying software.
- **z/OS Classic Interfaces.** Traditional z/OS interfaces that have been integrated into z/OSMF.

The following system management tasks are new in this release:

- **Capacity Provisioning.** This task is included under the Performance category. Use this task to view the status of the Capacity Provisioning Manager, and to view information about the active domain configuration and provisioning policy.
- **Deployment.** This task is included under the Software category. Use this task to deploy any SMP/E packaged and installed software and to identify software requisites and possible regressions.
- **ISPF.** This task is included under the z/OS Classic Interfaces category. Use this task to access the ISPF applications on your host system through z/OSMF.

For more information about new and changed tasks, see the z/OSMF Welcome page, which includes the topics “What’s new” and “z/OSMF tasks at a glance.” Usage information is provided in the online help for each task.

In this release, your installation can select to have z/OSMF user authorizations managed by your security management product, such as RACF®, rather than by z/OSMF. This comprehensive form of security is called *SAF Authorization Mode*, and is designed to take advantage of established security controls in z/OS and SAF. In previous releases, user authorizations were defined by the z/OSMF administrator in the z/OSMF data file system and enabled on the host system by your security administrator. This earlier form of authorization, now referred to as *Repository Authorization Mode*, remains a supported option in this release, however, SAF Authorization Mode is the default for z/OSMF.

Your installation should plan for using SAF Authorization Mode, accordingly. This release includes tools to help with converting your existing z/OSMF user authorizations to SAF profiles and groups, which is required for using SAF mode. For more information, see Chapter 3, “Planning security for z/OSMF,” on page 49.

During the configuration process, some input values require that you supply a unique UID or GID. In this release, flexibility is enhanced through the addition of the overrides IZU_AUTOGID_OVERRIDE and IZU_AUTOUID_OVERRIDE, which allow you to set these options globally for any UID or GID values that you choose not to specify individually. For a description of the inputs that you supply during configuration, see “Input for the core functions” on page 36.

z/OSMF includes global settings or environment variables that control certain aspects of your z/OS UNIX shell session during the configuration process. In this release, you can specify these settings in an editable file and export the location of the file to your shell session. This approach saves you from having to enter the individual export commands for each shell session. See “Setting the z/OSMF environment variables for your shell session” on page 62.
A new topic describes the use of various z/OS system components in the processing of a z/OSMF task; see "System components used by the Incident Log task" on page 231.

This publication now includes information on the use of application programming interfaces (APIs) in z/OSMF, as follows:

- z/OS jobs REST interface is a new API that allows a client application to perform operations with batch jobs on a z/OS system.
- Application Linking Manager interface is a new API that allows a client application to define event types and event handlers to z/OSMF.

More information is provided in Part 4, "Programming," on page 179.

**Changed information**

This release adds a number of configuration variables and removes others. z/OSMF includes tools to help with updating your existing configuration to the new settings. For more information, see the migration actions that are described in Chapter 7, "Migrating to a new release of z/OSMF," on page 103.

In this release, script log files and report files are written to the z/OSMF log file directory, which is identified by the IZU_LOGFILE_DIR environment setting for the UNIX shell. By default, this directory is `/var/zosmf/configuration/logs/`. In previous releases, some report files were written to the z/OSMF configuration directory.

In this release, the names of the tasks provided through the Resource Monitoring plug-in are changed, as follows:

- Monitoring Desktops task is now called Resource Monitoring task
- Sysplex Status task is now called System Status task.

**Moved information**

Messages are now described in a new publication, IBM z/OS Management Facility Messages SA38-0654.

**For z/OSMF Version 1 Release 12, SA38-0652-04**

This document contains information previously presented in IBM z/OS Management Facility Configuration Guide, SA38-0652-03, which supports IBM z/OS Management Facility Version 1 Release 12.

This release includes support for Microsoft Internet Explorer 8 and Windows 7 Professional 64-bit. For the supported environments, see the z/OSMF Supported Browsers web page.

This document contains updated information in support of the following APARs:

- OA29534
- OA35023
- PM24215
- PM24843.

Technical changes are indicated by a vertical line to the left of the change.
Information applicable to all releases

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

The "Readers' Comments - We'd Like to Hear from You" section at the back of this publication has been replaced with a new section "How to send your comments to IBM" on page xii. The hardcopy mail-in form has been replaced with a page that provides information appropriate for submitting comments to IBM.
Part 1. Planning

Planning for z/OSMF includes the following topics:

- Chapter 1, “Overview of z/OSMF,” on page 3
- Chapter 2, “Planning for the z/OSMF configuration process,” on page 23
- Chapter 3, “Planning security for z/OSMF,” on page 49.
Chapter 1. Overview of z/OSMF

IBM z/OS Management Facility (z/OSMF) provides a framework for managing various aspects of a z/OS system through a web browser interface. By streamlining some traditional tasks and automating others, z/OSMF can help to simplify some areas of system management and reduce the level of expertise needed for managing a system.

z/OSMF provides a single platform for hosting the web-based administrative functions of IBM server, software, and storage products. With z/OSMF, you manage solutions rather than specific IBM products.

- Because z/OSMF provides system management solutions in a task-oriented, web browser based user interface with integrated user assistance, both new and experienced system programmers can more easily manage the day-to-day operations and administration of the mainframe z/OS systems.
- z/OSMF provides you with a single point of control for:
  - Performing common system administration tasks
  - Defining and updating policies that affect system behavior
  - Performing problem data management.
- z/OSMF allows you to communicate with the z/OS system through a web browser, so you can access and manage your z/OS system from anywhere.

This chapter introduces you to the major functions, architecture, and facilities of z/OSMF. Later chapters provide more detail about configuration, usage, and troubleshooting.
z/OSMF and related system components

z/OSMF is offered by IBM as a separately licensed program product for z/OS.

Structurally, z/OSMF is a set of web applications hosted on your z/OS system. Depending on the task to be performed, z/OSMF interfaces with other z/OS components to offer a simplified interface for performing tasks. These components make up the environment necessary for using the z/OSMF functions. z/OSMF does not provide a separate client installation. You will need to provide a compatible browser to access the z/OSMF web application.

z/OSMF includes the following software:
- IBM WebSphere® Application Server OEM Edition for z/OS Version 7, which provides a native application server runtime environment for z/OSMF.
- A set of administration and system management applications that run on IBM WebSphere Application Server OEM Edition for z/OS.
- Technologies for serving the web browser interface, such as JavaScript and a Dojo framework.

The goal of this architecture is to provide simplified systems management function through a common, easy-to-use, graphical user interface. Figure 2 shows a typical architecture and flow, starting with the user’s browser session and continuing through z/OSMF and IBM WebSphere Application Server OEM Edition for z/OS, with information passed to various z/OS system components as needed.
Depending on the particular task being performed, z/OSMF makes use of new enabling technologies on z/OS, such as the following z/OS components:

- **Common Information Model (CIM) server running on the host z/OS system.** This component provides the z/OS data and administrative capability.
- **Common event adapter (CEA).** This component enables CIM providers to identify, receive and process selected z/OS events.
- **System authorization facility (SAF).** This component enables programs to use system authorization services to control access to resources, such as data sets and MVS™ commands. SAF either processes security authorization requests directly or works with RACF, or other security product, to process them.
- **System REXX (SYSREXX).** This component provides an infrastructure through which programs written in the REXX language can be run outside the normal TSO/E or batch environments, using a programming interface.

For a closer look at the z/OS components that play a role in the processing of the z/OSMF Incident Log task, see “System components used by the Incident Log task” on page 231.

### Software delivery options for z/OSMF

z/OSMF is available for installation as a Custom-Built Product Delivery Option (CBPDO) software delivery package or through the ServerPac order delivery process. How your installation sets up z/OSMF — the procedures you use and the instructions you follow—depends in part on the software delivery option that you selected.

These differences are explained as follows:

**ServerPac users:**

- If you select the full system replacement installation type, a default instance of z/OSMF is set up for you. Here, z/OSMF is configured through a ServerPac post-installation job, using mostly IBM-supplied defaults. If you use full system replacement, it is recommended that you review the setup steps in this document to ensure that z/OSMF is configured correctly for your installation.
- If you select the software upgrade installation type, you require the planning and configuration information in this document. Your installation’s system programmer must set up the product runtime, IBM WebSphere Application Server OEM Edition for z/OS, and z/OSMF, through shell scripts that are provided with the product.
  
  For a software upgrade installation, if you accept the system defaults, ServerPac provides customization guidance for configuring z/OSMF. See the copy of ServerPac: Installing Your Order that is supplied with your order.

**CBPDO users:**

If you receive z/OSMF in a Custom-Built Product Delivery Option (CBPDO) software delivery package, you require the planning and configuration information in this document. Your installation’s system programmer must set up the product runtime, IBM WebSphere Application Server OEM Edition for z/OS, and z/OSMF, through shell scripts that are provided with the product.
What setup is needed for z/OSMF?

z/OSMF is a z/OS product, and as such, requires careful planning to ensure a smooth installation and configuration process. In planning this work, understand that:

- z/OSMF, the product, requires the SMP/E installation of several FMIDs, according to Program Directory for z/OS Management Facility, GI11-2886.
- IBM WebSphere Application Server OEM Edition for z/OS must be configured, if not already done, and this process requires certain z/OS resources to be set up, shell scripts to be run, and jobs to be run to set up security for RACF or an equivalent security management product.
- z/OSMF, the application, requires certain z/OS resources to be set up, shell scripts to be run, and security set up performed for RACF (or the equivalent).

Using z/OSMF requires sufficient authority in z/OS. Specifically, on the z/OS system to be managed, the resources to be accessed on behalf of z/OSMF users (data sets, operator commands, and so on) are secured through the security management product at your installation; for example, Resource Access Control Facility (RACF). Your installation’s security administrator must create these authorizations. z/OSMF provides scripts and the information in this document to assist your security administrator. Information about security setup is provided in Chapter 3, “Planning security for z/OSMF,” on page 49.

If you are migrating to a new release of z/OSMF, you can re-use much of the customization from your current configuration. For details, see Chapter 7, “Migrating to a new release of z/OSMF,” on page 103.

Getting started with z/OSMF

After z/OSMF is installed and configured, users can log in with a web browser. Though any z/OS user with sufficient RACF authorization can log into z/OSMF, a user must be defined with sufficient access authority to start working with z/OSMF tasks.

The z/OSMF interface consists of a login area in the top left corner, a navigation area of task categories below the login area, and a work area on the right. Depending on the plug-ins that your installation selects when configuring z/OSMF, the product offers a number of traditional system programmer tasks.

Logging into z/OSMF requires a user ID and password (or pass phrase) to authenticate. All actions taken from that browser session after successful authentication are performed under the identity that was used to log in. The z/OSMF interface customizes this view, based on the user's level of access, as defined in your security management product. As a result, each user’s navigation area displays only those tasks for which the user is authorized.

To display the tasks for a category, click on the plus sign (+) to the left of the category in the navigation area.

Figure 3 on page 7 shows the Welcome page that is displayed to a logged in user. The Welcome page provides information to help you get started with z/OSMF and learn more about the product.
For the logged in user, the navigation area is automatically tailored to show the tasks for which the logged in user is authorized. In Figure 3 all of the available tasks are displayed; this view is displayed to a user who is authorized to all of the tasks.

Figure 3. z/OSMF Welcome task (after user login)

For the logged in user, the navigation area is automatically tailored to show the tasks for which the logged in user is authorized. In Figure 3 all of the available tasks are displayed; this view is displayed to a user who is authorized to all of the tasks.

z/OSMF provides the following categories and related tasks:

**Configuration**
Select this category to view tasks for working with the system configuration. This category contains the Configuration Assistant task, which provides a guided interface for configuring TCP/IP policy-based networking functions. An overview is provided in "Configuration Assistant task overview" on page 11.

**Links**
Select this category to view links to other websites for system management tools and information. Some useful links were provided with the installation of z/OSMF.

**Performance**
Select this category to view tasks that can help you manage and monitor the performance of the workloads in your installation. For overviews of the tasks in this category, see:
- "Capacity Provisioning task overview" on page 9
- "Resource Monitoring task overview" on page 16
- "System Status task overview" on page 18
- "Workload Management task overview" on page 19.

**Problem Determination**
Select this category to view tasks that can help you manage problems on z/OS. This category contains the Incident Log task, which provides a consolidated list of system problems, along with the details and the diagnostic data captured and saved with each problem. This task also helps you send the diagnostic data to IBM or a vendor for further diagnosis. An overview is provided in "Incident Log task overview" on page 13.

**Software**
Select this category to view tasks that can help you manage your z/OS.
software. This category contains the Deployment task, which lets you deploy any software that is installed using SMP/E, organize your software instances and deployments, and follow IBM recommendations for software deployment. An overview is provided in “Deployment task” on page 12.

z/OS Classic Interfaces
Select this category to access ISPF and traditional ISPF applications, such as SDSF and HCD.

z/OSMF Administration
This category contains the product administration tasks; these are typically performed by the z/OSMF administrator at your installation. See “Overview of the z/OSMF administration tasks.”

Overview of the z/OSMF administration tasks
The z/OSMF Administration category in the z/OSMF navigation area includes a number of tasks, which, by default, the z/OSMF administrator is authorized to perform.

z/OSMF includes one user ID that is authorized to access z/OSMF as the administrator.

The default authorizations of the z/OSMF administrator depend in part on the authorization mode that your installation selects for z/OSMF when configuring the product.

In SAF Authorization Mode, the z/OSMF administrator has access to the following tasks:
• Managing links through the Links task
• Manage task associations through the Application Linking Manager task.

In Repository Authorization Mode, the z/OSMF Administrator has access to the following tasks:
• Assigning users to roles through the Users task
• Assigning tasks to roles through the Roles task
• Managing links through the Links task
• Manage task associations through the Application Linking Manager task.

In SAF Authorization Mode, user and role assignments are managed through the groups and profiles defined in your security product, rather than through z/OSMF. In this mode, the z/OSMF Administrator does not manage user authorizations to tasks, and thus, the Users task and the Roles task are not displayed in the navigation area.

For more information about the administration tasks, see Chapter 10, “Performing administration tasks in z/OSMF,” on page 135. For information about the authorization modes for z/OSMF, see Chapter 3, “Planning security for z/OSMF,” on page 49.
Overview of z/OSMF system management tasks

Depending on the plug-ins that your installation selects when configuring z/OSMF, the product offers a number of traditional system programmer tasks. Brief overviews of each task are provided in the following sections:

- “Capacity Provisioning task overview”
- “Configuration Assistant task overview” on page 11
- “Deployment task” on page 12
- “Incident Log task overview” on page 13
- “ISPF task overview” on page 15
- “Resource Monitoring task overview” on page 16
- “System Status task overview” on page 18
- “Workload Management task overview” on page 19

For authenticated users, context sensitive help is accessible at all times to assist with these tasks. In each page is a link to help at the upper right hand side. Click on this link to open a new window with help information for the page. Similarly, each message displayed in the interface includes a link to the help for that message.

To allow users in your installation to access z/OSMF, your security administrator must authorize the users to resources on the z/OS system. As an aid to your security administrator, z/OSMF includes sample REXX programs with RACF commands for authorizing users. More information about security is provided in Chapter 3, “Planning security for z/OSMF,” on page 49.

When introducing the z/OSMF product to your environment, it is recommended that your installation use the concept of roles to group similar users for managing user access to tasks. z/OSMF supports your installation’s security requirements for specific user permissions for each of the tasks. Depending on the authorization mode that you select for the product (more on this later), role definitions can be managed entirely through your security product (SAF authorization mode) or by the z/OSMF administrator through the z/OSMF interface (repository authorization mode). More information is provided in Chapter 3, “Planning security for z/OSMF,” on page 49.

Capacity Provisioning task overview

The Capacity Provisioning task in z/OSMF provides a browser-based user interface for working with the Capacity Provisioning Manager on your z/OS system. Through this task, you can request various reports of the status of the Capacity Provisioning Manager.

Figure 4 on page 10 shows the main page for the Capacity Provisioning task.
Some of the key functions available in the Capacity Provisioning task in z/OSMF follow.

- Manage CIM connections to your Capacity Provisioning Manager. Here, you can create, modify and delete CIM connections that you can use to connect to your Capacity Provisioning Manager. You can use both local CIM servers running on the same system on which z/OSMF is running and connect to remote CIM servers.

- View a domain status report. This report contains information about the current setup of the domain that is managed by the Capacity Provisioning Manager. The data displayed is the same as the data that is retrieved when you enter the REPORT DOMAIN command on the z/OS console.

- View an active configuration report. This report contains information about the active domain configuration and the status of its elements. Beside the name and the status of the active configuration, you can inspect details about the CPCs and systems that belong to the active configuration. The data displayed is the same as the data that is retrieved when you enter the REPORT CONFIGURATION command on the z/OS console.

- View an active policy report. This report contains information about the active policy and its status. You can view detailed information about each policy element. The data displayed is the same as the data that is retrieved when you enter the REPORT POLICY command on the z/OS console.
Configuration Assistant task overview

Configuration Assistant for z/OS Communications Server is a z/OSMF task that simplifies the configuration of the TCP/IP policy-based networking functions. The Configuration Assistant task provides centralized configuration of TCP/IP networking policies and can help reduce the amount of time required to create network configuration files.

Figure 5 shows the main page for the Configuration Assistant task.

Through the Configuration Assistant task, you can:

• Configure new policies for the following TCP/IP, policy-based networking disciplines:
  – IP Security, including IKE
  – Network Security Services (NSS)
  – Defense Manager daemon (DMD)
  – Application Transparent TLS (AT-TLS)
  – Intrusion Detection Services (IDS)
  – Policy-based Routing (PBR)
  – Quality of Service (QoS).

• Import previously defined policies for IP Security, AT-TLS, IDS, and PBR.

• Review Application Setup Tasks containing detailed instructions for getting a supported policy discipline up and running.

For information about getting started, see the Welcome page within the Configuration Assistant task. Here you can find extensive help, which you can reference at any time. On the web, you can find information about the Configuration Assistant at the z/OS Communications Server web site: http://www.ibm.com/software/network/commsserver/zos/support/
Deployment task

At some point after you have finished installing software, you might need to deploy the software to create a backup copy, to move the software to another system, or to create another SMP/E-serviceable copy for installing service or other products. To assist you with performing these tasks, z/OSMF offers a software deployment solution, the Deployment task.

Key features

The Deployment task provides a Web-based, user-interface that contains a checklist, wizards, and property sheets designed to guide you through the software deployment process and help reduce common deployment errors. With the Deployment task, you can:

- **Deploy any software (IBM and vendor) that is SMP/E packaged and installed.** For example, you can deploy:
  - z/OS operating system and related products.
  - Subsystems and related products.
  - Individual products.
  - Service upgrades for all of the above (by way of complete replacement).
Installation of software or service upgrades is outside the scope of the Deployment task. Use SMP/E to assist with the installation process.

- **Perform local and remote deployments.** The Deployment task supports the deployment of software to DASD volumes shared within the same sysplex (local deployment) or to DASD volumes accessible to another sysplex (remote deployment). For more details, see the online help for the Deployment task.

- **Identify missing SYSMODs before deploying software.** The Deployment task assists with the identification of SYSMODs that are missing in the source software instance or any related software instances.

- **Manage your global zones, software instances, and deployments.** The Deployment task provides a tabular view of your software instances, global zones, and deployments so that you can manage these objects across your enterprise. For example, you can add, modify, view, and remove these objects.

- **Organize your software instances and deployments.** The Deployment task provides a category feature that you can use to organize your software instances and deployments. You can, for example, categorize them by product, subsystem, geography, or business unit.

- **Adhere to IBM recommendations for software deployment because many of those recommendations are integrated into the deployment process.** For example, the Deployment task:
  - Uses SMP/E DDDEF entries to automatically locate data sets, such as SMP/E data sets, target libraries, and distribution libraries.
  - Deploys all of the software included in a target zone and optionally the related distribution zone.
  - Copies the SMP/E consolidated software inventory (CSI) with the software. If you currently do not copy your SMP/E CSIs, you will see a slight increase in DASD usage per target software instance.

To open the Deployment task, in the navigation area, expand the Software category and select Deployment. To start using the Deployment task, select one of the actions listed on the Deployment page.
Incident Log task overview

When a problem occurs on a z/OS system, you might need to determine what happened and why, and then find the fix or report the problem to IBM or an independent software vendor (ISV). Typically, you need to get to the root of the problem quickly, but the task of gathering diagnostic data and sending it to a support team can be very time-consuming. To assist you with diagnosing and reporting the problem, z/OSMF offers a problem data management solution, the Incident Log task.

The Incident Log task streamlines and automates time-consuming and manual parts of the problem data management process. Specifically, the Incident Log task gathers and displays system-detected and user-initiated incidents, collects associated logs and dumps at the time of the problem, and facilitates sending that data to IBM or another vendor for further diagnostics. Using the Incident Log task reduces the possibility of errors while obtaining, aggregating and sending the collection of diagnostic data to IBM or an ISV.

To open the Incident Log task, in the navigation area, expand the Problem Determination category and select Incident Log. The Incident Log page is displayed.

Figure 7 on page 14 depicts the Incident Log page, which lists all incidents in the sysplex meeting your specified filter criteria.
Key features

With the Incident Log task, you can:

- **Manage the incidents that occurred on a system or in a sysplex.** The Incident Log task provides a consolidated view of all incidents occurring on all participating systems in the sysplex (those that communicate through the same sysplex dump directory).

- **Browse the logs collected for an incident.** When an incident occurs, the Incident Log task collects and saves the associated SVC dumps and diagnostic log snapshots. You can browse the error log, error log summary, and operations log.

- **Allow the next dump of an incident with the same MVS symptom string.** The Incident Log task provides the ability to update the DAE data set, so that you can capture the next instance of an SVC dump being suppressed by DAE.

- **Send diagnostic data and attachments to IBM or another vendor for further diagnostics.** The Incident Log task provides a wizard that you can use to send diagnostic data and additional attachments to IBM or another vendor. You can send files using standard FTP or using the z/OS Problem Documentation Upload Utility (PDUU), which supports parallel FTP and encryption. For more information about PDUU, see [z/OS MVS Diagnosis: Tools and Service Aids](#).

- **Associate the incident with problems recorded in other problem management systems.** The Incident Log task allows you to correlate an incident with an IBM problem number, an ISV problem number, or with a problem record in your installation's problem management system.

- **Track additional information with an incident.** The Incident Log task allows you to specify additional information that you want to track about an incident,
such as who is assigned to resolve the issue, which business applications are impacted, which component is the source of the issue, and which solution has been implemented.

- **Monitor the status of an FTP job.** An FTP job is created when you send diagnostic data to IBM or another vendor. The Incident Log task allows you to browse or cancel FTP jobs and view or delete the status of FTP jobs.

### ISPF task overview

The ISPF task allows you to access your host system ISPF applications from z/OSMF. For system administrators, the ISPF task provides a web-based alternative to using traditional, 3270 based ISPF.

Through the ISPF task, you can:

- Access any applications that you usually access through z/OS ISPF on the host system, such as System Display and Search Facility (SDSF) and Hardware Configuration Definition (HCD).
- Run TSO commands
- Use multiple sessions in parallel (split screen mode)
- Customize the ISPF settings as you do with ISPF on the host system
- Use dynamic areas in ISPF and attributes such as color highlighting
- Use ISPF functions and utilities (for example, ISPF option 3).

The ISPF task works with ISPF on your host z/OS system. User access to ISPF applications is controlled through the same authorizations that exist for your z/OS system.

**Figure 8** shows the main page for the ISPF task.

![Figure 8. ISPF task main page](image)
Usage considerations for ISPF task users

Some TSO/E and ISPF functions are restricted or unavailable under z/OSMF ISPF. Users should be aware of the following usage considerations:

- z/OS creates an address space for each ISPF task session that is started. An individual z/OSMF user can have up to ten active ISPF task sessions. To conserve system resources, z/OSMF allows no more than 50 ISPF task sessions to be started on your system at any one time.
- In some situations, logon pre-prompt exits IKJEFLD and IKJEFLD1 that set the Don't Prompt control switch bit on can prevent z/OSMF ISPF users from logging on, or might not work with z/OSMF ISPF.
- z/OSMF users can be canceled by the MVS operator, based on user ID, and ASID if needed. In some cases, however, these operations might have to be performed twice to take affect.
- An ISPF task user cannot:
  - Switch to TSO/E native mode from within a z/OSMF ISPF session.
  - Log in remotely to TSO/E on another z/OS system from z/OSMF ISPF.
  - Use full-screen applications that run outside of ISPF, such as OMVS, TELNET, or GDDM.
  - Receive TSO/E messages, such as messages from MVS operators or users in TSO/E native mode.
  - Use commands that are not allowed in traditional ISPF, such as TSOLIB and LOGON.
- Most VTAM terminal macros used by full screen applications, such as GTTERM or STFSMODE, are not supported under z/OSMF ISPF. However, you can use the GTSIZE macro or GETDEVSZ macro to obtain the screen size.
- Broadcast messages are not displayed at log on. You can view these messages in the TSO Messages window, which is displayed by clicking the TSO Messages link in the upper right corner of the ISPF task main page.
- Session Manager is not available; do not specify ADFMDF03 in your logon procedure. Your logon procedure should use the IBM-supplied terminal monitor program, IKJEFT01, which is specified on the PGM= operand of the EXEC statement.
- In some cases, the Attention button might appear to be unresponsive. If so, try clicking the Attention button again. If the request times out, click Cancel to interrupt the process. Doing so should have the same effect as clicking the Attention button.
- The REXX and CLIST system terminal ID (SYSTEMID) variable is blank for z/OSMF ISPF task sessions.

Resource Monitoring task overview

The Resource Monitoring task in z/OSMF provides a web-based user interface that you can use to monitor the performance of the z/OS sysplexes, AIX® system complexes (System p®), Linux system complexes (System z® and System x®), or Linux images (System z and System x) in your environment. With the Resource Monitoring task, you can monitor most of the metrics supported by Resource Measurement Facility™ (RMF™) Monitor III, create and save custom views of the metrics, and display real-time data as bar charts.

For z/OS sysplexes, the Resource Monitoring task takes its input from a single data server on one system in the sysplex. That data server collects data from the RMF Monitor III data gatherer on each image in the sysplex. This function is called
the Distributed Data Server (DDS). To allow monitoring of several sysplexes, ensure that each sysplex has an active DDS.

Similarly for Linux or AIX system complexes, the Resource Monitoring task collects input from a Cross Platform Distributed Data Server on a z/OS system that gathers data from CIM servers on the systems to be monitored.

The Resource Monitoring task can also monitor single Linux images or guests. Here, the task collects input from the RMF Linux data gatherer (rmfpms).

To display the Resource Monitoring task, expand the Performance category in the navigation area and select Resource Monitoring. The Resource Monitoring task main page is displayed, as shown in Figure 9.

Some of the key functions available in the Resource Monitoring task follow:

- **Create monitoring dashboards.** You can create monitoring dashboards or custom views that you can use to monitor the performance of the sysplexes, system complexes, or images in your environment.

- **Save monitoring dashboards.** You can save monitoring dashboards. Doing so allows you to reuse the monitoring dashboard or template so that you can easily view performance data for your monitored sysplexes, system complexes, or images from the same angle.

- **Work with multiple monitoring dashboards.** You can work with multiple monitoring dashboards simultaneously. To do so, open the dashboards with which you want to work in a new tab in the z/OSMF work area or in a new browser tab or window.

- **Monitor multiple resources simultaneously.** You can collect data for multiple resources at the same time. To do so, associate the metrics in a dashboard with different resources.
• **Create dashboards that are not associated with a specific sysplex.** Doing so streamlines the number of dashboards that you have to create because you can create one dashboard and use it for all of the sysplexes in your installation.

• **Monitor the performance over time.** The Resource Monitoring task provides controls that you can use to browse through the samples that have been collected for the metric groups contained in a monitoring dashboard. Up to 100,000 samples are collected for a dashboard. To browse the samples, use the slider and the backward and forward arrows provided in each metric group.

Before you can use the Resource Monitoring task, you must define the sysplexes, system complexes, or images to be monitored in the System Status task. To display the System Status task, expand the Performance category in the navigation area and select System Status.

**System Status task overview**

The System Status task in z/OSMF combines data from an entire sysplex into one performance indicator so that you can quickly assess the performance of the workloads running on the z/OS sysplexes in your environment. The System Status task also provides a single location where you can define the z/OS sysplexes to be monitored in the Resource Monitoring task.

You can also manage the AIX system complexes (System p) and Linux system complexes (System z and System x) to be monitored in the Resource Monitoring task. To do so, the RMF Cross Platform Distributed Data Server must be installed and configured properly. Further, you can manage single Linux images using the Linux data gatherer (rmfpms).

To display the System Status task, expand the Performance category in the navigation area and select **System Status**. The System Status task main page is displayed. See [Figure 10](#).

![Figure 10. System Status page](#)
Workload Management task overview

The Workload Management task in z/OSMF provides a browser-based user interface that you can use to manage z/OS Workload Manager (WLM) service definitions and provide guidelines for WLM to use when allocating resources. Specifically, you can define, modify, view, copy, import, export, and print WLM service definitions. You can also install a service definition into the WLM couple data set for the sysplex, activate a service policy, and view the status of WLM on each system in the sysplex.

Some of the key functions available in the Workload Management task follow.

- **Display list of service definitions.** The Workload Management task provides a list of the WLM service definitions that have been defined in z/OSMF along with history information (such as when the service definition was installed or modified), messages, and user activity. The list of service definitions is retrieved from the service definition repository, which refers to the directory in the z/OSMF data file system in which the data for the Workload Management task is stored.

- **Work with multiple service definitions.** In the Workload Management task, you can work with multiple service definitions simultaneously. To do so, open the service definitions with which you want to work in its own View, Modify, Copy, or Print Preview tab. You can also define multiple service definitions at the same time by opening several New tabs.

- **Install service definitions.** The Workload Management task provides features that you can use to install a service definition into the WLM couple data set for the z/OSMF host sysplex.

- **Extract the installed service definition.** The Workload Management task automatically extracts the service definition that is installed in the WLM couple data set for the z/OSMF host sysplex and stores it in the service definition repository so that you can view it, modify it, or activate one of its service policies.

- **Import and export service definitions.** The Workload Management task provides features that you can use to import a service definition from or export a service definition to your local workstation or a sequential data set on the z/OSMF host system. The exported service definition is formatted so that it can be opened with the z/OS WLM Administrative Application (also called the WLM ISPF application).

- **Provide table view and print preview of the service definition.** The Workload Management task provides two views of a service definition.
  - **Table View.** The table view displays the parts of the service definition as tables. You can display the table view by opening the service definition in the New, View, Modify, or Copy tab. If you open the service definition in the New, Modify, or Copy tab, you can modify the service definition. In the View tab, you cannot modify the service definition.
  - **Print Preview.** The print preview presents the service definition in HTML format and allows you to select which parts of the service definition you want to preview or print. You can display the print preview by opening the service definition in the Print Preview tab.

- **Activate service policies.** In the Workload Management task, you can specify which policy to activate when you install a service definition or you can activate a service policy that is defined in the service definition currently installed in the WLM couple data set for the sysplex.

- **Preview service policies with overrides applied.** The Workload Management task allows you to preview an HTML formatted version of the service policy...
with overrides applied. The HTML formatted service policy contains the information that would be included in the policy if it were activated. To preview a service policy, open the policy in the Print Preview tab.

- **View the WLM status.** The Workload Management task provides an HTML formatted view (WLM Status tab) of the same data that is retrieved when you enter the D WLM, SYSTEMS command on the z/OS console. Specifically, the WLM Status tab displays the status of WLM on each system in the sysplex, and lists details about the installed service definition and the active service policy.

- **Define settings.** The Workload Management task provides a shared location (Settings tab) where you can specify how long to keep the service definition history and define the code page, time zone, and backup sequential data set for the sysplex. You can also enable consistency checking between z/OSMF and the WLM couple data set, and indicate whether you want the Workload Management task to display or suppress information messages.

Actions that require the Workload Management task to interact with the sysplex are limited to the sysplex in which the z/OSMF host system is a member. Such actions include installing a service definition, activating a service policy, viewing the sysplex status, and so on. If you want to interact with another sysplex, z/OSMF must be installed on a system in that sysplex and you must log into that z/OSMF instance. You can use the service definition import and export functions to copy a service definition from one z/OSMF instance to another.

To display the Workload Management task, expand the Performance category in the navigation area and select Workload Management. Figure 11 shows the main page for the Workload Management task. The Overview tab serves as the launch point for the actions that your user ID is authorized to access within the Workload Management task. To start using the Workload Management task, select one of the actions listed in the Overview tab.
Online help in z/OSMF

For authenticated users, context sensitive help is accessible at all times to assist with understanding and performing a task, troubleshooting problems, entering information, and using all aspects of z/OSMF. In each product page is a link to help at the upper right hand side. Users can click on this link to open a new window with help information for the page. Similarly, each message displayed in the interface includes a link to the help for that message.

Troubleshooting problems in z/OSMF

Information on troubleshooting problems in z/OSMF, including a summary of tools provided to assist with diagnosis, is provided in Chapter 11, “Troubleshooting,” on page 143.

Descriptions of the messages you might encounter while using z/OSMF are provided in the document IBM z/OS Management Facility Messages SA38-0654.
Chapter 2. Planning for the z/OSMF configuration process

Determine on which z/OS operating system image you want to run this product. z/OSMF V1R13 must be run on z/OS Version 1 Release 13 or later.

The planning and configuration information in this document is intended for installations that install z/OSMF from a Custom-Built Product Delivery Option (CBPDO) software delivery package, or from a ServerPac order using the software upgrade method of installation. If you install z/OSMF as part of a ServerPac order using the full system replacement method of installation, this setup work is performed for you during the ServerPac post-installation process. Here, you use the jobs and documentation supplied with your ServerPac order to create an initial instance of z/OSMF. You might need sections of this document during the ServerPac process, and later, if you choose to create additional instances of z/OSMF.

It is required that IBM WebSphere Application Server OEM Edition for z/OS is installed and configured on your z/OS system, as described in IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide, GA32-0631. This step is required even if your system already includes a running instance of WebSphere Application Server for z/OS.

It is recommended that you complete the planning for both IBM WebSphere Application Server OEM Edition for z/OS and z/OSMF before attempting to configure either product.

Choosing which plug-ins to configure

In z/OSMF, a plug-in is a collection of one or more system management tasks. Most functions in the z/OSMF navigation area are provided through plug-ins, which you enable when you configure the product.

Table 1 shows which plug-ins are available for configuration in z/OSMF V1R13.

<table>
<thead>
<tr>
<th>Plug-in name</th>
<th>Tasks provided by the plug-in</th>
<th>Associated category in the z/OSMF navigation area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity Provisioning</td>
<td>Capacity Provisioning</td>
<td>Performance</td>
</tr>
<tr>
<td>Configuration Assistant</td>
<td>Configuration Assistant</td>
<td>Configuration</td>
</tr>
<tr>
<td>Incident Log</td>
<td>Incident Log</td>
<td>Problem Determination</td>
</tr>
<tr>
<td>ISPF</td>
<td>ISPF</td>
<td>z/OS Classic Interfaces</td>
</tr>
<tr>
<td>Resource Monitoring</td>
<td>• Resource Monitoring</td>
<td>Performance</td>
</tr>
<tr>
<td></td>
<td>• System Status</td>
<td></td>
</tr>
<tr>
<td>Software Deployment</td>
<td>Deployment</td>
<td>Software</td>
</tr>
<tr>
<td>Workload Management</td>
<td>Workload Management</td>
<td>Performance</td>
</tr>
</tbody>
</table>

Configuring a plug-in is optional. In general, you should configure the set of plug-ins that you are interested in during the initial z/OSMF configuration. You can always add more plug-ins later.
Your decision on which plug-ins to configure will depend in part on your installation's readiness to perform the various z/OS system customization updates associated with each plug-in. When planning for z/OSMF, review the system prerequisites for each plug-in, as described in this document. In some cases, you might find it easier to begin with a smaller number of plug-ins, and add more later as you coordinate this work with the necessary system customization.

To add a plug-in after the configuration process is completed, you will repeat most of the z/OSMF configuration steps. For more information, see “Adding plug-ins to a z/OSMF configuration” on page 124. After a plug-in is configured, you can remove it from z/OSMF only by repeating the z/OSMF configuration process and not selecting the plug-in.

It is possible to configure z/OSMF without any plug-ins selected. Doing so provides only the base functions of z/OSMF (referred to as core functions in this document). The core functions of z/OSMF include the Administration category and related tasks, the Welcome task, the Links category, and the online help. The core functions of z/OSMF are always enabled when you configure the product.

### System prerequisites for the z/OSMF plug-ins

This section describes the z/OS system setup actions that are required for enabling the various system management tasks in z/OSMF. Which steps you need to complete depend on which plug-ins you choose to deploy in z/OSMF.

In terms of security set-up, the amount of work needed will depend in part on the authorization mode that will be used for your configuration. In SAF Authorization Mode, which is the default for new z/OSMF V1R13 instances, enabling a task will require that you perform some customization of the security management product on your host system (for example, make updates to the RACF database). The configuration process provides a REXX exec with RACF commands to help with performing these changes. In Repository Authorization Mode, security product customization is less likely because authorizations are maintained through z/OSMF. The security set-up requirements for each plug-in are described in Chapter 3, “Planning security for z/OSMF,” on page 49. See “Adding plug-ins to a z/OSMF configuration” on page 124.

Regardless of which authorization mode you select, an additional set of authorizations is needed whenever you add users to z/OSMF. The z/OSMF configuration process creates a REXX exec with commands for your security administrator to use for authorizing users to the z/OSMF tasks. See “Authorizing users to z/OSMF” on page 120.

Some z/OSMF tasks require the Common Information Model (CIM) server to be running on the host z/OS system. Using these tasks will require that you ensure that the CIM server is configured on your system, including security authorizations and file system customization:

- Capacity Provisioning
- Incident Log
- Workload Management

Based on your selection of plug-ins, you must complete the associated system prerequisites, as appropriate. The requirements for each plug-in are described in the sections that follow:

- “System prerequisites for the Capacity Provisioning plug-in” on page 25
- “System prerequisites for the Configuration Assistant plug-in” on page 25
System prerequisites for the Capacity Provisioning plug-in

If you plan to use the Capacity Provisioning task, ensure that the capacity provisioning manager (CPM) is running on the system on which z/OSMF is installed.

Optional: Determine whether access to a remote Common Information Model (CIM) server is required. This work can be done after you have configured z/OSMF. See “Updating z/OS for the Capacity Provisioning plug-in” on page 83 for instructions.

System prerequisites for the Configuration Assistant plug-in

No system customization is required to enable the Configuration Assistant task.

Optional: If your installation uses the Windows desktop version of Configuration Assistant for z/OS Communications Server, and you want to continue using your existing data in z/OSMF, you can transfer your backing store files to the z/OSMF environment. This setup can be done after configuring z/OSMF; see “Updating z/OS for the Configuration Assistant plug-in” on page 84.

System prerequisites for the Incident Log plug-in

To use the Incident Log task, you must ensure that the following z/OS components and facilities are enabled on your system. These functions support the collection of diagnostic data and the creation of diagnostic logs.

Table 2 summarizes the z/OS system changes that are required or recommended for enabling the Incident Log task. Much of this work might already be done on your system, or might not be applicable. If so, you can skip the particular setup action. Other setup actions might require modifications to an existing setting, for example, if your installation has already defined a couple data set for the system logger component, you might need to increase the space allocation for system logger log stream records. For assistance with these setup actions, see the procedures referenced in the Where described column of Table 2.

For a detailed illustration of how z/OS system infrastructure is used in the processing of the Incident Log task, see “System components used by the Incident Log task” on page 231.

<table>
<thead>
<tr>
<th>Table 2. z/OS setup actions for the Incident Log task</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>z/OS setup action</strong></td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td>1.</td>
</tr>
</tbody>
</table>

Chapter 2. Planning for the z/OSMF configuration process 25
Table 2. z/OS setup actions for the Incident Log task (continued)

<table>
<thead>
<tr>
<th>z/OS setup action</th>
<th>Where described</th>
<th>Check when task is completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Create a sysplex dump directory. To see whether a sysplex dump directory is already defined on your system, check for the existence of data set SYS1.DDIR.</td>
<td>See &quot;Creating the sysplex dump directory&quot; on page 243.</td>
<td></td>
</tr>
<tr>
<td>5. Ensure that the common event adapter (CEA) component is configured on your system, including security authorizations. Usually, the CEA address space is started automatically during z/OS initialization.</td>
<td>IBM provides the CEASEC job to help you create the security authorizations for CEA; see member CEASEC in SYS1.SAMPLIB. For information about running CEA, see &quot;Ensuring that CEA is active&quot; on page 245.</td>
<td></td>
</tr>
<tr>
<td>To determine whether the CEA address space is active, enter the following command:</td>
<td>D A,CEA</td>
<td></td>
</tr>
<tr>
<td>6. Ensure that System REXX (SYSREXX) is set up and active on your system.</td>
<td>See &quot;Ensuring that System REXX is set up and active&quot; on page 247.</td>
<td></td>
</tr>
<tr>
<td>To determine whether SYSREXX is active, enter the following command:</td>
<td>D A,AXR</td>
<td></td>
</tr>
<tr>
<td>7. If your installation has chosen to rename a dump data set, ensure that the data set name in the sysplex dump directory is correct.</td>
<td>See &quot;Ensuring that dump data set names are correct&quot; on page 248.</td>
<td></td>
</tr>
<tr>
<td>8. Ensure that SYS1.MIGLIB is APF-authorized. This step allows the AMATERSE service aid to be called by System REXX execs, which are authorized.</td>
<td>See &quot;Authorizing the SYS1.MIGLIB data set&quot; on page 249.</td>
<td></td>
</tr>
<tr>
<td>To determine whether SYS1.MIGLIB is APF-authorized, enter the following command:</td>
<td>D PROG,APF,DSNAME=SYS1.MIGLIB</td>
<td></td>
</tr>
<tr>
<td>9. Enable message log snapshots on the host system, or, optionally, on a sysplex-wide basis.</td>
<td>See &quot;Setup considerations for log snapshots.&quot;</td>
<td></td>
</tr>
<tr>
<td>10. Enable error log snapshots on the host system, or, optionally, on a sysplex-wide basis.</td>
<td>See &quot;Setup considerations for log snapshots.&quot;</td>
<td></td>
</tr>
</tbody>
</table>

**Setup considerations for log snapshots**

The Incident Log task can work with incident data from throughout your sysplex, or from just the system on which z/OSMF is installed. Your installation should determine the scope of incident related data collection, or log snapshots, to be used for the Incident Log task. To obtain the most benefit from the Incident Log task, it is recommended that your installation enable log snapshots on a sysplex-wide basis. If you cannot do so, however, z/OSMF is ready to work with incident data from a single system.

This section describes the system setup to be completed, based on the scope of data collection that you require.
When message data is collected on a sysplex-wide basis, z/OSMF uses the operations log (OPERLOG) as the source for message data. This processing requires the following system setup:

- Enabling OPERLOG on each system for which message data is to be collected. See “Enabling the operations log (OPERLOG)” on page 235.
- Defining log streams for log snapshots to be obtained by the common event adapter (CEA) component of z/OS. See “Defining diagnostic snapshot log streams” on page 239.
- Defining a couple data set for sysplex-wide logging through system logger. See “Defining a couple data set for system logger” on page 233.

If you do not enable message data collection on a sysplex wide basis, z/OSMF collects message data for the z/OS host system only, using the system log (SYSLOG) as the source for creating diagnostic snapshots. This processing requires one of the following minimum levels of JES on your z/OS system:

- JES2 V1R11, or
- JES3 V1R11 (with the PTF for APAR OA29534).

Also, see “Enabling SYSLOG for diagnostic snapshots” on page 240.

When error log data is collected on a sysplex-wide basis, z/OSMF uses the logrec log stream as the source for error data. This processing requires that you set up system logger so that logrec data is written to a logger log stream. See “Defining and activating the LOGREC log stream” on page 237.

If you do not enable error log data collection on a sysplex wide basis, z/OSMF collects error log data for the z/OS host system only, using the logrec data set as the source for logrec data.

System prerequisites for the ISPF plug-in

This section describes the system setup actions required for using the ISPF task.

To use the ISPF task, a user should be an existing TSO/E user with a valid, non-expired password. For each user of the ISPF task, you must ensure that the corresponding user ID:

- Is authorized to TSO/E
- Is authorized to the JES spool. This authorization allows the user to use various functions in TSO/E, such as the SUBMIT, STATUS, TRANSMIT, and RECEIVE commands, and to access the SYSOUT data sets through the command TSO/E OUTPUT command.
- Has an OMVS segment defined, which allows for access to z/OSMF
- Has a home directory defined, which is required for z/OSMF.

By default, the ISPF task is setup to use the logon procedure IKJACCNT, which is supplied by IBM. A user can select to use a different logon procedure, as long as the user’s logon procedure is properly configured for ISPF.

Customizing for profile sharing

Some TSO/E users require the use of multiple ISPF sessions. For example, a user might need to:

- Log on simultaneously through a z/OSMF ISPF session and a telnet 3270 session, or
- Log on through multiple z/OSMF ISPF sessions (this is different than having split screens, which is also allowed).
If you plan to allow the use of multiple ISPF sessions, the user’s logon procedure must be configured to allow profile sharing. This option avoids enqueue lock outs and loss of profile updates when the same profile data set is used for concurrent ISPF sessions. With profile sharing enabled, the user’s logon procedure is required to allocate ISPF profile data sets with the disposition SHARED, rather than NEW, OLD, or MOD, and the data sets must already exist. Or, these data sets must be temporary data sets. For more information, see the topic on profile sharing in z/OS ISPF Planning and Customizing.

Profile sharing is only effective if enabled for each concurrent ISPF session. This includes running a 3270 z/OS ISPF session at the same time as a z/OSMF ISPF session. For a 3270 z/OS ISPF session, invoke ISPF with the SHRPROF option. For a z/OSMF ISPF session, select Profile Sharing “On” from the z/OSMF ISPF User Settings panel. If you intend to run ISPF by using a 3720 z/OS ISPF session and also with a z/OSMF ISPF session using the same user ID, specify the value of “YES” for the keyword PROFILE_SHARING in the ISPF Configuration Table. Then SHRPROF becomes the default option for the ISPF or ISPSTART command.

Otherwise, the default for the 3270 ISPF command is EXCLPROF which will prevent profile sharing between a z/OSMF ISPF user and a 3270 instance of the same user.

**Assigning the TRUSTED attribute to CEA**

To allow the CEA TSO/E address space manager to access or create any resource it needs, the CEA started task requires the TRUSTED(YES) attribute to be set on the RDEFINE STARTED CEA.* definition.


**Customizing for reconnecting user sessions**

For potentially faster logons for users of the ISPF task, you can customize your z/OS system to allow the use of reconnectable user sessions. Here, the user session is deactivated after log-off is requested, but the user is not logged off. Instead, the system maintains the session for a period of time so that the user can reconnect to it. Reconnecting to a session is faster and uses fewer resources than creating a new session because the session resources are retained and reused when the user reconnects to the session.

To set up this capability in z/OS, the common event adapter (CEA) component must have certain controls set. See the description of the CEA parmlib member, CEAPRMxx, in z/OS MVS Initialization and Tuning Reference, SA22-7592, specifically, the descriptions of the RECONTIME and RECONSESSIONS statements. By default, reconnectable user sessions are not enabled.
System prerequisites for the Resource Monitoring plug-in

This section describes the system setup actions required for using the Resource Monitoring and System Status tasks.

If you plan to use the Resource Monitoring and System Status tasks, see Table 3 for the z/OS system changes that are required or recommended. This work might already be done on your system, or might not be applicable. If so, you can skip the particular setup action.

**Note:** If you use RMF XP, the RACF profile name for the RMF XP DDS is GPM4CIM. Use this profile name instead of GPMSERVE when you complete Steps 2 and 3 in the following procedure. For information about setting up RMF XP, see z/OS RMF User’s Guide SC33-7990.

Table 3. z/OS setup actions for the Resource Monitoring and System Status tasks

<table>
<thead>
<tr>
<th>z/OS setup action</th>
<th>Check when task is completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enable the optional priced feature, Resource Measurement Facility (RMF), on one of the systems in your enterprise. For information about enabling features, see z/OS Planning for Installation GA22-7504.</td>
<td></td>
</tr>
<tr>
<td>2. For data collection and monitoring of your systems, ensure that the RMF distributed data server (DDS) is active on one of the systems in your sysplex. To monitor several sysplexes, ensure that a DDS is running on one system in each sysplex. You can use the following command to check for the existence of any GPMSERVE address spaces in your sysplex: ROUTE *ALL,D A,GPMSERVE or ROUTE <em>ALL,D A,GPM</em>. For more information about setting up the DDS server, see z/OS RMF User’s Guide SC33-7990.</td>
<td></td>
</tr>
<tr>
<td>3. Determine whether the RMF Distributed Data Server (DDS) is configured to require authentication. You can use the following command to display the active DDS options: MODIFY GPMSERVE,OPTIONS. In the command output, the HTTP_NOAUTH statement indicates the scope of authentication for the DDS, as follows: HTTP_NOAUTH0 All hosts must authenticate HTTP_NOAUTH(<em>) No authentication is required. HTTP_NOAUTH(specific_host_or_mask) All hosts except those matching the mask must authenticate. Perform one of the following tasks, as appropriate: • If your installation requires the authentication feature of the DDS: Ensure that the PassTicket is set up properly, and that the WebSphere Application Server servant user ID is authorized to generate PassTickets. This setup can be done after configuring z/OSMF. See “Updating z/OS for the Resource Monitoring plug-in” on page 85. • If your installation does not require the authentication feature of the DDS: It is recommended that you disable DDS authentication. Doing so allows the Resource Monitoring and System Status tasks to access the DDS on behalf of z/OSMF users without encountering authentication errors. To disable DDS authentication, modify the HTTP_NOAUTH statement in the GPMSRVxx parmlib member to bypass authentication for all users, as follows: HTTP_NOAUTH(</em>) Alternatively, you can bypass DDS authentication for the system on which z/OSMF is running (the server host name or IP address). In the following example, the HTTP_NOAUTH statement requires all hosts to require DDS authentication, with the exception of the specified host system host_system_IP_address: HTTP_NOAUTH(host_system_IP_address) For information about authentication for the DDS server, see z/OS RMF User’s Guide SC33-7990.</td>
<td></td>
</tr>
</tbody>
</table>
System prerequisites for the Software Deployment plug-in

No system customization is required to enable the Deployment task.

Optional: If you want to manage the priority of work performed by the Deployment task, your installation can define a Workload Manager transaction class to manage the execution of long-running work. This step is recommended.

Using the z/OSMF Workload Management task or the WLM ISPF Administration Application, add a classification rule for subsystem CB (Component Broker) to your WLM service definition. Specify qualifier type transaction class (TC) and qualifier name IZUGWORK for the classification rule and assign a service class with a goal of either discretionary or low velocity. The subject service class should not have multiple periods and should not have a response time goal. Also, create a report class specific for the IZUGWORK transaction class, for example, RIZUGWRK, and assign it to the classification rule, so that you can obtain a separate report on the actual usage of the Deployment task long-running work.

If your installation is running a System z Application Assist Processor (zAAP), and if IFAHONORPRIORITY is set to YES in the IEAOPTxx member of parmlib, discretionary work is not permitted to use a general central processor (GCP). If this processing style is desired, use a discretionary goal. To allow the work to cross-over to a GCP if the zAAP capacity is exhausted, use a low velocity goal.

For more information on WLM, see z/OS MVS Planning Workload Management, SA22-7602, and the WLM web page at: http://www.ibm.com/systems/z/os/zos/features/wlm

For sample WLM policy definitions, see the IBM z/OS WLM Sample WLM Service Policy Definition web page at: http://www.ibm.com/systems/z/os/zos/features/wlm/documents/sample/samplepol.html

For information about the IEAOPTxx member of parmlib, see z/OS MVS Initialization and Tuning Reference SA22-7592.

Additional customization steps for the Software Deployment plug-in

Later, after configuring the z/OSMF product on your system, you might need to perform additional system customization for the Software Deployment plug-in. This work is required if you want to allow the Deployment task to work with systems on other sysplexes in your installation. For the steps to follow, see “Updating z/OS for the Software Deployment plug-in” on page 86.
System prerequisites for the Workload Management plug-in

To use the Workload Management task, your installation must perform the system setup steps described in this section.

Table 4 summarizes the z/OS system changes that are required or recommended for enabling the Workload Management task. Some or all of this work might already be done on your system, if so, you can skip the particular setup action. For assistance with these setup actions, see the procedures referenced in the Where described column of Table 4.

Table 4. z/OS setup actions for the Workload Management task

<table>
<thead>
<tr>
<th>z/OS setup action</th>
<th>Where described</th>
<th>Check when task is completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Ensure that the Common Information Model (CIM) server is configured on your</td>
<td>CIM includes jobs to help you perform these tasks (CFZSEC and CFZRCUST). See</td>
<td></td>
</tr>
<tr>
<td>system, including security authorizations and file system customization.</td>
<td>the chapter on CIM server quick setup and verification in z/OS Common Information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can perform this work during the configuration process; see “Ensure that the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>z/OSMF administrator is authorized to the CIM server” on page 71.</td>
<td></td>
</tr>
<tr>
<td>2. Ensure that library BLDUXTID in SYS1.MIGLIB is program controlled. For</td>
<td>This step is performed in the CIM provided job CFZSEC. See the chapter on</td>
<td></td>
</tr>
<tr>
<td>example, in a RACF system, you can use the following commands to ensure that a</td>
<td>customizing the security for the CIM server in z/OS Common Information Model</td>
<td></td>
</tr>
<tr>
<td>RDEFINE PROGRAM BLDUXTID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RALT PROGRAM BLDUXTID +</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ADDMEM('SYS1.MIGLIB'/'******'/'NOPADCHK') +</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UACC(READ)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SETROPTS WHEN(PROGRAM) REFRESH</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Additional customization steps for the Workload Management plug-in

For help with creating user authorizations to the WLM resources on your system, see “Updating z/OS for the Workload Management plug-in” on page 95.
The configuration process

The shell scripts that are provided with z/OSMF are invoked in and use the z/OS UNIX System Services environment for proper execution. The scripts are supplied in a specific location that was determined at SMP/E installation time. The default path to this location is already defined to the scripts.

In z/OSMF V1R13, the default path is /usr/lpp/zosmf/V1R13. If this location is different on your system, you will need to set an environment variable, IZU_CODE_ROOT, in the shell before invoking the scripts. Because this variable represents a path, throughout this document, references to the path use the following convention: <IZU_CODE_ROOT>/bin refers to the path /usr/lpp/zosmf/V1R13/bin.

Similarly, the variable IZU_CONFIG_DIR represents the path for the configuration directory, which is by default /etc/zosmf. For the log file directory, the variable IZU_LOGFILE_DIR is used, and the default is /var/zosmf/configuration/logs.

Following are the main components of the z/OSMF configuration process:

izusetup.sh
The shell script, with several options, that is used to configure z/OSMF. You can run this script interactively or "quietly" (the fastpath mode), as you prefer. This script is located in the /bin subdirectory of the product file system: <IZU_CODE_ROOT>/bin.

izudflt.cfg
The configuration file that is shipped with z/OSMF. This file contains IBM-supplied configuration values that can be used as input to a base configuration. This file is located in the /defaults subdirectory of the product file system, by default: <IZU_CODE_ROOT>/defaults. Do not edit the IBM-supplied configuration file.

izudflt.ovr
The optional override file that is used to replace any of the settings found in the configuration file. A default copy of this file is located in the /defaults subdirectory of the product file system, by default: <IZU_CODE_ROOT>/defaults.

izu_env.sh
The optional environment variables file that can be used to modify the session defaults that are in effect when you run the shell script. A default copy of this file is located in the /defaults subdirectory of the product file system, by default: <IZU_CODE_ROOT>/defaults.

The z/OSMF configuration process occurs in four stages:

Configuration stage
You run a shell script to create a file of configuration settings for your z/OS system. The script requires that you provide input about your environment and the z/OSMF plug-ins that you plan to configure. You can change any values that are not appropriate for your system environment. The script saves your information as variables in the configuration file, which is used as input for subsequent steps in the configuration process.

Security setup stage
The configuration process generates a REXX language program (an exec) that contains RACF commands for security definitions and setup. This exec is specific to your system and contains information gathered during the
configuration stage. Your security administrator should review the exec before submitting it. If your system uses a security management product other than RACF, your security administrator can refer to the generated exec for examples when creating equivalent authorizations for your system.

**Priming stage**
During this part of the process, you run a shell script to initialize or "prime" the z/OSMF data file, and perform some or all of the following types of system customization, as applicable: Allocation and mounting of file systems, updates to parmlib, creating z/OSMF directories, and setting the ownership and permission of these directories.

**Deployment stage**
The configuration process uses the configuration file that was created in the configuration stage to deploy z/OSMF on your system.

**Authorizations needed during the configuration process**
To begin the configuration process, you need a user ID with superuser authority. This authority allows the izusetup.sh script to perform the following tasks on your system:

- Create directories
- Allocate and mount the z/OSMF data file system
- Change directory ownership and permissions.

There are three ways to assign superuser authority in z/OS:

- Using the UNIXPRIV class profiles, which is the recommended way.
- Using the BPX.SUPERUSER resource in the FACILITY class.
- Assigning a UID of 0, which is the least desirable way.

For information about how to define a user with superuser authority (a superuser), see [z/OS UNIX System Services User’s Guide](SA22-7801). For a list of the resource names available in the UNIXPRIV class, the z/OS UNIX privilege associated with each resource, and the level of access required to grant the privilege, see [z/OS UNIX System Services Planning](GA22-7800).

Besides superuser authority, the user of the izusetup.sh script requires update authority to the parmlib data set for any members that are modified during the z/OSMF configuration process.

Table 5 shows the performer for each step of the z/OSMF configuration process.

<table>
<thead>
<tr>
<th>Step to perform</th>
<th>Script invocation or action</th>
<th>Performed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Step 1: Create the initial configuration&quot; on page 65</td>
<td>izusetup.sh -file izuconfig1.cfg -config [...other options...]</td>
<td>Superuser</td>
</tr>
<tr>
<td>&quot;Step 2: Run the security commands&quot; on page 69</td>
<td>&lt;IZU_CONFIG_DIR&gt;/izuconfig1.cfg.rexx</td>
<td>Security administrator</td>
</tr>
<tr>
<td>&quot;Step 3: Verify the RACF security setup&quot; on page 72</td>
<td>izusetup.sh -file izuconfig1.cfg -verify racf</td>
<td>Security administrator</td>
</tr>
<tr>
<td>&quot;Step 4: Prime the z/OSMF data file system&quot; on page 73</td>
<td>izusetup.sh -file izuconfig1.cfg -prime</td>
<td>Superuser</td>
</tr>
<tr>
<td>&quot;Step 5: Complete the setup&quot; on page 75</td>
<td>izusetup.sh -file izuconfig1.cfg -finish</td>
<td>z/OSMF administrator</td>
</tr>
<tr>
<td>&quot;Step 6: Access the z/OSMF Welcome task&quot; on page 77</td>
<td>At the end of the z/OSMF configuration process, you can verify the success of your configuration actions by opening a web browser to the z/OSMF Welcome task.</td>
<td>z/OSMF administrator</td>
</tr>
</tbody>
</table>
Using an override file

You can choose to supply some of your configuration settings in an editable file called the override file. The values in the override file will override the IBM defaults for any properties that you specify.

Your override file does not need to have the complete set of properties required for z/OSMF configuration. Rather, it should contain the properties that are most likely to be modified by your installation. This approach allows you to gather your installation values in one place (the override file) and have this file serve as input to the configuration process.

As an added benefit, you might find that having an override file provides you with a convenient means for gathering and reviewing configuration data at your installation before proceeding with the z/OSMF configuration.

During the configuration process, specify the override file as input to the configuration script. In response, the configuration process presents your override file values as defaults for the script prompts for any properties specified in the override file. Press Enter to accept each value, or type an alternative value, as needed.

If you provide an override file, you must ensure that the variables specified in the override file are set to valid values for your installation. Some variables are initially set to the following value, which is not a valid setting: NO.DEFAULT.VALUE. If these variables are not set to valid values, you must manually update the override file before invoking the izusetup.sh script to perform the configuration.

For the content of the override file that is supplied with z/OSMF, see Appendix D, "Default configuration file and default override file," on page 255.

Choosing a script mode: Interactive or fastpath

To provide your configuration settings to z/OSMF, you run the shell script, izusetup.sh with the -config option. You can run the script either interactively or "quietly" using the fastpath option. In either mode, this script starts with the settings contained in the specified configuration file, and can accept an optional override file that overrides these settings.

When used in interactive mode, the izusetup.sh script presents you with a series of prompts, one for each z/OSMF configuration parameter. All prompts require a response; either an acceptance of the displayed value, or a value that you enter in response to the prompt. When you use the interactive mode, you have an opportunity to change the value in response to the prompt.

When used in fastpath mode, the izusetup.sh script runs without any interactive prompting. Any values not found in the override file are taken from the configuration file. If a value is not found in either location, the script ends with an error.

Regardless of which mode you use (interactive or fastpath), the izusetup.sh script saves the values in an updated configuration file, to be used as input to subsequent phases of the configuration process. Further, the same configuration file
can be used as input when configuring z/OSMF on other systems in your enterprise, thus saving you time and data entry effort.

If your prefer to supply the input data interactively, run the `izusetup.sh` script in interactive mode. If you prefer to supply the input data by editing a file rather than responding to a series of prompts, run the script in fastpath mode.

Table 6 summarizes the considerations for each mode.

<table>
<thead>
<tr>
<th>Script mode</th>
<th>Resulting behavior</th>
<th>When to use this mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interactive mode (without an override file)</td>
<td>Script prompts you for configuration values, displaying the values from the configuration file as defaults.</td>
<td>You have determined that most of the IBM-supplied defaults are appropriate for your installation, and you would prefer to supply the few needed modifications interactively in response to script prompts. Note that some values have no IBM defaults; these always require your input.</td>
</tr>
<tr>
<td>Interactive mode (with an override file)</td>
<td>Script prompts you for configuration values, displaying the values from your override file as defaults. Values not found in the override file are taken from the specified configuration file. In response to each prompt, you must either press Enter to accept your installation-specific value, or type a new value.</td>
<td>You want the configuration session to be preset with your installation-specific values. This method saves you from having to enter your values interactively in response to script prompts. Instead, you need only review each value displayed by the script and press Enter to accept it.</td>
</tr>
<tr>
<td>Fastpath mode (with an override file)</td>
<td>Script runs to completion without any interactive prompting. Values are used as supplied in the specified override file. Any values not found in the override file are taken from the configuration file. If a value is not found in either location, the script ends with an error message indicating the first value that could not be found.</td>
<td>You prefer to supply your data in a standalone file, and have no need to review the values interactively. You have verified that all of the necessary configuration data is supplied through the configuration file, or the optional override file, or a combination of both files. Or, you need to re-run the configuration process to update an erroneous value in an existing configuration file, and do not want to repeat the prompts. More information about this technique is provided in “If you need to repeat Step 1, use the -fastpath option” on page 69.</td>
</tr>
</tbody>
</table>

Planning worksheets for z/OSMF

Use the worksheets in this section as a guide for planning your input to the `izusetup.sh -config` script. Each worksheet entry includes a description of the input variable, its default value (if any), and a space to record your own value in case you do not want to use the default.

To save time during the configuration process, have this information at hand when you perform the steps in Chapter 4, “Configuring z/OSMF,” on page 61. The amount of information you need to gather depends on which plug-ins your installation plans to configure in addition to the core functions of z/OSMF.

The following planning worksheets are included:

- “Input for the core functions” on page 36
Input for the core functions

This topic provides the planning worksheet for configuring the core functions of z/OSMF.

Input for the script prompts and override file

Configuring the z/OSMF core functions requires that you have the following information available. This table includes the variable names and defaults, if any, for these values. Gathering some of this information might require the assistance of your installation’s security administrator.

Some values require that you provide a unique UID or GID. As an alternative to specifying these identifiers, you can specify the AUTOUID or AUTOGID operand to have RACF automatically generate a unique ID for you. To request RACF generated IDs for all of the settings that require a UID or GID, specify the values IZU_AUTOGID_OVERRIDE=Y and IZU_AUTOUID_OVERRIDE=Y, as needed. Doing so avoids the need to specify IDs for individual variables. For more information about the AUTOUID and AUTOGID operands, see z/OS Security Server RACF Security Administrator’s Guide SA22-7683.

Table 7. Worksheet for the core functions variables

<table>
<thead>
<tr>
<th>Input</th>
<th>Description</th>
<th>Variable name</th>
<th>Default value</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mount point of the z/OSMF data file system.</td>
<td>Mount point (the fully-qualified path name) for the z/OSMF data file system. The data file system is identified by the IZU_DATA_FS_NAME variable.</td>
<td>IZU_DATA_DIR</td>
<td>/var/zosmf/data</td>
<td></td>
</tr>
<tr>
<td>Name of the z/OSMF data file system.</td>
<td>z/OSMF data file system.</td>
<td>IZU_DATA_FSNAMESPACE</td>
<td>IZU.SIZUDATA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you pre-create the data file system, ensure that IZU_DATA_FS_NAME is set to your file system name. This file system must be mounted at the IZU_DATA_DIR mount point (do this manually or allow the configuration script to mount it for you).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>z/OSMF data file system type.</td>
<td>Type of file system (zFS or HFS) to be used for creating the z/OSMF data file system.</td>
<td>IZU_DATA FS_TYPE</td>
<td>ZFS</td>
<td></td>
</tr>
<tr>
<td>Input</td>
<td>Description</td>
<td>Variable name</td>
<td>Default value</td>
<td>Your value</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>---------------</td>
<td>------------</td>
</tr>
<tr>
<td>Volume name for the z/OSMF data file system, or SMS-managed storage.</td>
<td>Volume serial number (VOLSER) of the DASD to be used for creating the z/OSMF data file system. Specify the VOLSER (without single quotes) to specify a volume, or specify &quot;<em>&quot; (with single quotes) to let SMS select the volume. Using &quot;</em>&quot; requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle data set allocation automatically, list the volume explicitly. If you specify a volume, the volume must be online when you begin the configuration process described in Chapter 4, &quot;Configuring z/OSMF,&quot; on page 61.</td>
<td>IZU_DATA_FS_VOLUME</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>Allocation size (in cylinders) for the z/OSMF data file system.</td>
<td>Initial space allocation, in cylinders, for the z/OSMF data file system data set. The script uses 90% of this value for the primary allocation and 10% for the secondary allocation. The minimum suggested size (and default) is 200 cylinders, which causes the script to use 180 cylinders for the primary allocation and 20 cylinders for the secondary allocation.</td>
<td>IZU_DATA_FS_SIZE</td>
<td>200</td>
<td></td>
</tr>
<tr>
<td>Authorization mode.</td>
<td>Authorization mode to be used for this z/OSMF configuration. The valid modes are: • SAF. Security is based entirely on profiles and groups defined in your security product. SAF mode is the default. • REPOSITORY. Security is based on the user and role selections defined in z/OSMF. This value must be entered in uppercase characters. For information about the authorization modes for z/OSMF, see &quot;Authorization modes for z/OSMF&quot; on page 50.</td>
<td>IZU_AUTHORIZATION_MODE</td>
<td>SAF</td>
<td></td>
</tr>
<tr>
<td>AUTOID override</td>
<td>If you have AUTOID enabled, this variable indicates whether (Y or N) RACF is to assign unused UIDs for all group IDs required during the configuration process. If this variable is set to Y, the other prompts for UID are suppressed.</td>
<td>IZU_AUTUID_OVERRIDE</td>
<td>NO.DEFAULT.VALUE</td>
<td>You must provide a value for this.</td>
</tr>
</tbody>
</table>
### Table 7. Worksheet for the core functions variables (continued)

<table>
<thead>
<tr>
<th>Input</th>
<th>Description</th>
<th>Variable name</th>
<th>Default value</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTOGID override</td>
<td>If you have AUTOGID enabled, this variable indicates whether (Y or N) RACF is to assign unused GIDs for all group IDs required during the configuration process. If this variable is set to Y, other prompts for GID are suppressed.</td>
<td>IZU_AUTOGID_OVERRIDE</td>
<td>NO.DEFAULT.VALUE</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>You must provide a value for this.</td>
</tr>
<tr>
<td>Group name for the z/OSMF administrator.</td>
<td>The default group used when creating the z/OSMF administrator user ID. If your installation has selected SAF Authorization Mode for this configuration, this group name is used in association with the z/OSMF Administrator.</td>
<td>IZU_ADMIN_GROUP_NAME</td>
<td>IZUADMIN</td>
<td></td>
</tr>
<tr>
<td>Group GID for the z/OSMF administrator or AUTOGID.</td>
<td>Group ID (GID) for the z/OSMF administrator group. Instead of specifying the GID value, you can enter AUTOGID to have RACF automatically generate a unique ID. For more information about the AUTOGID operand, see z/OS Security Server RACF Security Administrator's Guide, SA22-7683.</td>
<td>IZU_ADMIN_GROUP_GID</td>
<td>9003</td>
<td></td>
</tr>
<tr>
<td>Group name for the z/OSMF users.</td>
<td>This group is used in both Repository Authorization Mode and SAF Authorization mode. The use varies depending on the mode; for more information, see Chapter 3, “Planning security for z/OSMF,” on page 49.</td>
<td>IZU_USERS_GROUP_NAME</td>
<td>IZUUSER</td>
<td></td>
</tr>
<tr>
<td>Group ID (GID) for z/OSMF users.</td>
<td>Group ID (GID) for the z/OSMF user group.</td>
<td>IZU_USERS_GROUP_GID</td>
<td>9004</td>
<td></td>
</tr>
<tr>
<td>z/OSMF administrator user ID.</td>
<td>Default user ID for the z/OSMF administrator.</td>
<td>IZU_ADMIN_NAME</td>
<td>ZOSMFAD</td>
<td></td>
</tr>
<tr>
<td>z/OSMF administrator UID or AUTOUID.</td>
<td>UID for the z/OSMF administrator. Instead of specifying the UID value, you can enter AUTOUID to have RACF automatically generate a unique ID. For more information about the AUTOUID operand, see z/OS Security Server RACF Security Administrator's Guide, SA22-7683.</td>
<td>IZU_ADMIN_UID</td>
<td>9001</td>
<td></td>
</tr>
</tbody>
</table>
Table 7. Worksheet for the core functions variables (continued)

<table>
<thead>
<tr>
<th>Input</th>
<th>Description</th>
<th>Variable name</th>
<th>Default value</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>z/OSMF administrator home directory.</strong></td>
<td>Home directory for the z/OSMF administrator. In many installations, this value should be replaced with an alternative directory. If so, specify a value that corresponds with the value you specify for the IZU_ADMIN_NAME variable. For example, if you specify the value ZOSMFAD for IZU_ADMIN_NAME, the IZU_ADMIN_HOME should be set to /u/zosmfad. Do not specify a home directory to be created under the mount point of the z/OSMF data file system, which by default is /var/zosmf/data. The mount point owner and group permissions do not allow the z/OSMF administrator ID access.</td>
<td>IZU_ADMIN_HOME</td>
<td>/u/zosmfad</td>
<td></td>
</tr>
<tr>
<td><strong>z/OSMF administrator shell program path.</strong></td>
<td>Program path for the z/OSMF administrator identity for z/OS UNIX system services. This value is used for the OMVS segment.</td>
<td>IZU_ADMIN_PROGRAM</td>
<td>/bin/sh</td>
<td></td>
</tr>
<tr>
<td><strong>z/OSMF administrator proc name.</strong></td>
<td>TSO/E logon procedure to be used by the z/OSMF administrator.</td>
<td>IZU_ADMIN_PROC</td>
<td>NO.DEFAULT.VALUE</td>
<td>You must provide a value for this.</td>
</tr>
<tr>
<td><strong>z/OSMF administrator account number.</strong></td>
<td>User account number for z/OSMF administrator identity.</td>
<td>IZU_ADMIN_ACCOUNT</td>
<td>NO.DEFAULT.VALUE</td>
<td>You must provide a value for this.</td>
</tr>
<tr>
<td><strong>WebSphere Application Server configuration file exists.</strong></td>
<td>The WebSphere Application Server response file exists and is available to be used as input to the z/OSMF configuration process. Your installation created this file when customizing IBM WebSphere Application Server OEM Edition for z/OS for this system. This file is described in IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide GA32-0631. If this file is not available, set this value to N. The configuration process prompts you for the WebSphere values individually (see Appendix E “Values from the WebSphere Application Server response file,” on page 261).</td>
<td>IZU_WAS_CONFIG_FILE_KNOWN</td>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>

Chapter 2. Planning for the z/OSMF configuration process  39
Table 7. Worksheet for the core functions variables  (continued)

<table>
<thead>
<tr>
<th>Input</th>
<th>Description</th>
<th>Variable name</th>
<th>Default value</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory path and name of the WebSphere Application Server configuration file.</td>
<td>Fully-qualified path name of the WebSphere Application Server response file. If you omit this value, the configuration process prompts you for the WebSphere values individually (see Appendix E, &quot;Values from the WebSphere Application Server response file,&quot; on page 261).</td>
<td>IZU_WAS_CONFIG_FILE_LOCATION</td>
<td>/etc/zWebSphereOEM/V7R0/conf/CONFIG1/CONFIG1.responseFile</td>
<td></td>
</tr>
<tr>
<td>Path of the WBEM root directory</td>
<td>Root directory path of the CIM server installation. Because it is usually not necessary to modify this value, this variable is not included in the override file that is supplied with z/OSMF If an override is required, you can copy this variable with a modified value to the override file you plan to use.</td>
<td>IZU_WBEM_ROOT</td>
<td>/usr/lpp/wbem</td>
<td></td>
</tr>
</tbody>
</table>

Planning your plug-in selections

The system management tasks in z/OSMF are provided through optional plug-ins, which you enable when you configure the product. To add plug-ins to z/OSMF, you must determine which plug-ins are needed for your installation. In general, you should configure all of the available plug-ins during the z/OSMF configuration process.

For your planning purposes, Table 8 shows the information you should have at hand when running the configuration script. This table includes the variable names for these values. Depending on which plug-ins you choose to configure, there might be additional prompts specific to those plug-ins. If you select plug-ins in response to script prompts (because you run the izusetup.sh script in interactive mode), you can select plug-ins by specifying one or more plug-in identifiers, which are shown in the ID column of the table.

Table 8. Worksheet for planning your plug-in selections

<table>
<thead>
<tr>
<th>Input</th>
<th>ID</th>
<th>Description</th>
<th>Variable name</th>
<th>Default value</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Incident Log plug-in (Y/N)?</td>
<td>1</td>
<td>Indicates whether (Y or N) the Incident Log plug-in is to be included in z/OSMF.</td>
<td>IZU_IL_CONFIGURE</td>
<td>NO.DEFAULT.VALUE</td>
<td></td>
</tr>
<tr>
<td>Configure Configuration Assistant plug-in (Y/N)?</td>
<td>2</td>
<td>Indicates whether (Y or N) the Configuration Assistant plug-in is to be included in z/OSMF.</td>
<td>IZU_CA_CONFIGURE</td>
<td>NO.DEFAULT.VALUE</td>
<td></td>
</tr>
<tr>
<td>Configure Workload Management plug-in (Y/N)?</td>
<td>3</td>
<td>Indicates whether (Y or N) the Workload Management plug-in is to be included in z/OSMF.</td>
<td>IZU_WLM_CONFIGURE</td>
<td>NO.DEFAULT.VALUE</td>
<td></td>
</tr>
<tr>
<td>Configure Resource Monitoring plug-in (Y/N)?</td>
<td>4</td>
<td>Indicates whether (Y or N) the Resource Monitoring plug-in is to be included in z/OSMF.</td>
<td>IZU_RMF_CONFIGURE</td>
<td>NO.DEFAULT.VALUE</td>
<td></td>
</tr>
</tbody>
</table>
Table 8. Worksheet for planning your plug-in selections  (continued)

<table>
<thead>
<tr>
<th>Input Description</th>
<th>Variable name</th>
<th>Default value</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Capacity Provisioning plug-in (Y/N)?</td>
<td>IZU_CP_CONFIGURE</td>
<td>NO.DEFAULT.VALUE</td>
<td></td>
</tr>
<tr>
<td>Configure Deployment plug-in (Y/N)?</td>
<td>IZU_DM_CONFIGURE</td>
<td>NO.DEFAULT.VALUE</td>
<td></td>
</tr>
<tr>
<td>Configure ISPF plug-in (Y/N)?</td>
<td>IZU_WISPF_CONFIGURE</td>
<td>NO.DEFAULT.VALUE</td>
<td></td>
</tr>
</tbody>
</table>

**Input for the Capacity Provisioning task**

If you choose to deploy the Capacity Provisioning plug-in, and your z/OSMF configuration is running in SAF Authorization Mode, you must provide additional information to the `izusetup.sh` script.

For your planning purposes, Table 9 shows the information you should have at hand when running the configuration script. Here, you must supply the names of the security groups that your installation has created for authorizing users to the Provisioning Manager on your system. Table 9 includes the variable names and defaults for these values. For more information about the Capacity Provisioning security groups, see the [z/OS MVS Capacity Provisioning User’s Guide](#). SC33-8299.

These variables are used only when z/OSMF is running in SAF Authorization Mode. If you choose not to deploy the Capacity Provisioning plug-in, or your z/OSMF configuration is running in Repository Authorization Mode, you can skip this planning worksheet.

Table 9. Worksheet for the Capacity Provisioning task variables

<table>
<thead>
<tr>
<th>Input Description</th>
<th>Variable name</th>
<th>Default value</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning Manager query security group.</td>
<td>IZU_CP_QUERY_GROUP_NAME</td>
<td>CPOQUERY</td>
<td></td>
</tr>
<tr>
<td>Provisioning Manager control security group.</td>
<td>IZU_CP_CONTROL_GROUP_NAME</td>
<td>CPOCTRL</td>
<td></td>
</tr>
</tbody>
</table>

**Input for the Incident Log task**

If you choose to deploy the Incident Log plug-in, you must provide additional information to the `izusetup.sh` script.
For your planning purposes, Table 10 shows the information you should have at hand when running the configuration script. Table 10 includes the variable names and defaults, if any, for these values. If you choose not to deploy the Incident Log plug-in, you can skip this planning worksheet.

Table 10. Worksheet for the Incident Log task variables

<table>
<thead>
<tr>
<th>Input</th>
<th>Description</th>
<th>Variable name</th>
<th>Default value</th>
<th>Your value</th>
</tr>
</thead>
</table>
| Do you want to enable the common event adapter (CEA) component and update related parmlib options for using the Incident Log task? | Indicates whether (Y or N) the script is to enable the common event adapter (CEA) component and update related parmlib options for using the Incident Log task.  
- If you reply Y, you are prompted for additional values for setting up your system for the Incident Log. The system changes include initializing a CEAPRMxx parmlib member with options set for Incident Log processing.  
- If you reply N, you are responsible for performing this setup before users can begin using the Incident Log task. The script will not prompt you for the CEA related values that follow. | IZU_IL_CEA_CONFIGURE | Y | |
| HLQ of the CEA data sets. | The high level qualifier to be used for CEA data sets, as defined in the CEAPRMxx parmlib member. This HLQ is used for the associated dump data sets. This value is one to four characters. | IZU_CEA_HLQ | CEA | |
| Country code. | IBM-defined country code for your site (3-character alphanumeric). | IZU_COUNTRY_CODE | NO.DEFAULT.VALUE | You must provide a value for this. |
| Branch. | IBM-defined branch code (or branch office) for your site (3-character alphanumeric). | IZU_BRANCH_CODE | NO.DEFAULT.VALUE | You must provide a value for this. |
| What STORAGE option do you want to use? | Indicates the volumes or a SMS STORAGE class to be used by CEA for storing diagnosis snapshots.  
- Enter V to specify one or more volumes.  
- Enter S to specify an SMS storage class.  
In response, the script prompts for each volume (up to seven) or a single storage class name. Specify each value on a separate line as prompted. | IZU_STORAGE_VALUE | NO.DEFAULT.VALUE | You must provide a value for this. |
### Table 10. Worksheet for the Incident Log task variables (continued)

<table>
<thead>
<tr>
<th>Input</th>
<th>Description</th>
<th>Variable name</th>
<th>Default value</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source data set for the CEAPRM00 member.</td>
<td>Source data set that contains the IBM-supplied member, CEAPRM00. Usually, this is your SMPE-installed SYS1.PARMLIB data set. Ensure that the data set exists and is cataloged.</td>
<td>IZU_CEAPRM_SOURCE_PARMLIB</td>
<td>SYS1.PARMLIB</td>
<td></td>
</tr>
<tr>
<td>Target data set for saving the new CEAPRMnn member.</td>
<td>Target data set to use for creating the new CEAPRMnn member for Incident Log processing. This data set cannot be edited or allocated to a user or job when the izusetup.sh script is running. If you do not want your system's active parmlib data set to be updated directly by the configuration process, you can instead allow updates to be made to an interim or temporary parmlib data set. You can later manually copy from this interim place into the active parmlib data set.</td>
<td>IZU_CEAPRM_TARGET_PARMLIB</td>
<td>SYS1.PARMLIB</td>
<td></td>
</tr>
<tr>
<td>Source data set for the Ieadmczm member.</td>
<td>Source data set for your existing Ieadmczm member. Usually, this is your SMPE-installed SYS1.SAMPLIB data set. Ensure that the data set exists and is cataloged.</td>
<td>IZU_IEADMC_SOURCE_PARMLIB</td>
<td>SYS1.SAMPLIB</td>
<td></td>
</tr>
<tr>
<td>Target data set for saving the new Ieadmczm member.</td>
<td>Target data set to use for creating the new Ieadmczm member for Incident Log processing. This data set cannot be edited or allocated to a user or job when the izusetup.sh script is running. If you do not want your system's active parmlib data set to be updated directly by the configuration process, you can instead allow updates to be made to an interim or temporary parmlib data set. You can later manually copy from this interim place into the active parmlib data set.</td>
<td>IZU_IEADMC_TARGET_PARMLIB</td>
<td>SYS1.PARMLIB</td>
<td></td>
</tr>
<tr>
<td>Suffix of the CEAPRMxx parmlib member.</td>
<td>Two-character suffix of a new CEAPRMxx parmlib member to be used for enabling captures or “snapshots” of the system logs. Two characters are required. If this member already exists, the script prompts you to choose whether to overwrite the existing member.</td>
<td>IZU_CEA_PARM_NAME</td>
<td>01</td>
<td></td>
</tr>
</tbody>
</table>
### Table 10. Worksheet for the Incident Log task variables (continued)

<table>
<thead>
<tr>
<th>Input</th>
<th>Description</th>
<th>Variable name</th>
<th>Default value</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suffix of the IEADMCxx parmlib member.</td>
<td>Two-character suffix of a new IEADMCxx parmlib member to be used for setting dump options. Two characters are required. If this member already exists, the script prompts you to choose whether to overwrite the existing member. If the IZU_IL_CEA_CONFIGURE variable is set to N, it is assumed that the IEADMCnn member already exists and resides in a concatenated parmlib data set; specify the member suffix on this variable. If the IEADMCnn member does not reside in the parmlib data set, you must place it there manually before running the izusetup.sh -verify script.</td>
<td>IZU_IEA_PARM_NAME</td>
<td>ZM</td>
<td></td>
</tr>
</tbody>
</table>

---

### Input for the Workload Management task

If you choose to deploy the Workload Management plug-in, you must provide additional information to the izusetup.sh script.

For your planning purposes, [Table 11](#) shows the information you should have at hand when running the configuration script. Here, you must supply the name of the security group that your installation has created for authorizing users to workload manager (WLM) resources on your system, such as the WLM couple data set. [Table 11](#) includes the variable name and default for this value.

If you choose not to deploy the Workload Management plug-in, you can skip this planning worksheet.

### Table 11. Worksheet for the Workload Management task variable

<table>
<thead>
<tr>
<th>Input</th>
<th>Description</th>
<th>Variable name</th>
<th>Default value</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group for accessing workload manager (WLM) resources.</td>
<td>Group name to use for allowing the Workload Management task to access WLM resources on your system. This group requires UPDATE access to facility MVSDADMIN.WLM.POLICY, as described in &quot;Controlling authorizations for the MVSDADMIN.WLM.POLICY facility&quot; on page 95. Your installation must create this group outside of the z/OSMF configuration process. If you do not plan to create this group, specify NO.KNOWN.VALUE for this group name.</td>
<td>IZU_WLM_GROUP_NAME</td>
<td>WLMGRP</td>
<td></td>
</tr>
</tbody>
</table>

---
Reviewing the z/OSMF advanced settings

z/OSMF includes a number of advanced settings that affect the behavior of the product. The configuration process obtains these settings from the file `izuadmin.env`, which is shipped with z/OSMF. For most typical configurations, the settings are correct and should not require modification. It is recommended, however, that you review the setting defaults to ensure that they are appropriate for your environment.

Table 12 describes the advanced settings that are used during the z/OSMF configuration process.

<table>
<thead>
<tr>
<th>izuadmin.env variable</th>
<th>Description</th>
<th>Allowable range of values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ltpatimeout</td>
<td>Amount of time (in minutes) for LTPA credentials to be forwarded between servers. z/OSMF user sessions expire when this period of time has elapsed. For information, see <a href="#">“Re-authenticating in z/OSMF” on page 79</a>.</td>
<td>25 – 359971</td>
<td>490</td>
</tr>
<tr>
<td>ltpacachetimeout</td>
<td>Amount of time (in seconds) for authentication settings to be held in cache. This value must be less than or equal to the ltpatimeout value multiplied by 60.</td>
<td>1500 – 2158260</td>
<td>29400</td>
</tr>
<tr>
<td>sessiontimeout</td>
<td>Amount of time (in minutes) for the session management session timeout. This value must be at least 5 greater than the ltpatimeout value.</td>
<td></td>
<td>495</td>
</tr>
<tr>
<td>izugwkmanwlmclass</td>
<td>WLM transaction class to be used for managing the execution of long-running work. This setting is applicable if your z/OSMF configuration includes the Software Deployment plug-in.</td>
<td>One to eight alphanumeric characters (A-Z, a-z, 0-9) or special characters (#, $, or @).</td>
<td>IZUGWORK</td>
</tr>
<tr>
<td>izuilunitvalue</td>
<td>Device to be used for storing data sets and z/OS UNIX files for the FTP jobs. This setting is applicable if your z/OSMF configuration includes the Incident Log plug-in.</td>
<td></td>
<td>SYSDA</td>
</tr>
<tr>
<td>izuiltempdirvalue</td>
<td>Temporary directory to be used for sending z/OS UNIX file attachments through FTP. This setting is applicable if your z/OSMF configuration includes the Software Deployment plug-in.</td>
<td></td>
<td>/tmp</td>
</tr>
</tbody>
</table>

A sample `izuadmin.env` file is supplied with z/OSMF in the following directory: `<IZU_CODE_ROOT>/defaults/`

where `<IZU_CODE_ROOT>` is the product file system. By default, this is `/usr/lpp/zosmf/V1R13/`.

If your installation currently uses a modified version of the `izuadmin.env` file, perhaps from a previous z/OSMF configuration, it is recommended that you make a backup copy of the file. Check for a modified version of the `izuadmin.env` file in the z/OSMF configuration directory and make note of any customized settings that should be preserved in the new copy. By default, the z/OSMF configuration...
To override any of the current settings, use this procedure:

1. Copy the file izuadmin.env from the directory <IZU_CODE_ROOT>/defaults to the directory <IZU_CONFIG_DIR>.

2. Edit the <IZU_CONFIG_DIR>/izuadmin.env file using an editor of your choice, updating the settings as needed.

To have your changes take effect as soon as z/OSMF is configured, make the changes before running the script described in “Step 5: Complete the setup” on page 75. If you later decide to change a setting, you can do so through the procedure described in Appendix E, “Modifying advanced settings for the z/OSMF configuration,” on page 263.

Preparing your workstation for z/OSMF

In preparing your workstation for use with z/OSMF, observe the considerations listed in this section.

- Your workstation requires a compatible operating system and web browser. For information, including usage considerations, see the z/OSMF Supported Browsers web page.
- The z/OSMF interface supports a minimum screen resolution of 1024 by 768 pixels. If your workstation is set to a lower resolution, you might experience some clipping of content.
- Ensure that your browser is enabled for JavaScript. For instructions, see Table 28 on page 146 or Table 29 on page 148 as appropriate.
- z/OSMF uses session cookies to track which users are logged in from a specific browser. If you want to allow multiple users to log in from a single location, or if you want the ability to log in to multiple servers from the same workstation, you might need to either launch another browser instance (as with Internet Explorer), or, configure another browser profile (as with Firefox). For information about creating Firefox profiles, see the Mozilla web site: http://www.mozilla.com
- If you plan to use the Internet Explorer browser to work with WLM service definitions, ensure that the browser is enabled for automatic prompting for file downloads. This setting prevents the file download blocker from being invoked when you download service definitions to your workstation. Otherwise, if automatic prompting is disabled (the default setting), the download blocker prompts you to accept these file downloads, causing your z/OSMF session to be reloaded and your active tabs to be closed. To avoid this disruption, enable automatic prompting for file downloads. For more information, see “Enabling automatic prompting for file downloads” on page 151.
- When using the Microsoft Internet Explorer 7 browser, you might experience slow responsiveness if you open multiple tabs, work with large WLM service definitions, or use the Resource Monitoring task for long periods of time. If so, consider using another supported browser to avoid this problem.

After you have configured z/OSMF, the product includes an environment checker tool that you can use to verify your browser and workstation settings at any time. For more information, see “Verifying your workstation with the environment checker” on page 144.
Planning a remote instance of z/OSMF

In some situations, you might need to create an instance of z/OSMF on another system in your sysplex. For example, you might do this to allow the Deployment task to work with systems on other sysplexes in your installation.

A key consideration is the need to manage the use of digital certificates in your installation. You can create a common certificate authority (CA) to be shared by both the primary instance of IBM WebSphere Application Server OEM Edition for z/OS and any secondary instances, but you must do this setup on the primary instance before creating the secondary instances. Or, if the secondary instances of IBM WebSphere Application Server OEM Edition for z/OS already exist, you must import their certificates into the primary instance.

For more information about sharing digital certificates, see "Configuring a primary z/OSMF for communicating with secondary instances" on page 93.

Planning a backup instance of z/OSMF

You can have only one active instance of z/OSMF in a sysplex at any given time. In some situations, however, you might choose to create more instances of z/OSMF on the same system or other systems in your sysplex. For example, you might want to have a backup instance of z/OSMF available for switchover or testing purposes.

For information about creating a backup instance of z/OSMF, see Chapter 8, "Multiple instances of z/OSMF," on page 111.

Planning service updates for z/OSMF

As with other IBM software products, IBM ships service for z/OSMF in the form of program temporary fixes or PTFs.

In planning for service updates, consider that z/OSMF consists of multiple functional modification identifiers (FMIDs):

- IBM WebSphere Application Server OEM Edition for z/OS is provided as one FMID
- z/OSMF core functions are provided as one FMID
- Each optional plug-in is provided as a separate FMID.

When handling service for these FMIDs, first complete the work for any PTFs you might have for IBM WebSphere Application Server OEM Edition for z/OS. Then, restart the IBM WebSphere Application Server OEM Edition for z/OS runtime instance before including the service from any other z/OSMF PTFs. Restarting IBM WebSphere Application Server OEM Edition for z/OS is required; failure to do so can leave the application server in an inconsistent state and cause subsequent z/OSMF maintenance to fail.

When working with PTFs for the z/OSMF core functions and plug-ins, check the PTF ++HOLD action for specific instructions for deploying the code, such as whether you must:

- Refresh any plug-ins
- Restart the IBM WebSphere Application Server OEM Edition for z/OS runtime instance.
Refreshing the plug-ins is done by running the izusetup.sh script with the -service option, which updates the product Enterprise Archive (EAR) files associated with the plug-ins. After you have applied the service for the PTFs, you need run this script only once to refresh the z/OSMF plug-ins for your configuration.

Information about using the izusetup.sh script with the -service option is provided in "Updating plug-ins after service is applied" on page 127.
Chapter 3. Planning security for z/OSMF

To perform work in z/OSMF, a user requires both a valid user ID on the z/OS system to be managed and authorization to one or more z/OSMF system management tasks on that system. This authorization can be handled through SAF interfaces on z/OS or through the administration tasks of z/OSMF. With the required security controls established on your system, a user can begin using z/OSMF to perform system management tasks.

Your installation determines which z/OS users will perform z/OSMF system management tasks, based on the z/OSMF plug-ins that you have chosen to deploy.

Security concepts in z/OSMF

As with other z/OS products and subsystems, security in z/OSMF is based on the concepts of user authentication and user authorization. User authentication occurs when a user attempts to log in to a system and the system's security management function examines the user's permission to do so. For z/OSMF, authentication occurs when the user attempts to log in to z/OSMF through a web browser. On log in, the user displays the z/OSMF Welcome page in the browser, and enters a z/OS user ID and password in the appropriate input fields. The login request is verified by the z/OS host system's security management product (for example, RACF) through the SAF interface. This processing ensures that the user ID is known to the z/OS system, and the password is valid.

Besides the ability to authenticate, a would-be z/OSMF user requires authorization to one or more z/OSMF resources (tasks and links), which is necessary before the user can do useful work in z/OSMF [Figure 12].

As of z/OSMF V1R13, z/OSMF supports user authorization in either of two modes: SAF Authorization Mode, which is based on SAF users and groups that your installation defines in its security management product, or Repository
Authorization Mode, in which your installation maintains user authorizations in z/OSMF itself. These modes are described in “Authorization modes for z/OSMF.”

To help with setting up security, z/OSMF includes scripts that can generate REXX programs with sample RACF commands for your installation. During the z/OSMF configuration process, your security administrator edits and runs one such REXX program to secure various resources on the z/OS system. After configuration, your security administrator runs another REXX program to authorize additional users to z/OSMF. If your installation uses a security management product other than RACF, your security administrator can refer to the REXX programs for examples when creating equivalent commands for the security management product on your system. The REXX programs are described later in this document.

z/OSMF also includes options for managing the access of guest users, that is, users who enter z/OSMF without authorization to tasks. Depending on how a guest user enters z/OSMF, the user is considered either authenticated or non-authenticated. A non-authenticated guest is a user who has displayed the welcome page, but has not logged in. An authenticated guest has logged in, but has not been granted authority to z/OSMF tasks.

**Authorization modes for z/OSMF**

z/OSMF supports two modes of user authorization: SAF Authorization Mode and Repository Authorization Mode.

The authorization modes are described, as follows:

- **SAF Authorization Mode.** z/OSMF user authorizations are managed by your security management product, such as RACF. Access to z/OSMF links and tasks is maintained through profiles in the ZMFAPLA resource class, which is new in z/OS V1R13. Here, authorizations are enabled when your security administrator defines groups, connects users to those groups, and permits those groups to the profiles that represent the z/OSMF tasks. This comprehensive form of security is called SAF Authorization Mode because it relies on traditional SAF interfaces to manage user authorizations, as is done today for most products and subsystems that run on z/OS. SAF Authorization Mode is the recommended and default authorization mode for z/OSMF.

- **Repository Authorization Mode.** z/OSMF user authorizations are managed internally by z/OSMF. This form of security is called Repository Authorization Mode because user authorizations are maintained in the z/OSMF repository, rather than in your security management product. Here, authorizations are created when the person who is designated as the z/OSMF Administrator assigns roles to users (through the Users page) and tasks to users (through the Roles page). Your installation is limited to the predefined roles of z/OSMF Administrator and z/OSMF User. You cannot modify these roles, or create additional roles.

In SAF Authorization Mode, your installation can define any number of user and group authorizations to z/OSMF resources. In Repository Authorization Mode, your installation is limited to the predefined roles that come with z/OSMF. During the z/OSMF configuration process, you select which authorization mode is to be used for your installation.

In previous releases of z/OSMF, Repository Authorization Mode was the only supported form of user authorization. Installations migrating from earlier releases
of z/OSMF are encouraged to convert existing authorizations to SAF authorizations (profiles and groups). z/OSMF includes tools to help with converting those authorizations to SAF Authorization Mode authorizations.

Choosing an authorization mode

To have user authorizations managed through your security management product, choose SAF Authorization Mode. This approach allows you to make user access to tasks as granular as you need. User roles are represented by groups, which your security administrator creates in your security management product. In this mode, the z/OSMF administrator responsibilities are limited to adding web site links to the z/OSMF user interface, and managing application links. SAF Authorization Mode is the default authorization mode for z/OSMF.

Consider using Repository Authorization Mode if you have determined that the IBM-supplied user roles are sufficient for your installation. If so, any person defined as z/OSMF user could be granted access to any system management task.

Table 13 summarizes the decision points for each authorization mode.

<table>
<thead>
<tr>
<th>Security concept or task</th>
<th>SAF Authorization Mode</th>
<th>Repository Authorization Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning for z/OSMF user responsibilities</td>
<td>Your security administrator determines which groups are to be created for managing user access. By default, the IBM-supplied REXX exec creates groups for the z/OSMF Administrator and z/OSMF User. You can use these groups as supplied, or replace or supplement them with other groups that you create as needed.</td>
<td>Your installation is limited to the predefined roles supplied with z/OSMF: • z/OSMF Administrator • z/OSMF User</td>
</tr>
<tr>
<td>Authorizing users to z/OSMF tasks</td>
<td>Your security administrator authorizes users to tasks by connecting users to the z/OSMF groups created previously. To do so, the security administrator edits and runs the IBM-supplied REXX exec with security commands for connecting users to the groups.</td>
<td>Both of the following steps are needed: • The z/OSMF Administrator performs user and role assignments through the administration tasks in the z/OSMF navigation area. • Your security administrator edits and runs the IBM-supplied REXX exec with security commands for completing the user assignments on the z/OS host system.</td>
</tr>
<tr>
<td>Adding links to the z/OSMF navigation area</td>
<td>To define links to z/OSMF, a user requires authorization to the ZOSMF.ADMINTASKS.LINKSTASK resource, which is controlled through the ZOSMF.ADMINTASKS.** resource profile in the default z/OSMF configuration. By default, the z/OSMF Administrator is authorized to add links. When defining links, the z/OSMF Administrator uses the Links task in the z/OSMF navigation area. This includes specifying a resource name for the link. For ease of security management, specify a resource name that falls within the ZOSMF.LINKS.** profile. Doing so will allow all z/OSMF users to access the links. If necessary, your installation can limit the access of links through the creation of discrete ZMFAPLA resource profiles.</td>
<td>By default, the z/OSMF Administrator role is authorized to add links. When defining links, the z/OSMF Administrator uses the Links task in the z/OSMF navigation area. This includes specifying a resource name for the link. The z/OSMF Administrator manages user access to links through the Roles task in the z/OSMF navigation area.</td>
</tr>
</tbody>
</table>
Managing guest user access in z/OSMF

z/OSMF includes options for managing the access of guest users, that is, users who enter z/OSMF without authorization to tasks. Depending on how a guest user enters z/OSMF, the user is considered either authenticated or non-authenticated, as follows:

- **z/OSMF Authenticated Guest.** A user who logs into z/OSMF with a valid user ID and password (or pass phrase), but who is not permitted to any tasks.
- **z/OSMF Guest.** A user who does not log into z/OSMF.

How you manage guest user access will depend on the authorization mode that your installation selects for z/OSMF. In SAF Authorization Mode, guest user access is managed through your security product. In Repository Authorization Mode, guest user access is managed by the z/OSMF Administrator through the Roles task.

z/OSMF automatically applies the guest user classification to users who enter z/OSMF without a task authorization. It is not possible to designate a user as a non-authenticated or authenticated guest user, for example, through a group assignment (in SAF Authorization Mode) or through the Users task (in Repository Authorization Mode).

By default, a non-authenticated guest user can access the z/OSMF Welcome task and access the provided links. An authenticated guest can access everything a non-authenticated guest can, and also view the online help.

Setting up security in SAF Authorization Mode

This section describes the actions for setting up security in SAF Authorization Mode.

When z/OSMF is operated in SAF Authorization Mode, the authorization of users to z/OSMF resources (tasks and links) is based on traditional z/OS security controls, such as user IDs and groups, and SAF resource profiles.

For an installation that uses RACF as its security management product, the z/OSMF configuration process creates the required security definitions. Specifically, z/OSMF provides a set of REXX execs with RACF commands that your security administrator can use to secure z/OSMF resources and users. These execs are created during the z/OSMF configuration process, and are customized for your installation, based on the plug-ins you have selected to configure.

Figure 13 on page 53 shows a typical security setup for z/OSMF. To conserve space, this figure includes only a subset of the available tasks: Incident Log, Deployment, and ISPF.
The z/OSMF configuration process creates the security definitions, as follows:

- During the configuration process, your security administrator runs the REXX exec `izuconfig1.cfg.rexx`. This exec contains commands for setting up a default security environment through the RACF security product. For example, the REXX exec includes commands for:
  - Activating the ZMFAPLA resource class and enabling it for RACLST processing.
  - Creating ZMFAPLA resource class profiles for each of the z/OSMF tasks to be enabled on your system.
  - Creating groups and permitting those groups to the ZMFAPLA resource class profiles.

By default, the REXX exec creates the groups IZUADMIN and IZUUSER, which correspond to the administrator and user roles, respectively.

For the security structures that are created during the z/OSMF configuration process, see Table 46 on page 228.

If your installation uses a security management product other than RACF, you must create equivalent commands for your security management product. If so, you can refer to the REXX execs for the authorizations that are needed.

- After the configuration process is completed, your security administrator can use the IBM supplied script, `izuauthuser.sh`, and the REXX exec it generates, to authorize users to z/OSMF and to the z/OS components used in z/OSMF operations. Your security administrator runs the REXX exec for each user to be authorized to z/OSMF.

When used as provided, the generated REXX exec connects the supplied user ID to the z/OSMF User group (IZUUSER). The exec also contains commented commands for connecting the user to the z/OSMF Administrator group. For a list of the tasks that are permitted to these groups by default, see Appendix A, "Default security setup for z/OSMF," on page 227.

You can create more user groups as needed, for example, one group per z/OSMF task. Note, however, that the `izuauthuser.sh` script is based on the default group assignments. If you create more groups, those groups will not be reflected in the IBM-supplied REXX exec.

Figure 13. SAF authorizations in z/OSMF
Depending on the plug-ins to be configured, your installation might need to create additional authorizations to various system resources. These requirements are described in this document.

Figure 14 shows the relationship between users, groups, and z/OSMF resource profiles in a default z/OSMF security environment. To conserve space, this figure includes only a subset of the available tasks: Incident Log, Deployment, and ISPF. In the figure, the group names and profiles are z/OSMF defaults.

For the complete set of profiles that are created during the z/OSMF configuration process, and the groups that are permitted to the z/OSMF resources by default, see Table 46 on page 228.

The ZMFAPLA class requires the RACLIST option to ensure optimal performance through the caching of profiles. If you make changes to the profiles, you must refresh the ZMFAPLA class to have the changes take effect.

As shown in Figure 14 z/OSMF V1R13 provides a default authorization for the Deployment task through profile <safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.**. Further, when APARs PM40764 and PM50651 are installed, your installation can create more granular authorizations for this task through an additional profile: <safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.**. For more information, see "Creating access controls for the Deployment task" on page 86.
Security setup for plug-ins in SAF Authorization Mode

During the configuration process, z/OSMF creates a REXX exec with RACF commands for your security administrator to use for controlling access to the z/OSMF tasks.

For your reference, the contents of the exec are provided in this document, as follows:

- “Commands for permitting z/OSMF tasks to your CIM server” on page 280
- “Commands for configuring the Capacity Provisioning plug-in” on page 281
- “Commands for configuring the Configuration Assistant plug-in” on page 282
- “Commands for configuring the Incident Log plug-in” on page 283
- “Commands for configuring the ISPF plug-in” on page 285
- “Commands for configuring the Resource Monitoring plug-in” on page 286
- “Commands for configuring the Software Deployment plug-in” on page 287
- “Commands for configuring the Workload Management plug-in” on page 288.

Managing security for links in SAF Authorization Mode

In SAF authorization mode, a link in the z/OSMF navigation area is treated as a resource. Your installation must determine whether access to a link should be limited to certain users or unrestricted. This topic describes the security considerations for managing links in SAF Authorization Mode.

Defining a link to z/OSMF requires both of the following steps:

- The link is defined on the product level by anyone who is permitted to the Links task.
- Access to the link is controlled by the security administrator, through a ZMFAPLA resource class profile.

The z/OSMF configuration process defines the ZOSMF.LINK** profile and permits groups to it. Specifically, z/OSMF permits the groups for z/OSMF users (IZUUSER) and z/OSMF administrators (IZUADMIN) to this profile. As a result, these users will be able to see all of the links in the navigation tree.

Defining a link as a protected resource

By default, links in z/OSMF are protected under the generic resource profile: <SAF-prefix>.ZOSMF.LINK.** where <SAF-prefix> is the SAF profile prefix defined in the WebSphere configuration (BBNBASE by default).

Depending on your installation’s security procedures, a link might require further protection through a discrete profile. When planning for new links, it is recommended that the z/OSMF Administrator work with the security administrator to determine whether a new link requires protection through a discrete profile.

In the Links task, the z/OSMF Administrator defines a link by specifying a name for the link and its URL. The Links task also includes a text entry window that requires the z/OSMF Administrator to further qualify the link resource name with a suffix, which can be used if a discrete profile is required for the link. If so, the z/OSMF Administrator can provide this fully-qualified resource name to the security administrator to use to create the user authorizations for the link.

As an example, Figure 15 on page 56 shows the RACF commands that a security administrator can use to define a discrete profile for a new link (the z/OS Basics
Information Center web site) and permit a group (IZUUSER) to that link.

```plaintext
RDEFINE ZMFAPLA (BBNBASE.ZOSMF.LINK.Z.OS_BASICS_INFORMATION_CENTER) UACC(NONE)
PERMIT BBNBASE.ZOSMF.LINK.Z.OS_BASICS_INFORMATION_CENTER CLASS(ZMFAPLA) ID(IZUUSER) ACC(READ)
```

Figure 15. Example: Defining a link resource name and permitting a group to it

Deleting an existing link will potentially require that your security administrator delete the discrete profile, if one was used to secure access to the link.

For more information about the Links task, see “Defining links for z/OSMF” on page 135.

Rules for defining links

When working with links, be aware that the SAF resource name suffix for the link is limited to 220 characters. Valid characters for resource names are: A-Z, a-z, 0-9, underscore (_), hyphen (-), period (.). The first character following a period must be alphabetic.

The link suffix must be unique among your existing link definitions. If you attempt to add a non-unique link name, z/OSMF issues an error message to indicate that the name already exists for another link.

If you change a link resource name through the links panel, you should ensure that the new link resource name is adequately protected through a ZMFAPLA resource profile definition. Here, a new profile might be needed to properly secure the link.

Setting up security in Repository Authorization Mode

In Repository Authorization Mode, the authorization of users to tasks is based user-to-role assignments that are administered in z/OSMF.

Using z/OSMF requires sufficient authority in both z/OS and z/OSMF, as follows:

- On the z/OS system to be managed, the resources to be accessed on behalf of z/OSMF users (data sets, operator commands, and so on) are secured through the security management product at your installation, for example, RACF.
- In z/OSMF, access to tasks is secured through the management of user roles.

Both levels of security must exist for z/OSMF users to work with a z/OS system; it is not sufficient for a z/OSMF administrator to assign users to a role for performing z/OSMF tasks. Users also require sufficient authorization on the z/OS system, such as a valid z/OS user ID and password, and a RACF group assignment.

On a system with RACF, for example, the RACF database contains profiles for all of the users, groups, data sets, and other resources that have been defined to RACF. When a z/OSMF user attempts to access a protected resource, RACF verifies the user’s identity (by checking the user profile in the RACF database) and performs authorization checking to ensure that the user may access the requested resource.
If a z/OSMF user attempts to access a resource without sufficient authority on the z/OS host system, the user’s request is rejected with an error message (insufficient authorization).

z/OSMF includes the script izuauthuser.sh, which creates a REXX exec with RACF commands that your security administrator can use to authorize z/OS user IDs to z/OSMF. The izuauthuser.sh script is described in “Authorizing users to z/OSMF” on page 120.

The process of authorizing a user to z/OSMF is based on two sets of tasks:

- The z/OSMF configuration process creates a REXX exec with security commands for defining resources on the z/OS host system, creating groups and permitting those groups to z/OSMF resources.
- The process of authorizing a user for z/OSMF work is continued after configuration with the z/OSMF administrator, who is responsible for assigning tasks to roles, and authorizing users to the roles.

**Roles in z/OSMF**

In Repository Authorization Mode, a role represents the ability to perform one or more tasks. These tasks include both general administrative actions for z/OSMF and task-specific actions for the z/OS system to be managed.

z/OSMF is shipped with two predefined roles to which you can assign users, as follows:

- The **z/OSMF Administrator** role allows a z/OSMF administrator to manage user access to z/OSMF and to define the tasks that users can perform. A z/OSMF administrator makes these determinations based on the type of work that each user is expected to perform on the z/OS system, as required by your installation.
- The **z/OSMF User** role allows a user to perform one or more tasks from the navigation area, as defined by a z/OSMF administrator. By default, the z/OSMF User role allows the user to perform any tasks, except for those defined as z/OSMF administration tasks.

Authorizing a user involves defining the user to z/OSMF and associating the user with a specific role, based on the type of work the user is expected to perform. This step is usually done by the z/OSMF Administrator.

By default, your configuration is defined with one z/OSMF administrator user. Your security administrator can use the IBM supplied script, izuauthuser.sh, and the REXX exec it generates, to quickly authorize more users to z/OSMF. This work is described in “Authorizing users to z/OSMF” on page 120.

**Note:**

- Though your installation can modify these roles extensively, it is recommended that you use the roles as provided, and reserve the access management related tasks for users assigned to the z/OSMF Administrator role.
- You cannot add additional roles. If the IBM supplied roles are not sufficient for your installation, based on your installation’s security procedures and also on the specific plug-ins that you want to install, it is recommended that you configure z/OSMF with SAF Authorization Mode instead.

z/OSMF also includes options for managing the access of guest users. Depending on how a guest user enters z/OSMF, the user is considered either authenticated or
non-authenticated. A non-authenticated guest is a user who has displayed the welcome page, but has not logged in. An authenticated guest has logged in, but has not been granted authority to z/OSMF tasks.

**Managing guest users in Repository Authorization Mode**

z/OSMF automatically applies the guest user classification to users who enter z/OSMF without a role assignment.

In Repository Authorization Mode, guest user access is managed by the z/OSMF Administrator through the **Roles** task.

By default, a non-authenticated guest user can access the z/OSMF **Welcome** task and access the z/OSMF provided links. An authenticated guest can access everything a non-authenticated guest can, and also view the online help.

**Managing security for links in Repository Authorization Mode**

In Repository Authorization Mode, the **Links** task is used to manage link assignments to roles and guest users.

The process of adding a link to z/OSMF includes specifying a resource name suffix for the link (up to 220 characters). The suffix is required even though resource profiles are not used when z/OSMF is running in Repository Authorization Mode.

For more information about the Links task, see "Defining links for z/OSMF" on page 135.
Part 2. Configuration

Configuring z/OSMF includes the following topics:

- Chapter 4, “Configuring z/OSMF,” on page 61
- Chapter 5, “Additional steps for setting up your z/OS system,” on page 81
- Chapter 6, “Changing the authorization mode for z/OSMF,” on page 99
- Chapter 7, “Migrating to a new release of z/OSMF,” on page 103
- Chapter 8, “Multiple instances of z/OSMF,” on page 111.
Chapter 4. Configuring z/OSMF

z/OSMF provides a script, called `izusetup.sh`, that collects installation-specific data that is used in the configuration of the product. As part of its processing, this script starts with the variable settings that are contained in the configuration file, and substitutes any installation-specific changes that you supply to make the resulting configuration more appropriate for your environment.

**Attention:**
- It is strongly recommended that you review all of the steps in this chapter before performing the configuration.
- If your installation is upgrading from a previous release of z/OSMF, you must migrate your existing configuration file and, if applicable, override file to the latest formats before configuring the new release of z/OSMF. Your upgraded files are used as input to the z/OSMF configuration process. For information, see Chapter 7, “Migrating to a new release of z/OSMF,” on page 103.

Users of this information

This book assumes that your installation has already installed z/OSMF through SMP/E, according to the instructions provided in Program Directory for z/OS Management Facility, GI11-2886, and that you used the default product directories.

Before you begin

Before continuing with the z/OSMF configuration process, ensure that the following work is done in this order:

1. z/OSMF is installed on your z/OS system and the appropriate program directory jobs have been run. See Program Directory for z/OS Management Facility, GI11-2886.

2. IBM WebSphere Application Server OEM Edition for z/OS is installed and configured on your z/OS system, but is not currently running. For the installation steps, see Program Directory for z/OS Management Facility, GI11-2886. For the configuration steps, see IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide GA32-0631.

3. Ensure that you have collected the list of variables and other information described in “Planning worksheets for z/OSMF” on page 35. You will supply these values as input to the configuration script that you use to set up z/OSMF.

How to access and run the script

You can run the `izusetup.sh` script from an OMVS or telnet/rlogin session. **You cannot run this script from ISHELL.**

The `izusetup.sh` script resides in the `/bin` subdirectory of the z/OSMF product file system. By default, this is `/usr/lpp/zosmf/V1R13/bin`. To access the script, ensure that this directory is specified in your shell environment path. To check your path, run the following command from your shell session: `echo $PATH`

If your path does not contain the script directory, you can add it to your path. Or, you can ensure that the current directory indicator `:` is included in your `PATH` and...
change to the script directory before running the script. To add the script directory
to your path, enter the export command from z/OS UNIX. In the following
example, the export command is used to add the default location for the script
directory to the PATH setting:

```
export PATH=/usr/lpp/zosmf/V1R13/bin:$PATH
```

If you configured z/OSMF in a prior release, ensure that your PATH setting has
the correct version of z/OSMF that you want to configure on your z/OS system.

For more information about the z/OS UNIX shell, including how to switch
between the shell and TSO/E, see [z/OS UNIX System Services User’s Guide]( SA22-7801).

### Setting the z/OSMF environment variables for your shell session

z/OSMF includes global settings or *environment variables* that control certain
aspects of your z/OS UNIX shell session during the configuration process. For
most typical configurations, the default values are correct and should not require
modification. It is recommended, however, that you review the defaults and
modify them if necessary before running the shell scripts. If the defaults are
appropriate for your environment, you do not need to modify them.

Table 14 shows the z/OSMF related environment variables that are used during
your shell session.

#### Table 14. Worksheet for the z/OSMF environment variables

<table>
<thead>
<tr>
<th>Environment Variable</th>
<th>Description</th>
<th>Variable name</th>
<th>Default value</th>
<th>Your value</th>
</tr>
</thead>
</table>
| z/OSMF configuration
directory. | Specifies the directory (the fully-qualified path name) for the z/OSMF configuration. | IZU_CONFIG_DIR | /etc/zosmf |            |
| z/OSMF log file
directory. | Specifies the directory (the fully-qualified path name) to be used for storing log files created during the z/OSMF configuration process. | IZU_LOGFILE_DIR | /var/zosmf/configuration/logs |            |
| z/OSMF root code
directory path. | Specifies the mount point (the fully-qualified path name) for the z/OSMF product file system that was created earlier when you ran the jobs described in the z/OSMF Program Directory. This value is release-specific; ensure that it matches the installed release of z/OSMF. | IZU_CODE_ROOT | /usr/lpp/zosmf/V1R13 |            |
| Path statement for the z/OSMF binary files. | Specifies the */bin subdirectory of the z/OSMF product file system. This value is release-specific; ensure that it matches the installed release of z/OSMF. | PATH | /usr/lpp/zosmf/V1R13/bin:$PATH |            |
| _BPX_SHAREAS setting | Specifies whether the child process is to be run in a separate address space from the login shell’s address space. | _BPX_SHAREAS | NO | This setting can help to avoid a potential out-of-memory error. |
To view the active environment values for your shell session, run the following command from your shell session:

```
env
```

To modify the environment variables, you can export them in your z/OS UNIX shell environment before running the scripts, or add them to the .profile for the user ID that you use to run the scripts. The following examples show the format of the export commands to use for modifying these settings:

```
export IZU_CODE_ROOT="directory-path"
export IZU_CONFIG_DIR="directory-path"
export IZU_LOGFILE_DIR="directory-path"
export PATH="directory-path":$PATH
export _BPX_SHAREAS="value"
```

To minimize the number of exports needed, you can place your export commands in an editable file (the environment variables file) and export the location of the file to your shell session. This approach saves you from having to enter the individual export commands for each shell session.

If you include an environment variables file, use the sample environment variables file that is supplied with z/OSMF as a model:

```
<IZU_CODE_ROOT>/defaults/izu_env.sh
```

To modify the environment variables for your shell session, follow these steps:

1. **Copy the IBM-supplied environment variables file to a read/write directory.**
   - Copy the file to a location that will be accessible from your shell session, such as the z/OSMF configuration directory `/etc/zosmf`.
   - Choose a file name that is meaningful; the examples in this section use `izu_env.sh`. This name is case sensitive.

2. **Modify the existing export commands with new values, as needed.** As shown in Figure 16, the IBM supplied environment variables file contains the following export commands:

   ```bash
   # Default value for the configuration directory
   export IZU_CONFIG_DIR=/etc/zosmf
   
   # Default value for the logfile directory
   export IZU_LOGFILE_DIR=/var/zosmf/configuration/logs
   
   # Default value for the product binaries
   export IZU_CODE_ROOT=/usr/lpp/zosmf/V1R13
   
   # Setup PATH so the zOSMF binaries are accessible.
   export PATH=.:/usr/lpp/zosmf/V1R13/bin:$PATH
   
   # For problems with out of memory starting jvms
   export _BPX_SHAREAS=NO
   ```

   **Figure 16. Contents of the izu_env.sh file**

   Replace any of the exported values, as appropriate. You must ensure that the variables specified in the file are set to valid values for your session. Your values are used as supplied. Specify only the exported values that you want to replace. Any variables that you omit from the file are defaulted to the values shown in Table 14 on page 62.

3. **Make your changes effective.** Before running the z/OSMF shell scripts, export the variable IZU_ENV_FILE, setting it to the location of this file, or add it to your .profile.
the .profile for the user ID that you use to run the scripts. The following export command example assumes that you have placed the environment variables file in the configuration directory and named it izu_env.sh:

```bash
export IZU_ENV_FILE=/etc/zosmf/izu_env.sh
```

**Ensuring that your user ID has enough storage**

To run the `izusetup.sh` script, your user ID requires sufficient virtual storage both above and below the two gigabyte bar. Before running the script, follow the instructions in this section to ensure that your user ID has sufficient storage.

For the below-the-bar storage allocation:
- If you plan to run the script in an OMVS session, ensure that the TSO/E region size (REGION) is set to 2G.
- If you plan to run the script in a telnet or rlogin session, ensure that ASSIZE in the OMVS segment for your user profile is set to 2G. This value can also be set through the BPXPRMxx parmlib member.

For the above-the-bar storage allocation, ensure that the MEMLIMIT value for your user ID is at least 2G (the default). This value can be set in a variety of ways, such as through the MEMLIMIT setting in your OMVS segment, or through the BPXPRMxx or SMFPRMxxx parmlib members.

**Figure 17** shows the format of the RACF ALTUSER command as it would be used to assign the storage allocations for a user. Here, the MEMLIMIT value is set in the OMVS segment for the user.

```
ALU "UserName" TSO(SIZE(2096128)) OMVS(ASSIZEMAX(2147483647) MEMLIMIT(2G))
```

**Figure 17. Format of the RACF ALTUSER command**

It is also possible to set the MEMLIMIT temporarily, through the ulimit shell command, if your z/OS UNIX system settings are configured to allow this action. Entering `ulimit -M 2048` sets the storage limit to 2048 megabytes (2 GB) for the duration of your OMVS session.

For more information about the MEMLIMIT system parameter, see z/OS MVS Programming: Extended Addressability Guide. For information about the ulimit command, see z/OS UNIX System Services Command Reference.

**Removing command aliases**

The z/OSMF configuration script makes use of built-in z/OS UNIX shell commands and defaults. If your z/OS UNIX shell profile (.profile) or system profile alters or aliases shell commands, remove the aliases before running the script. At a minimum, it is recommended that you remove the aliases for the following shell commands: `chmod`, `chown`, `cp`, `mkdir`, `mv`, and `rm`.

To determine which aliases are currently set, run the following command from the z/OS UNIX shell: `alias`.

To remove an alias, run the following command: `unalias <alias>`. Thereafter, for the duration of the session, the shell does not perform alias substitution when you specify the particular shell command.
Refreshing session status (for OMVS users)

In an OMVS session, the status of your session is displayed in the lower right-hand corner of the screen, just above the function key lines. This indicator lets you know the status of your session, such as whether an application is running or the shell session is ready for input.

When you run a script in OMVS, the status of your session is displayed as **RUNNING**. After a short time, the status indicator changes to **INPUT**; this means the shell session is ready for input and will not send any more output or messages to the display screen. If the status indicator changes to **INPUT** before you have received any or all of your output, press the Refresh function key and the shell will display more output on your screen. (If you don't have a Refresh function key, you can press a <Clear> key, <PA2>, or <PA3>.)

For more information about the status indicators for an OMVS session, see z/OS UNIX System Services User’s Guide SA22-7801.

---

Step 1: Create the initial configuration

This section describes script **izusetup.sh** when it is used with option `-config`. In short, when you use the `-config` option with this script, you create the initial configuration for z/OSMF.

About this step

When you run the **izusetup.sh** script, you specify a configuration file to be created as output, based on your input values. You gathered this input earlier in “Planning worksheets for z/OSMF” on page 35. The examples in this document use the name `izuconfig1.cfg` to refer to this output file.

If you retained the configuration file from a previous release of z/OSMF, and you want to re-use your settings for this release, you can select your existing configuration file when you invoke this script. Before doing so, you must migrate the configuration file to the latest format; see Chapter 7, “Migrating to a new release of z/OSMF,” on page 103.

As described in “The configuration process” on page 32, you can use an optional override file to specify the settings for your environment; these values replace the settings found in the IBM-supplied configuration file, `izudflt.cfg`. Any changes that you make to the override file should be completed before you invoke the `izusetup.sh` script. A default copy of the override file is located in the `/usr/lpp/zosmf/V1R13/defaults` directory, which is read-only. To create an override file for your installation, copy the default `izudflt.ovr` file to a read/write directory, and edit the file with an editor of your choice. It is recommended that you name the override file `izudflt.ovr`. For the contents of the override file that was supplied in this release of z/OSMF, see Figure 70 on page 259.

As described in “Choosing a script mode: Interactive or fastpath” on page 34, you can run the `izusetup.sh` script either interactively or “quietly” through the fastpath mode. When used in interactive mode, the `izusetup.sh` script provides a prompt environment that makes it easy to modify the configuration settings needed to create a working instance of z/OSMF. However, in some cases, if you prefer to supply the configuration values in a file with no interactive prompting, use the fastpath mode. For more about these modes, see “Using the script interactively” on page 66 and “Using the script in fastpath mode” on page 67.
Regardless of which mode you use, the script does the following:

- Creates a configuration file as output.
- As an aid to your security administrator, the script creates RACF commands in a REXX program, which your security administrator can verify and run. If your installation uses another security management product, you can create a REXX program with equivalent SAF commands. The REXX exec is tailored based on the plug-ins that you choose to configure for z/OSMF.

If during this step, your installation is changing the authorization mode for z/OSMF, this process produces a second security commands REXX exec. This exec contains only the delta of security commands that are required for setting up security under the new authorization mode.

You need run only one of the REXX execs that are created during this step. More information about the execs is provided in "Step 2: Run the security commands" on page 69.

For descriptions of the variables provided in the default configuration file, see Appendix D, “Default configuration file and default override file,” on page 255.

**Using the script interactively**

When used in interactive mode, this script prompts you for the installation-specific values that you gathered earlier in "Planning worksheets for z/OSMF" on page 35. All prompts require a response; either an acceptance of the displayed value, or a value that you enter in response to the prompt. If you specify your installation-specific values in an optional override file, the displayed values will be taken from the override file. Otherwise, you will be presented with the IBM default values (or no value, when an installation-specific value is mandatory).

If necessary, you can exit from the interactive session before completing it. When you exit, the script saves your in-progress configuration file up to the point at which you exit. To exit from a telnet or rlogin session, enter the Ctrl+C key combination. For an OMVS session, use the escape key sequence that is defined for your terminal emulator session.

When responding to the script prompts, observe the following considerations:

- To use an existing configuration file as input, specify the file name as input to the script. This file is expected to reside in the z/OSMF configuration directory `<IZU_CONFIG_DIR>`. Enter Y in response to the script prompt that asks whether to overwrite the existing configuration file. Your changes will be stored in that file (you might want to back up the contents of the file before invoking the configuration script in this manner). To create another configuration file, specify a new file name when prompted by the "save file" message.

- The script prompts you for a number of installation-specific values, such as the z/OSMF data file system, administrator ID default group and home directory, root directory path of the application server, and the other values you collected earlier.

- The z/OSMF administrator home directory (IZU_ADMIN_HOME) is set to `/u/zosmfad` by default. In many installations, this value should be replaced with an alternative directory. If so, specify a value that corresponds with the value you specify for the IZU_ADMIN_NAME variable. For example, if you specify the value ZMFAD for IZU_ADMIN_NAME, the IZU_ADMIN_HOME should be set to `/u/zmfad`.

- The script prompts you for the directory path and name of the WebSphere Application Server response file. Your installation created this file earlier when
installing IBM WebSphere Application Server OEM Edition for z/OS. If you cannot supply this value, for example, because the response file is not accessible or no longer exists, the script will prompt you for the WebSphere values listed in Appendix E, “Values from the WebSphere Application Server response file,” on page 261.

- The script prompts you to select which plug-ins are to be configured. Or, if you specified Y in your override file for any plug-ins, the script prompts you to confirm your plug-in selections.

To select plug-ins, respond to this prompt, as follows:
- All of the plug-ins, enter 0 (zero).
- None of the plug-ins, enter N.
- Particular plug-ins, enter the plug-in IDs, as needed:
  1  Incident Log
  2  Configuration Assistant
  3  Workload Management
  4  Resource Monitoring
  5  Capacity Provisioning
  6  Software Deployment
  7  ISPF

For multiple selections, separate each plug-in identifier with a comma.

If the script displays a prompt for the DASD Management plug-in, do not select it. This plug-in is not available for use.

Using the script in fastpath mode

To avoid prompting, you can specify the -fastpath option on the izusetup.sh script. This optional script parameter indicates that the set of variable values specified in the configuration file and the override file are complete and correct for your installation. If any variables are omitted from the override file, the izusetup.sh script checks your specified configuration file for the values. Omitted values will cause the script to end with errors.

Ensure that the variables specified in the override file are set correctly for your installation. The script uses these values as you provide them. Some variables are initially set to the following value, which is not a valid setting: NO.DEFAULT.VALUE. If these variables are not set to valid values, you must manually update the override file before invoking the izusetup.sh script.

Running the script

Authority
You require a user ID with superuser authority to run this script. For information about how to define a user with superuser authority (a superuser), see z/OS UNIX System Services User’s Guide SA22-7801.

Environment
Run the script in either an OMVS or telnet/rlogin session. You cannot run it from ISHELL.

Storage allocation
Your user ID should have at least two gigabytes (2 GB) of storage allocated for its use. For information, see “Ensuring that your user ID has enough storage” on page 64.

Location
The script resides in the following directory:
<IZU_CODE_ROOT>/bin
where `<IZU_CODE_ROOT>` is the product file system. By default, this is
`/usr/lpp/zosmf/V1R13`.

**Invocation**

From your shell session, run the script, as follows:

```
izusetup.sh -file <pathname>/izuconfig1.cfg -config
[-overridefile <pathname>/izudflt.ovr] [-fastpath]
```

Where:

- `<pathname>` is optional; if you specify a path name and the directory exists, it is used. If you omit a path name, the script uses the z/OSMF configuration directory `<IZU_CONFIG_DIR>` as the directory. This behavior is recommended as it ensures that configuration files are created in the z/OSMF configuration directory.
- `izuconfig1.cfg` identifies the configuration file to be created as output. You can choose another name for the configuration file, but the `.cfg` file type is required. If you use a different name, choose one that will be easy to remember and make a note of it. You will need to specify this name several times during the z/OSMF configuration process.
- `izudflt.ovr` identifies an optional override file, which you can use to substitute values in place of the IBM defaults. You can choose another name for this file, but the `.ovr` file type is required.

To run the script in fastpath mode, include the `-fastpath` option.

For descriptions of the options that you can specify on the `izusetup.sh` script, see [Appendix C, “izusetup.sh script,” on page 251](#).

**Results**

On completion, the script saves the output configuration file in the directory that you specified on the script invocation. By default, this is the configuration directory, which is specified on the IZU_CONFIG_DIR configuration variable and defaults to `/etc/zosmf`.

You can view the script output messages in the following log file:

```
<IZU_LOGFILE_DIR>/izusetup_config.mm.dd.yy.hh.mm.ss.tt.log
```

where `<IZU_LOGFILE_DIR>` is the location identified by the IZU_LOGFILE_DIR environment setting for the UNIX shell. By default, this is `/var/zosmf/configuration/logs/`.

The script creates either one or two REXX execs with RACF commands for creating the security definitions for your installation. The script saves the execs in the configuration directory (by default, `/etc/zosmf`). More information about the execs is provided in “Step 2: Run the security commands” on page 69.

If the configuration directory already contains an exec from a previous configuration effort, the script creates a backup copy of the original exec, using the exec name followed by a timestamp. Over time, your z/OSMF administrator can review the directory contents for time-stamped files, and remove the files, if desired.
If you need to repeat Step 1, use the -fastpath option

To update an erroneous configuration value, you must re-run the `izusetup.sh` 
`-config` script. However, instead of repeating the prompts, you can manually 
update your override file from the previous pass with the correct value, and run 
the `izusetup.sh` script with the -fastpath option. Here, the `izusetup.sh` script 
bypasses the prompt session, and uses the configuration file from the previous 
pass and your updated override file as input.

Adding a plug-in to z/OSMF later

If you need to add another plug-in to z/OSMF, you can do so later after you have 
completed an initial z/OSMF configuration. See the procedure described in 
"Adding plug-ins to a z/OSMF configuration" on page 124.

Step 2: Run the security commands

This section describes the REXX exec `izuconfig1.cfg.rexx` that was generated in the 
previous step. This exec contains RACF commands for securing the z/OSMF 
functions and tasks. Also described is a second REXX exec that was generated if 
your installation selected a new z/OSMF authorization mode in the previous step. 
You need run only one exec. This section includes considerations for determining 
which exec to run. Regardless of which exec is run, it is strongly recommended 
that your security administrator review the contents of each exec before running it.

About this step

The REXX exec `izuconfig1.cfg.rexx` contains RACF commands that your 
installation's security administrator can use to secure the z/OSMF functions and 
tasks. The contents of the exec depend on which plug-ins you have selected to 
configure with z/OSMF. The exec also contains commented sections for additional 
authorizations that might be useful for your installation. These sections should be 
reviewed by your security administrator and uncommented as needed. If your 
installation uses a security management product other than RACF, your installation 
must create equivalent commands for your security product.

Use caution in editing the contents of the exec. Subsequent steps depend on the 
consistency between the configuration file values and the resources created in 
RACF. Do not modify the names that are in the REXX exec. Instead, modify the 
respective value in the override file and then re-run the -config step. Doing so will 
cause the REXX exec to be regenerated with the desired value.

For your reference, Appendix I, “Contents of the RACF commands exec,” on page 
277 contains the sample REXX output that would be created if all plug-ins were to 
be deployed, and SAF Authorization Mode is selected for the z/OSMF 
configuration.

For an existing z/OSMF configuration, if your installation selected to change the 
authorization mode for z/OSMF in “Step 1: Create the initial configuration” on 
page 65, the configuration process created a second security commands REXX exec 
for your use. For help with determining which exec to use, see “Which commands 
exec to use” on page 70.
Which commands exec to use

The z/OSMF configuration process always creates the REXX exec `izuconfig1.cfg.rexx`. This exec contains the complete set of RACF commands for your configuration. Usually, this is the appropriate exec to use.

If your installation has already configured an instance of z/OSMF, however, and you are using the configuration process to change the authorization mode for z/OSMF, you might find it more appropriate to run just the delta set of security commands that are required for the new authorization mode. If so, you should review and run the conversion REXX exec instead of `izuconfig1.cfg.rexx`. The name and contents of this exec depend on which authorization mode is to be used, as follows:

- If your installation has selected to convert from Repository Authorization Mode to SAF Authorization Mode, the configuration process created the file `izuconfig1.cfg.convertFromREPtoSAF.rexx`. This file contains only the commands needed for establishing security in SAF Authorization Mode.
- If your installation has selected to convert from SAF Authorization Mode to Repository Authorization Mode, the configuration process created the file `izuconfig1.cfg.convertFromSAFtoREP.rexx`. For an existing installation, this exec is likely to be empty, except for commented sections indicating that no action is needed.

For help with determining which exec to use, see Table 15.

Table 15. Which commands exec to use

<table>
<thead>
<tr>
<th>Your scenario</th>
<th>Action to take</th>
</tr>
</thead>
<tbody>
<tr>
<td>New installation of z/OSMF</td>
<td>Run <code>izuconfig1.cfg.rexx</code></td>
</tr>
<tr>
<td>Migrating from an earlier release of z/OSMF to a new z/OSMF configuration</td>
<td>Run <code>izuconfig1.cfg.rexx</code></td>
</tr>
<tr>
<td>New z/OSMF configuration is already created; just changing the authorization mode from Repository to SAF.</td>
<td>Run <code>izuconfig1.cfg.convertFromREPtoSAF.rexx</code></td>
</tr>
<tr>
<td>New z/OSMF configuration is already created; just changing the authorization mode from SAF to Repository.</td>
<td>Run <code>izuconfig1.cfg.convertFromSAFtoREP.rexx</code> (the exec might consist of commented sections only).</td>
</tr>
</tbody>
</table>

Before running the exec

These commands should be reviewed by your security administrator and modified as needed for your installation’s environment.

Running the exec

Have your installation’s security administrator review the RACF commands in this exec, modify them as necessary, and run the exec to issue the commands.

Authority

This exec is run by your installation’s security administrator.

Environment

Run the exec from an OMVS or telnet/rlogin session. You cannot run it from ISHELL.
Location
The exec resides in the configuration file system (IZU_CONFIG_DIR). By
default, this is /etc/zosmf.

Invocation
From your shell session, do the following:
1. Make the IZU_CONFIG_DIR directory your active directory. For example:
   ```
cd /etc/zosmf
   ```
2. Run the exec, as follows:
   ```
./izuconfig1.cfg.rexx
   ```

Tip: By default, no log file is created. If you want a log file, you can use a z/OS
UNIX command, such as tee, to direct the output from this exec to a log file. If so,
you could direct this output to the z/OSMF log file directory for your installation
(IZU_LOGFILE_DIR). By default, this is /var/zosmf/configuration/logs/. For
example:
   ```
izuconfig1.cfg.rexx | tee
/var/zosmf/configuration/logs/izuconfig1.cfg.rexx.output
   ```

For techniques, see [z/OS UNIX System Services User’s Guide](SA22-7801).

Results
On completion, the exec creates the security definitions needed for your
configuration of z/OSMF.

If you run the exec more than once, message IKJ56702I INVALID data is issued for
any user IDs or groups that were defined previously, such as the ZOSMFAD user
ID. You can ignore this message.

Ensure that the z/OSMF administrator is authorized to the CIM
server
If your z/OSMF configuration includes tasks that require the Common Information
Model (CIM) server to be active, you must ensure that the z/OSMF administrator
user ID has the proper level of access to CIM server resources. In effect, the
z/OSMF administrator user is also a CIM administrator. CIM includes the CFZSEC
job to help you perform these authorization tasks. See the chapter on CIM server
quick setup and verification in [z/OS Common Information Model User’s Guide](SC33-7998). After the job is run, your security administrator must connect the
z/OSMF administrator user ID to the CFZADMG group.

If your installation does not plan to run the CFZSEC job, your security
administrator can perform these tasks manually by doing the following:
1. Grant the z/OSMF administrator user UPDATE access to the CIMSERV profile
   in the WBEM class. By default, this user ID is ZOSMFAD. This access can be
   granted through an explicit PERMIT command, or, if the CIM administrator
group is already permitted with UPDATE access, you can connect the user to
   the group. If necessary, refresh the WBEM class.
2. Ensure that the user ID under which the CIM server is running has
   SURROGAT access for the z/OSMF administrator user. If a generic BPX.SRV.**
   profile is already authorized in the SURROGAT class, no additional action is
   required. Otherwise, define a discrete profile for the z/OSMF administrator and
   authorize it. If necessary, refresh the SURROGAT class.
3. Verify that the z/OSMF administrator profile is properly set up for the z/OS UNIX shell environment. By default, the file profile.add, which is shipped with the CIM server, provides the environment variables that you need to define for the administrator; see /usr/lpp/wbem/install/profile.add. If you are not using the defaults, you should modify the appropriate settings. Copy the contents of the profile.add file to the .profile file in the home directory of the z/OSMF administrator user ID. The .profile file should be owned by the z/OSMF administrator, and have read-write-execute access for the owner.

These updates should be made before logging in to z/OSMF as the administrator, as described in “Logging into z/OSMF” on page 78.

Step 3: Verify the RACF security setup

This section describes script izusetup.sh when it is used with option -verify racf. In short, when you use the -verify racf option with this script, you verify the RACF security setup performed previously.

About this step

The izusetup.sh script verifies the results of the RACF commands that were performed through the generated REXX exec, described in “Step 2: Run the security commands” on page 69.

If your security administrator modifies the REXX exec, such as changing an access level to a profile or class, the script might interpret the change as an error. If so, you can ignore the related error messages.

To avoid errors, do not reduce the access authority of the z/OSMF administrator to less than what is specified by the commands in the exec.

If your installation uses a security management product other than RACF, do not perform this step. Instead, take the appropriate steps to verify your security setup.

Running the script

Authority
This script is run by your installation's security administrator.

Environment
Run the script in either an OMVS or telnet/rlogin session. You cannot run it from ISHELL.

Location
The script resides in the following directory:
<IZU_CODE_ROOT>/bin

where <IZU_CODE_ROOT> is the product file system. By default, this is /usr/lpp/zosmf/V1R13.

Invocation
From your shell session, run the script, as follows:
izusetup.sh -file izuconfig1.cfg -verify racf

where izuconfig1.cfg is the configuration file that you created previously in “Step 1: Create the initial configuration” on page 65.
**Results**

On completion, the script creates a report file called *izuracfverify.report*, which is stored in the following location:

<IZU_LOGFILE_DIR>/izuracfverify.report

If this directory already contains a report file, for example, from a previous -verify racf invocation, the script creates a backup copy of the original report file, using the file name followed by a timestamp.

Have your installation's security administrator review the report file for any areas that might require corrective action. As a possible technique for verifying the completion of the script, your security administrator can edit the report file and search for z/OSMF messages (IZU\*nnnnn). Each message should end with a reason code of zero.

You can view the script output messages in the following log file:

<IZU_LOGFILE_DIR>/izusetup_verify.mm.dd.yy.hh.mm.ss.tt.log

where <IZU_LOGFILE_DIR> is the log file directory for your installation. By default, this is /var/zosmf/configuration/logs/.

**Ensure that the CIM server is started**

If your configuration includes a plug-in that uses the CIM server (see “System prerequisites for the z/OSMF plug-ins” on page 24), you must ensure that the CIM server is active on your system before continuing to the next step. You can verify that the CIM server is started by entering a command like the following from the operator console:

D A,CFZCIM

This example assumes that the CIM server runs as a started task, using the default name CFZCIM.

If the CIM server is not already started, follow the steps described in [z/OS Common Information Model User’s Guide](SC33-7998). This book also includes information about customizing your CIM server start-up procedure and details on how to set environment variables for the CIM server.

---

**Step 4: Prime the z/OSMF data file system**

This section describes script *izusetup.sh* when it is used with option -prime. In short, when you use the -prime option with this script, you initialize the z/OSMF data file system.

**About this step**

The *izusetup.sh* script performs the following updates for z/OSMF:

- Initializes or "primes" the z/OSMF data file system. This work includes:
  - Allocating the z/OSMF data file system and mounting it, by default, at /var/zosmf/data.

  The script mounts the filesystem with the option UNMOUNT to ensure that it is unmounted if the z/OS system becomes unavailable. Also, for a zFS filesystem, the script mounts the filesystem with the option AGGRGROW to allow the filesystem to grow dynamically, as needed.
- The script also sets the permissions and ownership of the directories and files in the z/OSMF data file system.
- Creates the home directory for the z/OSMF administrator, if one does not already exist. By default, this directory is /u/zosmfad
- Changes ownership and permissions for the other directories that z/OSMF uses.
- Creates and updates parmlib members as needed for the plug-ins to be configured. For example, if you configured the Incident Log plug-in, this script creates members in the target parmlib data set. By default, this is SYS1.PARMLIB.
- Performs other data set allocations, as needed for z/OSMF processing.

Earlier, in “Step 1: Create the initial configuration” on page 65, you might have selected an interim or temporary parmlib data set to be used instead, perhaps because you did not want your system’s active parmlib data set to be updated directly by the script. If so, your installation’s system programmer must ensure that the temporary parmlib is accessible to z/OSMF by adding it to the list of active parmlib data sets.

**Before running the script**

By default, the z/OSMF administrator home directory is /u/zosmfad. If this directory is automount managed, you must pre-create it before running the script.

**Running the script**

**Authority**
You require a user ID with superuser authority to run this script.

**Environment**
Run the script in either an OMVS or telnet/rlogin session. You cannot run it from ISHELL.

**Location**
The script resides in the following directory:

<IZU_CODE_ROOT>/bin

where <IZU_CODE_ROOT> is the product file system. By default, this is /usr/lpp/zosmf/V1R13.

**Invocation**
From your shell session, run the script, as follows:

izusetup.sh -file izuconfig1.cfg -prime

where izuconfig1.cfg is the configuration file that you created previously in “Step 1: Create the initial configuration” on page 65.

**Results**
On completion, the script primes the z/OSMF data file system and creates the necessary directories and files for z/OSMF.

You can view the script output messages in the following log file:

<IZU_LOGFILE_DIR>/izusetup_prime.mm.dd.yy.hh.mm.ss.tt.log

where <IZU_LOGFILE_DIR> is the log file directory for your installation. By default, this is /var/zosmf/configuration/logs/.
Step 5: Complete the setup

This section describes script izusetup.sh when it is used with option -finish. In short, when you use the -finish option with this script, you complete the configuration of the z/OSMF.

About the script

The izusetup.sh script deploys z/OSMF, using the values you supplied earlier. Specifically, the script:

- Registers z/OSMF with IBM WebSphere Application Server OEM Edition for z/OS.
- Updates the WebSphere Application Server configuration, based on settings from the izuadmin.env file. For the setting defaults, see "Reviewing the z/OSMF advanced settings" on page 45.
- Prepares your z/OS system for running the tasks associated with the plug-ins that you selected to configure earlier.
- Verifies the setup for the z/OSMF functions and tasks. If you configured the Incident Log task, the script runs an installation verification program (IVP) that verifies the setup of the following z/OS system components:
  - Sysplex dump directory
  - System logger
  - Common event adapter (CEA)
  - System REXX.

The script creates a report indicating any areas that might require further action on your part.

Lastly, the script issues message IZUG349I, which provides the link (a URL) for accessing z/OSMF after the application server is started on your system, as described in "Step 6: Access the z/OSMF Welcome task" on page 77. z/OSMF will be available to users at the indicated URL.

In the message, the URL is based on the configured WebSphere hostname. In some installations, a network alteration such as dynamic VIPA (DVIPA) might invalidate this URL. If your network administrator has set up an alternate means for accessing the z/OSMF application, check with this person on the correct URL to use.

Before running the script

Before running this script, you must do the following:

1. Create a password for the z/OSMF administrator user ID, which is ZOSMFAD, by default. For RACF, you can use a command like the following to assign a password to ZOSMFAD:

   ALU ZOSMFAD PASSWORD(PutYourPasswordHere) NOEXPIRED

2. If you configured the Incident Log plug-in, you should have completed the z/OS system setup tasks. Use the checklist in "System prerequisites for the Incident Log plug-in" on page 25 to verify that all of these setup tasks have been completed.

3. Ensure that IBM WebSphere Application Server OEM Edition for z/OS is not running. If IBM WebSphere Application Server OEM Edition for z/OS is active, you must enter the appropriate STOP command to shut it down. For more
information about starting and stopping IBM WebSphere Application Server
OEM Edition for z/OS, see IBM WebSphere Application Server OEM Edition for

4. Optional: You can update certain settings for the WebSphere application server,
if the default values are not acceptable for your environment. For information,
see Appendix E, “Modifying advanced settings for the z/OSMF configuration,”
on page 263. In most cases, you should not need to change these values.

Considerations for the z/OSMF administrator user ID

This script is run from the z/OSMF administrator user ID that you created
previously (ZOSMFAD, by default). Before running this script, ensure that the
ZOSMFAD user ID is authorized to work with the directories, data sets, and file
systems in the locations specified by the variables in the configuration file. For
example, if you configured the Incident Log plug-in, and you allowed z/OSMF to
configure the common event adapter (CEA) component of z/OS earlier in “Step 1:
Create the initial configuration” on page 65, the user ID that runs this script must
be authorized on the z/OS system to activate the CEA parmlib member.

To complete the configuration process, the ZOSMFAD user ID must have at least
two gigabytes (2 GB) of storage allocated for its use. By default, the z/OSMF
configuration process assigns 2 GB of storage to the z/OSMF administrator user
ID. For an example of how storage is configured for a user ID, see “Ensuring that
your user ID has enough storage” on page 64.

Also, ensure that the following is done for the z/OSMF administrator user ID:

- Command aliasing is disabled, as described in “Removing command aliases” on
  page 64.
- If you selected one or more plug-ins that require the use of the CIM server on
  your z/OS system, verify that the z/OSMF administrator profile is properly set
  up for the z/OS UNIX shell environment. By default, the file profile.add, which
  is shipped with the CIM server, provides the environment variables that you
  need to define for the administrator; see “Ensure that the z/OSMF administrator
  is authorized to the CIM server” on page 71.

To determine which plug-ins require the CIM server, see “System prerequisites
for the z/OSMF plug-ins” on page 24.

Running the script

Authority
Run this script from the z/OSMF administrator user ID that you created
previously (ZOSMFAD, by default). The administrator user ID is connected to
the IBM WebSphere Application Server OEM Edition for z/OS default
configuration group.

Environment
Run the script in either an OMVS or telnet/rlogin session. You cannot run it
from ISHELL.

Location
The script resides in the following directory:

<IZU_CODE_ROOT>/bin

where <IZU_CODE_ROOT> is the product file system. By default, this is
/usr/lpp/zosmf/V1R13.
Invocation
From your shell session, run the script, as follows:

`izusetup.sh -file izuconfig1.cfg -finish`

where `izuconfig1.cfg` is the configuration file that you created previously in "Step 1: Create the initial configuration” on page 65.

This script might take some time to complete. As it runs, the script writes messages to the script log file.

If you run this script under OMVS, the status of your session is displayed as RUNNING. After a short time, the status indicator changes to INPUT; this means the shell session is ready for input and will not send any more output or messages to the display screen. If your output has not yet been displayed when the status changes to INPUT, press the Refresh function key and the shell will display more output on your screen. (If you don’t have a Refresh function key, you can press a <Clear> key, <PA2>, or <PA3>.)

Results
On completion, the script displays message IZUG349I, which provides the link for accessing z/OSMF, as described in “Step 6: Access the z/OSMF Welcome task.”

This message is also written to the script log file:

`<IZU_LOGFILE_DIR>/izusetup_finish.**mm.dd.yy.hh.mm.ss.tt**.log`

where `<IZU_LOGFILE_DIR>` is the log file directory for your installation. By default, this directory is `/var/zosmf/configuration/logs/`. If the script ends with errors, see the troubleshooting actions listed in “Problems during configuration” on page 155.

If you selected to configure the Incident Log task, the script runs an installation verification program (IVP) to verify the setup of z/OS system components. To see the results of the IVP, check the report file named `izuincidentlogverify.report`, which resides in the log directory (`IZU_LOGFILE_DIR`). For more information, including corrective actions for problems identified in the report, see “Using the installation verification program” on page 161.

If this directory already contains a report file from a previous -finish invocation, the script creates a backup copy of the original report file, using the file name followed by a timestamp.

Step 6: Access the z/OSMF Welcome task

At the end of the z/OSMF configuration process, you can verify the results of your work by opening a web browser to the z/OSMF Welcome task.

Before accessing the z/OSMF Welcome task, you must ensure that IBM WebSphere Application Server OEM Edition for z/OS is running. To start it, you can use either the MVS START command or the `startServer.sh` script, as follows:

- To use the MVS START command from ISPF, enter the command with the following syntax:

```sh
START appserver_proc_name JOBNAME=server_short_name,
    ENV=cell_short_name.node_short_name.server_short_name
```

For example:
To invoke the startServer.sh script from z/OS UNIX, enter a command with the following syntax:

```
$IZU_APPSERVER_ROOT/AppServer/bin/startServer.sh $APPSERVER_NAME
```

For example:

```
/zWebSphereOEM/V7R0/config1/AppServer/bin/startServer.sh server1
```

Leave the instance running for this step. If you need to shut it down, use the STOP command. For information about starting and stopping the server, see [WebSphere Application Server OEM Edition for z/OS Configuration Guide](https://www.ibm.com). GA32-0631.

To verify the z/OSMF configuration, open a web browser to the z/OSMF Welcome task. The URL for the Welcome task has the following format:

```
https://hostname:port/zosmf/
```

where:

- **hostname** is the hostname or IP address of the system in which IBM WebSphere Application Server OEM Edition for z/OS is installed
- **port** is the secure application port for the IBM WebSphere Application Server OEM Edition for z/OS configuration.

To find the URL, see message IZUG349I, which was written to the log file that was created when you ran the izusetup.sh script with the -finish option, as described in “Step 5: Complete the setup” on page 75. This log file is in the format:

```
<IZU_LOGFILE_DIR>/izusetup_finish.mm.dd.yy.hh.mm.ss.tt.log
```

where `<IZU_LOGFILE_DIR>` is the log file directory for your installation. By default, this directory is `/var/zosmf/configuration/logs/`.

If you encounter errors when opening your web browser to the z/OSMF Welcome task, you might need to modify your workstation setup. z/OSMF includes a tool that you can run to check your browser settings and workstation configuration. For more information, see “Verifying your workstation with the environment checker” on page 144.

### Logging into z/OSMF

To log into z/OSMF, enter a valid z/OS user ID and password or pass phrase in the log in section in the navigation area. By default, the z/OSMF administrator user ID is already authorized. You can use that user ID and password to log in.

### About this task

You can launch multiple instances of z/OSMF using different computers, different browsers, or multiple instances of the same browser. If you use multiple instances of the same browser (new window or tab) and your browser is configured to use the same browser session for each instance, when you log into or log out of one z/OSMF instance, you are automatically logged into or logged out of each instance. If you launched multiple z/OSMF instances using different computers or different browsers or using multiple instances of a browser that is not configured to use the same browser session, you must log into and log out of each z/OSMF instance.
Procedure
1. In the User ID field in the navigation area, enter your z/OS user ID that is specified in the z/OS security management facility (for example, RACF) associated with the host system.
2. In the Password or pass phrase field in the navigation area, enter the password or pass phrase associated with the z/OS user ID.
3. Click the Log in button.

Results
If the user ID and password or pass phrase are valid, you are authenticated to z/OSMF. The Welcome guest in the header is changed to Welcome <your_user_ID> and the navigation area is updated and lists the tasks to which you are authorized. If you are not authorized to work with certain tasks, those tasks are not displayed in the navigation area for you.

To log out of z/OSMF, click the Log out link in the banner area.

Re-authenticating in z/OSMF
When your z/OSMF session expires, you can re-authenticate using the re-authentication dialog box.

About this task
Your z/OSMF session expires after a period of time has elapsed. By default, this period is 490 minutes from the time you log into z/OSMF. Your installation can choose to modify this setting (the ltpatimeout value) during the configuration of z/OSMF. For more details, see Appendix F, “Modifying advanced settings for the z/OSMF configuration,” on page 263.

The re-authentication dialog box is displayed for 15 minutes. If you re-authenticate before the period ends, the tabs (in the work area) are unaffected by the re-authentication. If you do not respond before the re-authentication period ends, you are logged out, the tabs in the work area are closed, and any unsaved data is lost.

If you launched multiple instances of z/OSMF in the same browser (using new tabs or new windows) and your browser is configured to use the same browser session for new windows or tabs, the session for each instance will expire simultaneously; hence, a re-authentication dialog box is displayed in each tab or window. In this case, you can respond to one re-authentication dialog box and you are automatically re-logged into or logged out of each instance. If you launched multiple z/OSMF instances using different computers or different browsers or using multiple instances of a browser that is not configured to use the same browser session, the browser sessions are treated independently and each z/OSMF instance will require its own re-authentication.

While the re-authentication dialog box is displayed, you cannot interact with any tasks in that z/OSMF instance. You cannot explicitly close the dialog box. You can only close it by choosing to log in or log out.
**Procedure**

1. Verify the user ID. You cannot modify the user ID. If it is incorrect, click **Log out**. Otherwise, proceed to Step 2. When you click **Log out**, z/OSMF closes all opened tabs and discards any unsaved changes.
2. Enter the password or pass phrase that corresponds with the z/OS user ID.
3. Click **Log in** to re-authenticate.

**Results**

If the password or pass phrase is valid, you are logged in again. If you selected to log out (by clicking **Log out**), the *Welcome* page is displayed. If the password or pass phrase is incorrect, an error message is displayed and the re-authentication dialog box is still displayed. In this case, try logging in again. If you are unable to authenticate before the re-authentication period expires, z/OSMF will automatically log you out.
Chapter 5. Additional steps for setting up your z/OS system

This topic describes additional the customization steps that might be needed for your z/OS system, as follows:

- “Using FTP in your network”
- “Updating the BPXPRMxx member of parmlib”
- “Reviewing your CIM server setup” on page 83
- “Updating z/OS for the Capacity Provisioning plug-in” on page 83
- “Updating z/OS for the Configuration Assistant plug-in” on page 84
- “Updating z/OS for the Incident Log plug-in” on page 85
- “Updating z/OS for the Resource Monitoring plug-in” on page 85
- “Updating z/OS for the Software Deployment plug-in” on page 86
- “Updating z/OS for the Workload Management plug-in” on page 95

Using FTP in your network

Some z/OSMF tasks, such as the Incident Log, use FTP to transmit data. If your network contains a firewall that blocks FTP traffic or does not allow authentication using FTP, you must perform an additional action to allow the traffic to pass.

For considerations, see the online help for the Send Diagnostic Data wizard in the Incident Log task.

Updating the BPXPRMxx member of parmlib

This topic describes several changes for parmlib member BPXPRMxx that might be needed on your system.

This topic contains the following information:

- “Ensuring that z/OSMF file systems are mounted at IPL time”
- “Using the automount facility” on page 82

Ensuring that z/OSMF file systems are mounted at IPL time

To have the z/OSMF file systems automatically mounted at IPL time, you must update your auto-mount process or BPXPRMxx parmlib member. By default, the z/OSMF file systems use the following names:

- **Product file system**: IZU.SIZUHFS is the default file system name for an HFS file system and IZU.SIZUZFS is the default file system name for a zFS file system. The product file system is mounted in read mode at the location specified on the IZU_CODE_ROOT environment variable.

- **Data file system**: The default name is IZU.SIZUDATA. The z/OSMF data file system is mounted in read/write mode at the location specified on the IZU_DATA_DIR configuration variable.

To have these file systems mounted automatically at IPL time, add MOUNT commands for the file systems to your currently active BPXPRMxx parmlib member. For your reference, Table 16 on page 82 provides sample MOUNT commands.
Table 16. Sample MOUNT commands for z/OSMF file systems

<table>
<thead>
<tr>
<th>z/OSMF file system to be mounted</th>
<th>MOUNT command example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product file system</td>
<td>MOUNT FILESYSTEM(Izu.SIZUZFS) MOUNTPOINT(/usr/lpp/zosmf/V1R13) TYPE(ZFS) MODE(READ)</td>
</tr>
<tr>
<td>Data file system</td>
<td>MOUNT FILESYSTEM(Izu.SIZUDATA) TYPE(ZFS) MODE(RDWR) MOUNTPOINT(/var/zosmf/data)</td>
</tr>
</tbody>
</table>

When z/OSMF allocates and mounts the configuration and data file systems, it uses your installation’s defaults. If AUTOMOVE=Y is in effect for your installation, you might see following message displayed when your system is shut down:

```
BPXMO48I BPXJOINIT FILESYSTEM SHUTDOWN INCOMPLETE.
2 FILESYSTEM(S) ARE STILL OWNED BY THIS SYSTEM.
```

To remove this restriction, add a MOUNT statement with the UNMOUNT parameter to your BPXPRMxx member, as shown in the previous MOUNT command examples.

For more information about the AUTOMOVE setting, see [z/OS UNIX System Services Planning](https://www.ibm.com/support/docview’ai=90319313) GA22-7800.

**Using the automount facility**

The automount facility of z/OS automatically mounts file systems when they are accessed. It manages the creation of the mount point and the mount of the user file system for you. Whenever someone accesses a directory managed by the automount facility, the mount is issued automatically.

The mount point directory for the z/OSMF data file system is specified on the IZU_DATA_DIR configuration variable; by default, the directory is /var/zosmf/data. If the z/OSMF mount point directory is controlled by the automount facility, you must either disable the automount rule for this mount point before running the script that configures z/OSMF, or perform the following steps manually before running the configuration script:

1. Configure your automount policy appropriately for the z/OSMF data file system and mount point.
2. Allocate the z/OSMF data file system data set.
3. Enter the following commands. If you selected different values for these default settings, substitute the actual values that you selected for your installation:
   a. chmod 770 /var/zosmf/data
   b. chown WSSRU1:WSCFG1 /var/zosmf/data

By default, the z/OSMF administrator home directory is /u/zosmfad. If this directory is automount managed, you must pre-create it before running the script described in “Step 4: Prime the z/OSMF data file system” on page 73.

For more information about the automount facility, see [z/OS UNIX System Services Planning](https://www.ibm.com/support/docview’ai=90319313) GA22-7800.
Reviewing your CIM server setup

If your installation is using plug-ins that require the CIM server, see this section for additional considerations.

This section contains the following topics:

- "Ensuring that the CIM server is started at IPL time"
- "Advanced settings for the CIM server configuration."

Ensuring that the CIM server is started at IPL time

It is recommended that you ensure that the CIM server is started automatically at IPL time. For information about customizing the CIM server startup, see z/OS Common Information Model User’s Guide SC33-7998.

Advanced settings for the CIM server configuration

If the CIM server times out frequently during z/OSMF operations, you can increase the length of time that z/OSMF waits for a response from the CIM server. See Appendix F, “Modifying advanced settings for the z/OSMF configuration,” on page 263.

Updating z/OS for the Capacity Provisioning plug-in

If you have configured the Capacity Provisioning plug-in, determine whether access to a remote CIM server is required. If so, follow the steps in this section.

Before you begin

Determine whether the remote server is configured to require secured sign-on authentication. If so, you will need to ensure that the PassTicket is set up properly for users of this task.

For information about setting up Capacity Provisioning, see z/OS MVS Capacity Provisioning User’s Guide SC33-8299.

About this task

If access to a remote Common Information Model (CIM) server is required, you will need to do the following:

- Ensure that users are members of the Provisioning Manager query security group (by default, the CPOQUERY group)
- Ensure that PassTickets are enabled for every user who might require access to the remote CIM server
- Verify that users are defined in the security management product for your installation
- Verify that the WebSphere Application Server servant user ID is authorized to generate PassTickets.

The following procedure shows how this setup can be done for a system that uses RACF as its security management product. Included are the definitions that are needed to use the secured signon function and to generate PassTickets. Some or all of this work might already be done on your system, or might not be applicable. If so, you can skip any setup actions that are not applicable.
Procedure

1. Activate the security class PTKTDATA, if this action is not already done. For example:
   ```
   SETROPTS CLASSACT(PTKTDATA)
   SETROPTS RACLIST(PTKTDATA)
   ```

2. Define the profile CFZAPPL in the PTKTDATA class. If a common cryptographic architecture (CCA) product is installed on the systems with the secured signon function you can encrypt the secured signon application keys. If not, you can mask the secured signon application key by using the SSIGNON operand and a 64-bit KEYMASKED value. For example:
   ```
   RDEFINE PTKTDATA CFZAPPL SSIGNON(KEYMASKED(key))
   APPLDATA('NO REPLAY PROTECTION')
   SETROPTS RACLIST(PTKTDATA) REFRESH
   ```
   where `key` is a user-supplied 16-digit value used to generate the PassTicket. You can specify a value of your choice. Valid characters are 0 - 9 and A - F.

3. To enable PassTicket creation for users, define the profile IRRPTAUTH.CFZAPPL.* in the PTKTDATA class, and give the WebSphere Application Server servant user ID at least UPDATE access authority. For example:
   ```
   RDEFINE PTKTDATA IRRPTAUTH.CFZAPPL.* UACC(NONE)
   PERMIT IRRPTAUTH.CFZAPPL.* CLASS(PTKTDATA) ID(passticket_creator_userid)
   ACCESS(UPDATE)
   SETROPTS RACLIST(PTKTDATA) REFRESH
   ```
   where `passticket_creator_userid` is the user ID of the WebSphere Server servant.

4. Activate the changes, for example: SETROPTS RACLIST(PTKTDATA) REFRESH

What to do next

For more information about PassTickets, see z/OS Security Server RACF Security Administrator’s Guide SA22-7683.

Updating z/OS for the Configuration Assistant plug-in

The Windows desktop version of Configuration Assistant for z/OS Communications Server allows you to store configuration backing store files on your local drive, a LAN drive, or on z/OS.

About this task

If your installation uses the Windows desktop version of Configuration Assistant, and you want to continue using your existing data in z/OSMF, you can transfer your backing store files into the z/OSMF environment.

Procedure

1. Determine the location of your existing backing store files. They might reside on your Windows local drive, a LAN drive, or already on z/OS. Use the File > Properties menu option from the Windows client to view the location.

2. If the backing store files reside on your Windows local drive or LAN drive, copy them to the z/OS system on which Configuration Assistant is running. Backing store files are binary and can be placed in a data set or in the z/OS UNIX System Services (z/OS UNIX) file system.

3. From Configuration Assistant in z/OSMF, use the Actions > Tools > Transfer Backing Store file to z/OSMF option to perform the transfer.
4. Enter the name and path of your existing backing store file on z/OS. This required value can be a data set or a z/OS UNIX file.

5. Click on Transfer to copy the backing store file into z/OSMF.

What to do next

You have now transferred the file into the z/OSMF environment. The file can be used in all subsequent Configuration Assistant operations.

Updating z/OS for the Incident Log plug-in

Enabling your z/OS system for the Incident Log plug-in requires customization of the z/OS host system.

As described in “System prerequisites for the Incident Log plug-in” on page 25, the Incident Log task requires that a number of z/OS components and facilities be enabled on your system. Much of this work might already be done on your system; for instructions, see Appendix B, “z/OS system setup for the Incident Log task,” on page 231.

Updating z/OS for the Resource Monitoring plug-in

If you have selected to configure the Resource Monitoring plug-in, determine whether the RMF Distributed Data Server (DDS) on the target system is configured to require authentication. If so, you must ensure that the PassTicket is set up properly. Also, you must verify that users are defined in the security management product for your installation, and that the WebSphere Application Server servant user ID is authorized to generate PassTickets.

About this task

The following procedure shows how this setup can be done for a system that uses RACF as its security management product.

Note: If you use RMF XP, the RACF profile name for the RMF XP DDS is GPM4CIM. Use this profile name instead of GPMSERVE when you complete Steps 2 through 4 in the following procedure.

Procedure

1. Activate the security class PTKTDATA, if this action is not already done. For example:

   ```
   SETROPTS CLASSACT(PTKTDATA)
   SETROPTS RACLIST(PTKTDATA)
   ```

2. Define the profile GPMSERVE for the DDS in the PTKTDATA class and associate a secret secured signon key with the profile. The key must be the same on both the system on which the PassTicket is to be generated (the z/OSMF system) and the system on which the PassTicket is to be verified (the DDS system). For example:

   ```
   RDEFINE PTKTDATA GPMSERVE SSIGNON([KEYENCRYPTED]KEYMASKED)(key)
   SETROPTS RACLIST(PTKTDATA) REFRESH
   ```

   where key is a user-supplied 16-digit value used to generate the PassTicket. You can specify a value of your choice. Valid characters are 0 - 9 and A - F.

3. To enable PassTicket creation for users, define the profile IRRPTAUTH.GPMSERVE.* in the PTKTDATA class, and set the universal access
authority to NONE. You can do enable PassTicket creation for either for all user IDs or for a specific user ID, as shown in the examples that follow.

- Example (for all user IDs):
  RDEFINE PTKTDATA IRRPTAUTH.GPMSERVE.* UACC(NONE)

- Example (for a specific user ID):
  RDEFINE PTKTDATA IRRPTAUTH.GPMSERVE.specific_dds_login_userid UACC(NONE)

4. Grant the z/OSMF product permission to generate PassTickets for GPMSERVE.

- Example (for all user IDs):
  PERMIT IRRPTAUTH.GPMSERVE.* CLASS(PTKTDATA) ID(passticket_creator_userid) ACCESS(UPDATE)

- Example (for a specific user ID):
  PERMIT IRRPTAUTH.GPMSERVE.specific_dds_login_userid CLASS(PTKTDATA) ID(passticket_creator_userid) ACCESS(UPDATE)

where passticket_creator_userid is the user ID of the WebSphere servant region for z/OSMF.

5. Activate the changes, for example: SETROPTS RACLIST(PTKTDATA) REFRESH

**What to do next**

For more information about setting up the DDS server and RMF XP, see z/OS RMF User’s Guide SC33-7990. For more information about PassTickets, see z/OS Security Server RACF Security Administrator’s Guide SA22-7683.

---

**Updating z/OS for the Software Deployment plug-in**

If you selected to configure the Software Deployment plug-in, follow the instructions in the sections that follow.

By default, the z/OSMF configuration process gives equal access to deployment objects to all users authorized to the Deployment task. Your installation can further refine these authorizations, as described in the topic “Creating access controls for the Deployment task.”

By default, the Deployment task works only with systems in the local sysplex. Optionally, your installation can allow the Deployment task to work with systems on other sysplexes in your installation. To do so, you must enable the sharing of digital certificates. For instructions, see “Configuring a primary z/OSMF for communicating with secondary instances” on page 93.

**Creating access controls for the Deployment task**

The Deployment task allows users with proper authorization to manage global zones, software instances, deployments, and categories. For some actions, users must also have appropriate authorization to the physical resource these objects describe, such as a target zone or data set. This topic describes how to control user access to the objects in the Deployment task. Creating access controls for the actual physical resource is outside the scope of z/OSMF.

In Repository Authorization Mode, you can control which users are authorized to the Deployment task, but you cannot restrict user access to an object or an action. In this case, all users authorized to the Deployment task have equal access to these objects.
In SAF Authorization Mode, if APARs PM40764 and PM50651 are installed, you can use your security product to control access to the task and to create more granular authorizations, such as restricting access to an object or an action. Access to the Deployment task and its objects are controlled through the following default resource profiles, which are defined in the ZMFAPLA class:

<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.**
<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.**

If your installation is using RACF, by default, the IZUADMIN and IZUUSER groups are permitted READ access to profile <safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.** and CONTROL access to profile <safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.**. These permissions allow z/OSMF administrators and z/OSMF users to perform all actions for all objects.

**Important:** All users of the Deployment task should be permitted at least READ access to profile <safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.**. Otherwise, no actions can be performed because users will not have access to any objects.

To further restrict access to the objects and actions, define a SAF resource profile for each object and grant users the appropriate access authority. Regardless of where the physical resource described by an object resides, the SAF profiles for that object must be defined on the z/OS system that hosts the z/OSMF instance to which a user's Web browser is connected. The Deployment task uses this z/OS system when performing SAF authorization checking.

Use the SAF resource names, which are generated by the Deployment task, to help you define profiles that will control user access to an object or an action. The SAF resource names for each object are constructed using properties of the object. The casing used for each property value is preserved; therefore, SAF resource names are case sensitive. The SAF resource name format used for each object type and supported actions are described in the sections that follow.

**Authorizing users to global zones**

A global zone object describes an SMPCSI data set that contains an SMP/E global zone. To control access to a specific global zone, define a SAF resource profile for that resource. The SAF resource name for a global zone object has the following format:

<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.GZN.systemName.dsname

where:
- **GZN** indicates that the object associated with this SAF resource is a global zone.
- **systemName** is the name of the z/OSMF host system that has access to the global zone CSI data set. The system is defined on the Systems page in the Deployment task.
- **dsname** is the name of the CSI data set that contains the global zone.

For example, if you have a global zone CSI data set named MVSBUILD.ZOS113.CSI that can be accessed by system AQFT, the SAF resource name for the global zone would be

<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.GZN.AQFT.MVSBUILD.ZOS113.CSI
Table 17 lists the access authorities you can assign to global zone resources and the actions that are permitted for each access authority. The Deployment task does not perform authorization checks to determine which global zones to display in a list or table; therefore, all global zones will be displayed regardless of access authority.

Table 17. Actions users can take against global zones by access authority

<table>
<thead>
<tr>
<th>Access Authority</th>
<th>Actions Allowed</th>
</tr>
</thead>
</table>
| READ             | • View the properties of the global zone.  
                   • Copy the properties of the global zone.  
                   • Select the global zone when defining a software instance.  
                   • Connect a target software instance to the global zone during a deployment. |
| UPDATE           | In addition to the actions specified for READ access, users can perform the following action:  
                   • Modify the global zone properties that are not used to create the SAF resource name for the global zone. |
| CONTROL          | In addition to the actions specified for READ and UPDATE access, users can perform the following actions:  
                   • Create new global zones explicitly using the Add action or implicitly as part of the Copy action.  
                   • Modify the global zone properties that are used to create the SAF resource name for the global zone and control access to the global zone. Note that, regardless of access level, the CSI data set name cannot be changed.  
                   • Remove the global zone. |

Authorizing users to software instances

A software instance describes a deployable unit of software, composed of data sets containing SMP/E installed software. To control access to a specific software instance, define a SAF resource profile for that resource. The SAF resource name for a software instance object has the following format:

<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.SWI.category.systemName.instanceName

where:
- **SWI** indicates that the object associated with this SAF resource is a software instance.
- **category** is the name of the category assigned to the software instance. If multiple categories are assigned, a separate SAF resource name is created for each category. If no category is assigned, the category value is NOCATEGORY.

To perform an action, users must have the access authority required for that action for all the SAF resource names associated with the software instance.

- **systemName** is the name of the z/OSMF host system that has access to the volumes and data sets where the software instance resides. The system is inherited from the global zone associated with the software instance, and is defined on the Systems page in the Deployment task.
- **instanceName** is the name of the software instance.

For example, if you have a software instance named z/OSV1R13_Test that can be accessed by system AQFT and is assigned to categories z/OS and Test, its SAF resource names would be
Table 18 lists the access authorities you can assign to software instance resources and the actions that are permitted for each access authority. The Deployment task does not perform authorization checks to determine which software instances to display in a list or table; therefore, all software instances will be displayed regardless of access authority.

### Table 18. Actions users can take against software instances by access authority

<table>
<thead>
<tr>
<th>Access Authority</th>
<th>Actions Allowed</th>
</tr>
</thead>
</table>
| **READ**         | • View the properties of the software instance.  
|                  | • Copy the properties of the software instance. 
|                  | • Deploy the software instance during a deployment. 
|                  | • Use the software instance as the model for priming a deployment configuration. 
|                  | • Generate requisite and regression reports for the software instance. |
| **UPDATE**       | In addition to the actions specified for READ access, users can perform the following actions: 
|                  | • Modify the software instance properties that are *not* used to create the SAF resource name for the software instance. This includes modifying the software instance explicitly using the **Modify** action or implicitly when completing a deployment where the objective is to replace the software instance. 
|                  | • Replace the software instance during a deployment. |
| **CONTROL**      | In addition to the actions specified for READ and UPDATE access, users can perform the following actions: 
|                  | • Create new software instances explicitly using the **Add with Wizard** and **Add without Wizard** actions or implicitly as part of the **Copy** action or when completing a deployment where the objective is to create a new software instance. 
|                  | • Modify the software instance properties that are used to create the SAF resource name for the software instance and control access to the software instance. This includes modifying the software instance explicitly using the **Modify** action or implicitly when completing a deployment where the objective is to replace the software instance. 
|                  | • Remove the software instance. |

## Authorizing users to deployments

A deployment is a checklist that guides users through the process of cloning or deploying a software instance, and it is the object in which z/OSMF stores information about the clone, such as its data set names and locations, catalog structure, and SMP/E zone names. To control access to a specific deployment, define a SAF resource profile for that resource. The SAF resource name for a deployment object has the following format:

<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.DEP.category.deploymentName

where:

- **DEP** indicates that the object associated with this SAF resource is a deployment.
category is the name of the category assigned to the deployment. If multiple categories are assigned, a separate SAF resource name is created for each category. If no category is assigned, the category value is NOCATEGORY.

To perform an action, users must have the access authority required for that action for all the SAF resource names associated with the deployment.

deploymentName is the name of the deployment.

For example, if you have a deployment named z/OS_R13_Production that is not assigned to any category, its SAF resource name would be

<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.DEP.NOCATEGORY.z/OS_R13_Production

Table 19 lists the access authorities you can assign to deployment resources and the actions that are permitted for each access authority. The Deployment task does not perform authorization checks to determine which deployments to display in a list or table; therefore, all deployments will be displayed regardless of access authority.

Table 19. Actions users can take against deployments by access authority

<table>
<thead>
<tr>
<th>Access Authority</th>
<th>Actions Allowed</th>
</tr>
</thead>
</table>
| READ             | • View the properties of the deployment.  
• Copy the properties of the deployment. |
| UPDATE           | In addition to the actions specified for READ access, users can perform the following actions:  
• Modify the deployment properties that are not used to create the SAF resource name for the deployment.  
• Cancel the deployment. This action ends the deployment, unlocks the associated software instances, and limits all future actions for the deployment to **View** and **Remove**. |
| CONTROL          | In addition to the actions specified for READ and UPDATE access, users can perform the following actions:  
• Create new deployments explicitly using the **New** action or implicitly as part of the **Copy** action.  
• Modify the deployment properties that are used to create the SAF resource name for the deployment and control access to the deployment.  
• Remove the deployment. |

Authorizing users to categories

A category is a string or label used to organize and group software instances and deployments. A category might denote a system, subsystem, software vendor, software life cycle state, business function, or geographic location. There are no predefined categories.

To control access to a specific category, define a SAF resource profile for that resource. The SAF resource name for a category object has the following format:

<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.CAT.categoryName

where:

• CAT indicates that the object associated with this SAF resource is a category.  
• categoryName is the name of the category.
For example, if you have a category named z/OS, its SAF resource name would be

<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.CAT.z/OS

Table 20 lists the access authorities you can assign to category resources and the actions that are permitted for each access authority. Note that the Deployment task does not perform authorization checks to determine which categories to display in a list or table; therefore, all categories will be displayed regardless of access authority.

Table 20. Actions users can take against categories by access authority

<table>
<thead>
<tr>
<th>Access Authority</th>
<th>Actions Allowed</th>
</tr>
</thead>
</table>
| READ            | • View the properties of the category.  
                 | • Copy the properties of the category.  
                 | • Assign deployments and software instances to the category. |
| UPDATE          | In addition to the actions specified for READ access, users can perform the following action:  
                 | • Modify the category properties that are not used to create the SAF resource name for the category. |
| CONTROL         | In addition to the actions specified for READ and UPDATE access, users can perform the following actions:  
                 | • Create new categories explicitly using the Add action or implicitly as part of the Copy action.  
                 | • Modify the category properties that are used to create the SAF resource name for the category and control access to the category.  
                 | • Remove the category. |

Using categories to authorize users to groups of software instances and deployments

Because category names are part of the SAF resource name for software instances and deployments, you can use categories to control access to groups of software instances and deployments. For example, if you want to give DB2 system programmers CONTROL access to all software instances and deployments in the DB2 category and give other users READ access to these objects, define a SAF profile for the following resource:

<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.*,DB2.**

If your installation is using RACF and your DB2 system programmers are defined in a group called DB2PROG, you can create a profile like the following:

RDEFINE ZMFAPLA +
(BBNBASE.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.*,DB2.**) UACC(NONE)
PERMIT +
BBNBASE.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.*,DB2.** +
CLASS(ZMFAPLA) ID(DB2PROG) ACCESS(CONTROL)
PERMIT +
BBNBASE.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.*,DB2.** +
CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)
Controlling who can manage categories

By default, z/OSMF users and administrators are authorized to add, copy, modify, and remove categories. However, if you plan to use categories to authorize users to groups of software instances and deployments, it is important to control who can perform these actions. Therefore, it is recommended that you permit READ access to the following resource to z/OSMF administrators or trusted users only:

<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DEPLOYMENT.CATEGORIES.MODIFY

If your installation is using RACF and you want to allow only administrators to perform these actions, you can define a profile like the following:

RDEFINE ZMFAPLA +
(BBNBASE.ZOSMF.SOFTWARE_DEPLOYMENT.DEPLOYMENT.CATEGORIES.MODIFY) +
UACC(NONE)
PERMIT +
BBNBASE.ZOSMF.SOFTWARE_DEPLOYMENT.DEPLOYMENT.CATEGORIES.MODIFY +
CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)

Users who are not permitted at least READ access to this profile can only view a list of the categories and assign categories to software instances and deployments. This is true even if other controls exist that would otherwise allow such a user to perform actions on a specific category.

Ensuring that all objects are assigned to a category

When using categories to control access to groups of software instances and deployments, it is also important to ensure that all software instances and deployments are assigned to a category. To do so, permit no users access to the following resource:

<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DEPLOYMENT.DATA.*.NOCATEGORY.**

If your installation is using RACF and you want to force all objects to be assigned to at least one category, you can define a profile like the following and permit no users to the profile:

RDEFINE ZMFAPLA +
(BBNBASE.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.*.NOCATEGORY.**) UACC(NONE)

Migration considerations for the Deployment task

z/OSMF V1R13 provides support for authorizing users to the Deployment task. No support is provided for controlling user access to specific objects or actions.

If you are using z/OSMF V1R13 and APARs PM40764 and PM50651 are installed, however, support is provided for controlling user access to the task and its objects as previously described. To support these object-level and action-level authorizations, the characters that can be included in the name of a category, software instance, and deployment have been restricted to alphanumeric characters (A-Z, a-z, and 0-9), mathematical symbols (< > = ! \), punctuation marks (? ! : ’ “ /), and special characters ($ _ @ ^ ). These characters ensure that the Deployment task can create valid SAF resource names for each object.

If users have already created software instances, deployments, or categories and your installation chooses to exploit SAF authorization for these objects, your security administrator may not be able to create SAF resource profiles to control
access to any objects where the name contains characters that are no longer valid. To resolve this issue, users can modify the name of those objects and use only the previously mentioned characters.

**Configuring a primary z/OSMF for communicating with secondary instances**

To allow the Deployment task to work with systems on other sysplexes in your installation, you must enable the sharing of digital certificates, as described in this section.

The Deployment task is capable of communicating with a remote instance of z/OSMF, if one is running in another sysplex. In this case, the z/OSMF instance that initiates the communication is considered to be the primary instance because it serves as the repository for the deployment related data at your installation.

The primary instance communicates with the secondary instance through the HTTPS protocol, which requires an exchange of digital certificates. To allow this exchange of certificates, the primary system must be configured to trust the certificate from the secondary system.

This setup involves the following steps:
- "Retrieving the certificate from a secondary system" on page 94.
- "Importing the certificate on the primary system" on page 94.

These steps are not required if the two IBM WebSphere Application Server OEM Edition for z/OS instances are configured to use the same certificate authority (CA). By default, however, each instance creates and uses its own certificate authority and certificates.

Performing these steps will require that you have the information in Table 21 available.

<table>
<thead>
<tr>
<th>Variable name</th>
<th>System</th>
<th>Default value</th>
<th>Your value (if different)</th>
</tr>
</thead>
<tbody>
<tr>
<td>zSSLCaKeylabel</td>
<td>Secondary system</td>
<td>WebSphereCA</td>
<td></td>
</tr>
<tr>
<td>zControlUserId</td>
<td>Secondary system</td>
<td>WSCRU1</td>
<td></td>
</tr>
<tr>
<td>zDefaultSAFKeyringName</td>
<td>Primary system</td>
<td>WASKeyring.BBNBASE</td>
<td></td>
</tr>
<tr>
<td>zServantUserId</td>
<td>Primary system</td>
<td>WSSRU1</td>
<td></td>
</tr>
</tbody>
</table>

These values are contained in the WebSphere Application Server response file, which your installation created earlier when installing IBM WebSphere Application Server OEM Edition for z/OS. There is one response file for each instance of IBM WebSphere Application Server OEM Edition for z/OS at your installation.


**Retrieving the certificate from a secondary system**

On the secondary system, export the certificate that identifies the certificate authority (CA).
Do the following:

1. Export the certificate. In the following example, the export is performed through the RACDCERT command:

   ```
   RACDCERT EXPORT(LABEL('WebSphereCA')) ID(WSCRU1)
   CERTAUTH DSN('WASOEM.CERT.AUTH.DER') FORMAT(CERTDER)
   ```

   In this example:
   - `WebSphereCA` is the name of the key label that identifies the CA to be used in generating server certificates. See the variable zSSLCaKeylabel in the WebSphere response file.
   - `WSCRU1` is the name of the WebSphere application server control region user ID. See the variable zControlUserid in the WebSphere response file.

2. Transfer the WASOEM.CERT.AUTH.DER data set to the primary system in binary format.

   **Importing the certificate on the primary system**

   On the primary system, import the certificate that was exported from the secondary system.

   Do the following:

   1. Import the certificate in the data set into RACF. In the following example, the import is performed through the RACDCERT command:

      ```
      RACDCERT ADD('WASOEM.CERT.AUTH.DER')
      CERTAUTH TRUST WITHLABEL('WebSphereCA–remote_system_ID')
      ```

      Ensure that the label name is unique, otherwise RACF cannot add the certificate. If necessary for ensuring uniqueness, you can add characters to the original label name of the secondary system certificate (a maximum of 32 characters can be used, including blanks and mixed-case characters). In this example, you can replace `remote_system_ID` with some set of characters to help uniquely identify this certificate as the CA from a secondary system.

      The label name is stripped of leading and trailing blanks. If a single quotation mark is intended to be part of the label-name, use two single quotation marks together for each single quotation mark within the string, and enclose the entire string within single quotation marks.

   2. On the primary system, connect the newly imported certificate to the keyring owned by the WebSphere servant identity. In the following example, the connect is performed through the RACDCERT command:

      ```
      RACDCERT CONNECT(CERTAUTH LABEL('WebSphereCA–remote_system_ID'))
      RING(WASKeyring.BBNBASE) USAGE(CERTAUTH) ID(WSSRU1)
      SETROPTS RACLIST(DIGTCERT, DIGTRING) REFRESH
      ```

      In this example:
• WASKeyring.BBNBASE is the default name given to the RACF key ring used by IBM WebSphere Application Server OEM Edition for z/OS. See the variable zSSLCaKeylabel in the WebSphere response file.
• WSSRU1 is the user ID associated with the application server servant. See the variable ServantUserid in the WebSphere response file.
• If your installation does not use RACLIST processing for the DIGTCERT and DIGTRING classes, you can skip the SETROPTS,REFRESH command.

3. Restart the WebSphere server on the primary system to have these changes take effect.

### Updating z/OS for the Workload Management plug-in

This section describes additional steps for authorizing users to specific functions within the Workload Management task.

This section contains the following topics:
- "Controlling authorizations for the MVSADMIN.WLM.POLICY facility"
- "Controlling user authorizations for the Workload Management task" on page 96
- "Migration consideration for the Workload Management task" on page 97.

### Controlling authorizations for the MVSADMIN.WLM.POLICY facility

Users of the Workload Management task require access to the RACF facility MVSADMIN.WLM.POLICY. If your installation runs the Common Information Model (CIM) security setup job, CFZSEC, as part of setting up the CIM server for z/OSMF, all users who are authorized for the CIM server will also be authorized for this RACF facility. If this set of authorizations is acceptable in your environment, no further steps are needed.

However, if not all CIM server users should have access to facility MVSADMIN.WLM.POLICY, you have additional customization to perform to avoid creating unwanted authorizations.

Complete the following steps:
- If you run the job CFZSEC, edit the job before running it to remove any unneeded authorization commands from the job step ENWLM.
- Have your security administrator create a separate group for WLM users. That group needs to have UPDATE access to RACF facility MVSADMIN.WLM.POLICY. If such a group already exists in your environment, you can use the existing group instead of creating a new one.
- During the z/OSMF configuration process, the script prompts you for the name of the WLM group, as follows: Enter the Workload Manager group name, or press Enter to accept "WLMGRP". In response, specify the WLM group name to be used. Alternatively, you can specify this value in your override file on the variable IZU_WLM_GROUP_NAME. As a result, the z/OSMF configuration script is updated to include commands to connect users to the WLM group.

The following example shows how you might create a separate RACF WLM user group and authorize it for the RACF facility MVSADMIN.WLM.POLICY:
1. Create the WLM group:
   ```
   ADDGROUP "WLMGroupName" OMVS(GID("WLMGroupGID"))
   ```
2. Authorize the WLM group:
   ```
   PERMIT MVSADMIN.WLM.POLICY CLASS(FACILITY) ID("WLMGroupName") ACCESS(UPDATE)
   ```
3. Have these changes take effect:
   SETROPTS RACLST(FACILITY) REFRESH
   
   For an additional example, see “Commands for configuring the Workload Management plug-in” on page 288.

Controlling user authorizations for the Workload Management task

The Workload Management task supports the following levels authorization levels, which permit access to functions within the Workload Management task:

View
   This authorization level allows the user to invoke the Workload Management task, and view service definitions, service policies, and WLM status.

Install
   This authorization level allows the user to install service definitions and activate service policies. A user authorized for this level also must be authorized for the View level in order to invoke the Workload Management task.

Modify
   This authorization level allows a user to modify service definitions and to import service definitions from host data sets or local workstation files into z/OSMF. A user authorized for this level also must be authorized for the View level in order to invoke the Workload Management task. To install service definitions and activate service policies, the user must also be authorized for the Install level.

If your installation is running z/OSMF in Repository Authorization Mode, your installation manages user authorizations through the Roles task. For the Workload Management, assign tasks to roles, as shown in Table 22.

Table 22. Workload Management task authorizations when z/OSMF is running in Repository Authorization Mode

<table>
<thead>
<tr>
<th>Required authorization level of role</th>
<th>Task to be selected in the Roles page</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Workload Management</td>
</tr>
<tr>
<td>Install</td>
<td>Workload Management Install</td>
</tr>
<tr>
<td>Modify</td>
<td>Workload Management Modify</td>
</tr>
</tbody>
</table>

By default, z/OSMF administrators are authorized for the View, Install, and Modify functions, which is equivalent to a WLM policy administrator. z/OSMF users are authorized for the function View, which is equivalent to a WLM performance analyst.

If your installation is running z/OSMF in SAF Authorization Mode, you control the authorization through your security management product, for example, RACF. Grant access authority to the appropriate users or groups, as shown in Table 23 on page 97.
Table 23. Workload Management task authorizations when z/OSMF is running in SAF Authorization Mode

<table>
<thead>
<tr>
<th>Required authorization level of user or group</th>
<th>Required SAF access authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>READ access for profile</td>
</tr>
<tr>
<td>Install</td>
<td>READ access for profile</td>
</tr>
<tr>
<td>Modify</td>
<td>READ access for profile</td>
</tr>
</tbody>
</table>

By default, z/OSMF administrators are authorized for the View, Install, and Modify functions. z/OSMF users are authorized for the View function.

If these default settings do not meet your needs, you can change the SAF authority of these respective groups (<IZU_ADMIN_GROUP_NAME> and <IZU_USERS_GROUP_NAME>) for the profiles shown in Table 23 or you can define new custom groups.

For example, the following RACF commands can be used to define a custom group WLMPOLOP that is authorized for the View and Install functions, which is equivalent to a WLM policy operator:

ADDGROUP WLMPOLOP
PERMIT <SAF-prefix>.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.VIEW
  CLASS(ZMFAPLA) ID(WLMPOLOP) ACCESS(READ)
PERMIT <SAF-prefix>.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.INSTALL
  CLASS(ZMFAPLA) ID(WLMPOLOP) ACCESS(READ)
SETROPTS RACLIST(ZMFAPLA) REFRESH

To authorize a user to this group in RACF, you can use a CONNECT command, that is:

CONNECT "userid" GROUP(WLMPOLOP)

Understand that the z/OSMF configuration scripts do not consider any custom groups you might create. To authorize users, you have to connect them to your custom groups manually.

Migration consideration for the Workload Management task

z/OSMF V1R12 supported only one authorization level for the Workload Management task, however, z/OSMF V1R13 supports several authorization levels, as described previously. For a z/OSMF V1R13 migration consideration, see "Verify the user authorizations for the Workload Management task" on page 107.
Chapter 6. Changing the authorization mode for z/OSMF

Your installation can select the authorization mode for z/OSMF when creating the z/OSMF configuration, or at any time afterward. This chapter provides the steps for changing the authorization mode outside of the usual z/OSMF configuration process.

As of z/OSMF V1R13, SAF Authorization Mode is the recommended and default authorization mode for z/OSMF. Your installation should plan for this changed mode, accordingly; see Chapter 3, “Planning security for z/OSMF,” on page 49 for details.

For the steps to convert to SAF Authorization Mode, see “Converting to SAF Authorization Mode.”

If, for some reason, your installation needs to revert to Repository Authorization Mode, see “Converting to Repository Authorization Mode” on page 101 for details.

Converting to SAF Authorization Mode

If your installation is currently running z/OSMF in Repository Authorization Mode, you can convert your existing security setup to SAF Authorization Mode. Doing so will require you to repeat the steps of the z/OSMF configuration process, supplying your current configuration file as input. The z/OSMF configuration process generates new REXX execs, which your security administrator can use to set up security for z/OSMF and authorize additional users to the product. If more than the default set of user authorizations is required, your security administrator is responsible for converting your existing z/OSMF user authorizations to SAF profiles and groups, for use under SAF authorization mode.

The steps in this section assume that:
• You have a valid z/OSMF configuration
• The z/OSMF data file system is mounted
• IBM WebSphere Application Server OEM Edition for z/OS has been started previously.

To switch your current configuration to SAF Authorization Mode, follow these steps:
1. **Stop the WebSphere server.** Ensure that IBM WebSphere Application Server OEM Edition for z/OS is not running. If IBM WebSphere Application Server OEM Edition for z/OS is active, you must enter the appropriate STOP command to shut it down.
2. **Configure z/OSMF as you normally would, but specify SAF Authorization Mode for your configuration.** For example, if you use an override file when configuring z/OSMF, you can specify the authorization mode as a property in your override file, as shown in Figure 18.

```
IZU_AUTHORIZATION_MODE=SAF
```

*Figure 18. Override file updated for SAF Authorization Mode*
Run the `izusetup.sh` script, as follows:
```
izusetup.sh -file izuconfig1.cfg -config
-overriderfile filename.ovr] [-fastpath]
```

where `izuconfig1.cfg` is the configuration file that was used during the initial configuration of z/OSMF. This action will update the configuration file with the new values.

You can include the `-fastpath` option to have the `izusetup.sh` script run without any interactive prompting. Instead, the script uses the values from the configuration file and the override file. Omitted values will cause the script to end with errors.

For reference on the `izusetup.sh` script and the z/OSMF configuration process, see "Step 1: Create the initial configuration" on page 65.

3. **Run the security commands for the new authorization mode.** When you convert an existing z/OSMF configuration to SAF Authorization Mode, the configuration process creates two security commands REXX execs for your use:
   * `izuconfig1.cfg.rexx` contains the complete set of RACF commands for a new configuration.
   * `izuconfig1.cfg.convertFromREPtoSAF.rexx` contains only the delta of security commands of RACF commands that are required for setting up security under SAF Authorization Mode.

   You need run only one of the two execs. Most likely, you will run the conversion exec. If during the preceding step, however, you added more plug-ins to your configuration, use the `izuconfig1.cfg.rexx` exec. Have your security administrator review the contents of the REXX execs before running either.

   With the IZU_CONFIG_DIR directory as your active directory, run the REXX exec. For example:
   ```
   ./izuconfig1.cfg.convertFromREPtoSAF.rexx
   ```

   When running the RACF rexx exec, some commands might fail due to duplicate security settings. You can ignore these messages.

   On completion, the REXX exec creates the security definitions needed for your configuration.

   For reference, see "Step 2: Run the security commands" on page 69.

4. **Verify security for the plug-ins.** Run the `izusetup.sh` script, as follows:
   ```
   izusetup.sh -file izuconfig1.cfg -verify racf
   ```

   For reference, see "Step 3: Verify the RACF security setup" on page 72.

5. **Prime the z/OSMF data file system.** Run the `izusetup.sh` script, as follows:
   ```
   izusetup.sh -file izuconfig1.cfg -prime
   ```

   For reference, see "Step 4: Prime the z/OSMF data file system" on page 73.

6. **Deploy the plug-ins.** From the z/OSMF administrator user ID (ZOSMFAD, by default), run the `izusetup.sh` script, as follows:
   ```
   izusetup.sh -file izuconfig1.cfg -finish
   ```

   This script might take some time to complete. As it runs, the script writes messages to the script log file. For reference, see "Step 5: Complete the setup" on page 75.

   Optionally, you can verify the results of this step by running the `izusetup.sh` script with the `-verify` option for the deployed plug-ins; see "Using the verify function as needed" on page 123.

7. **Restart the WebSphere server.**
Converting to Repository Authorization Mode

Though it is possible to revert to Repository Authorization Mode, it is not recommended. If you had previously converted from Repository Authorization Mode to SAF Authorization Mode, the user authorizations that were last in effect are restored. Any users authorized while running in SAF Authorization Mode will need to be added to z/OSMF in Repository Authorization Mode through the Users task in the z/OSMF navigation area.

The steps in this section assume that you have a valid z/OSMF configuration.

To switch your current configuration to Repository Authorization Mode, follow these steps:

1. **Stop the WebSphere server.** Ensure that IBM WebSphere Application Server OEM Edition for z/OS is not running. If IBM WebSphere Application Server OEM Edition for z/OS is active, you must enter the appropriate STOP command to shut it down.

2. **Configure z/OSMF as you normally would, but specify Repository Authorization Mode for your configuration.** For example, if you use an override file when configuring z/OSMF, you can specify the authorization mode as a property in your override file, as shown in Figure 19.

   Run the `izusetup.sh` script, as follows:
   ```bash
   izusetup.sh -file izuconfig1.cfg -config -overridefile filename.ovr [-fastpath]
   ```

   where `izuconfig1.cfg` is the configuration file that was used during the initial configuration of z/OSMF. This action will update the configuration file with the new values.

   You can include the `-fastpath` option to have the `izusetup.sh` script run without any interactive prompting. Instead, the script uses the values from the configuration file and the override file. Omitted values will cause the script to end with errors.

   For reference on the `izusetup.sh` script and the z/OSMF configuration process, see "Step 1: Create the initial configuration" on page 65.

3. **Determine whether security commands need to be run for the new authorization mode.** When you convert an existing z/OSMF configuration to Repository Authorization Mode, the configuration process creates two security commands REXX execs for your use:

   - `izuconfig1.cfg.rexx` contains the complete set of RACF commands for a new configuration.
   - `izuconfig1.cfg.convertFromSAFtoREP.rexx` contains only the delta of security commands of RACF commands that are required for setting up security under Repository Authorization Mode. Typically, this file is empty, except for comments indicating that no commands are needed. However, if during the previous step, your installation identified new plug-ins to be configured, this exec contains the set of RACF commands that are required for setting up security under Repository Authorization Mode.
Have your security administrator review the contents of the REXX execs to determine whether it is necessary to run either program.

To run an exec, ensure that the IZU_CONFIG_DIR directory is your active directory, and run the REXX exec. For example:

```
./izuconfig1.cfg.convertFromSAFtoREP.rexx
```

On completion, the REXX exec creates the security definitions needed for your configuration.

For reference, see “Step 2: Run the security commands” on page 69.

4. **Verify security for the plug-ins.** Run the `izusetup.sh` script, as follows:

```
izusetup.sh -file izuconfig1.cfg -verify racf
```

For reference, see “Step 3: Verify the RACF security setup” on page 72.

5. **Prime the z/OSMF data file system.** Run the `izusetup.sh` script, as follows:

```
izusetup.sh -file izuconfig1.cfg -prime
```

For reference, see “Step 4: Prime the z/OSMF data file system” on page 73.

6. **Deploy the plug-ins.** From the z/OSMF administrator user ID (ZOSMFAD, by default), run the `izusetup.sh` script, as follows:

```
izusetup.sh -file izuconfig1.cfg -finish
```

This script might take some time to complete. As it runs, the script writes messages to the script log file. For reference, see “Step 5: Complete the setup” on page 75.

Optionally, you can verify the results of this step by running the `izusetup.sh` script with the `-verify` option for the deployed plug-ins; see “Using the verify function as needed” on page 123.

7. **Authorize users to z/OSMF tasks.** In changing to Repository Authorization Mode, you will need to authorize users to z/OSMF again. Your security administrator can use the IBM supplied script, `izauthusers.sh`, and the REXX exec it generates, to authorize more users to z/OSMF. This procedure is described in “Authorizing users to z/OSMF” on page 120.

8. **Restart the WebSphere server.**
Chapter 7. Migrating to a new release of z/OSMF

Migrating to a new release of z/OSMF from an older release is a two-step process. Start by migrating your existing configuration file and override file to the latest format. Then, configure the product as you would normally, supplying the updated configuration and override files as input to the z/OSMF configuration process.

This chapter describes the steps for migrating your configuration file and override file to the latest format, using the IBM-supplied script `izumigrate.sh`. See "Migrating your configuration file and override file" on page 104.

Depending on your current release of z/OSMF, you might also need to perform additional migration actions. For the considerations specific to your particular migration path, see one of the following sections, as appropriate:

- "Migrating from z/OSMF V1R12 to z/OSMF V1R13" on page 106
- "Migrating from z/OSMF V1R11 to z/OSMF V1R13" on page 107

After you have completed these actions, you are ready to configure the new release of z/OSMF on your system. Follow the steps described in Chapter 4, "Configuring z/OSMF," on page 61, which involves running the `izusetup.sh` script through a series of invocations.

When configuring the new release of z/OSMF, use the `izusetup.sh` script in interactive mode, rather than fastpath mode, so that you have the opportunity to verify the settings for your configuration. Running the script in fastpath mode bypasses the prompting for these values. For more information, see "Choosing a script mode: Interactive or fastpath" on page 34.

If you need to add another plug-in to z/OSMF, you can do so during the configuration process, or afterward, as described in "Adding plug-ins to a z/OSMF configuration" on page 124.

Generally, after migrating to a new release of z/OSMF, you should not attempt to revert (fall back) to a previous release of the product. Doing so can result in configuration script errors or a configuration that is difficult to manage. Before attempting a fallback, see "Considerations for reverting to a previous release of z/OSMF" on page 109.

Each new release of z/OSMF can potentially add new plug-ins, thus, it is possible to add plug-ins during the configuration step (`izusetup.sh -config`). If your installation chooses to add plug-ins during a migration, understand that your security administrator will be required to create the user authorizations for the new plug-ins. Generally, this step involves entering a RACF CONNECT command (or its equivalent) to connect users to a group that is permitted to the z/OSMF task resource. By default, the group IZUUSER is permitted to the z/OSMF tasks.
Migrating your configuration file and override file

This section describes the script izumigrate.sh, which allows you to migrate your configuration file and override file to the latest format.

About this script

This script migrates your configuration file, and, if specified, your override file from a previous release of z/OSMF to the latest format.

In updating the configuration file and override file, the script retains your current settings when possible. For any properties that are no longer valid for z/OSMF, the script omits the properties when creating the updated files.

If your existing configuration file contains commented sections (it should not; the configuration is not intended to be edited by your installation), the script removes this information from the updated configuration file.

If you choose to migrate an existing override file, understand that:

- The script processes only the properties that are specified in the override file. The script does not add any new properties to the updated override file.
- The script determines the version of the override file by examining the override file property IZU_OVERRIDE_FILE_VERSION. This property, which was introduced in z/OSMF V1R12, should not be modified. If this property is missing from the override file, the script processes the override file as though it had originated from a z/OSMF V1R11 configuration. If this property is set incorrectly in the override file, the script fails with an error message.
- If your existing override file contains user comments, these commented sections are retained in the updated override file, though the placement of these sections might change as a result of the migration processing, which removes properties that no longer apply.

You can migrate the configuration file and override file together in one invocation of this script. Or, if you prefer, you can migrate these files individually by running separate invocations of the script.

Other outputs from the script are the following:

- The script records the results of the migrate operation in the migration report file. You can review this file to see what settings were changed during the migrate operation, and what new properties are available.
- The script saves backup copies of your current configuration and override files, for historical purposes.

For the contents of the configuration file and override file that were supplied in this release of z/OSMF, see Appendix D, “Default configuration file and default override file,” on page 255.
Format

```bash
izumigrate.sh -file izuconfig1.cfg
izumigrate.sh -overridefile izudflt.ovr
izumigrate.sh -file izuconfig1.cfg -overridefile izudflt.ovr
```

*Figure 20. izusetup.sh syntax*

**Running this script**

**Authority**

Run this script from a user ID with superuser authority or from the z/OSMF administrator user ID that you created previously (ZOSMFAD, by default). You should have superuser authority if you plan to do additional configuration steps without changing user IDs.

**Environment**

Run the script in either an OMVS or telnet/rlogin session. You cannot run it from ISHELL.

**Location**

The script resides in the following directory:

```
<IZU_CODE_ROOT>/bin
```

**Invocation**

Run the script, as follows:

```
izumigrate.sh -file izuconfig1.cfg
[-overridefile izudflt.ovr]
```

Where:

- `izuconfig1.cfg` is the configuration file from a previous release of z/OSMF. This file is expected to reside in the z/OSMF configuration directory `<IZU_CONFIG_DIR>`.
- `izudflt.ovr` identifies an override file from a previous release of z/OSMF. You can choose another name for this file, but the `.ovr` file type is required. This file is expected to reside in the z/OSMF configuration directory `<IZU_CONFIG_DIR>`.

The script saves the updated files, along with a backups of your current files, to the directory specified on the `IZU_CONFIG_DIR` configuration variable. By default, this is `/etc/zosmf`.

As the script runs, it writes log information to the z/OSMF log file directory, which is identified by the `IZU_LOGFILE_DIR` environment setting for the UNIX shell. By default, this directory is `/var/zosmf/configuration/logs/`.

**Results**

On completion, the `izumigrate.sh` script migrates your configuration file to the correct format for the new release of z/OSMF. If you included an override file as input, the script migrates the override file in a similar manner.

As part of this processing, the script creates backups of your existing files, using a file name qualifier to help you correlate the backups with the particular release of z/OSMF. If your installation is migrating from z/OSMF V1R12, for example, the script creates backup files named `izuconfig1.cfg.V1R12` and `izudflt.ovr.V1R12`. If
your installation is migrating from z/OSMF V1R11, the script creates backup files named izuconfig1.cfg.V1R11 and izudflt.ovr.V1R11.

In the event that your installation needs to regress to an older level of z/OSMF, you can rename these files to their original names and use them again in the regressed configuration. For related information, see "Considerations for reverting to a previous release of z/OSMF" on page 109.

The script also creates a report file named izumigration.report. The report file records the actions that were taken to migrate your configuration and override files—the settings that have been modified, removed, or added between releases. The report file is divided into two sections, one for the configuration file and one for the override file, if applicable.

You can view the migration report file in the <IZU_LOGFILE_DIR> directory, which is the location identified by the IZU_LOGFILE_DIR environment setting for the UNIX shell. By default, this is /var/zosmf/configuration/logs/. The location of the migration report file is also provided in an informational message that is written to the script log file.

**Sample migration report file**

For your reference, a sample migration report is shown in Appendix K, “Example of the migration report,” on page 291. In this example, the report file records the results of updating the configuration file and the override file from the z/OSMF V1R12 format to the z/OSMF V1R13 format.

---

### Migrating from z/OSMF V1R12 to z/OSMF V1R13

If you are migrating from z/OSMF V1R12 to z/OSMF V1R13, see the following topic for additional considerations:

- "Migrating the CIM server security setup from z/OSMF V1R12"

---

**Migrating the CIM server security setup from z/OSMF V1R12**

Previously, in z/OSMF V1R12, the z/OSMF configuration process included the option of creating sample RACF authorizations for the Common Information Model (CIM) server on your z/OS system. To request this setup, you responded yes (Y) to the configuration script prompt "Do you need assistance in setting up security for the Common Information Model (CIM) server?" or specified Y for the variable IZU_CIM_CONFIGURE in your override file. If so, the z/OSMF configuration process included additional prompts to allow you to create the CIM related authorizations for z/OSMF V1R12.

Beginning in z/OSMF V1R13, z/OSMF no longer includes the option to create sample security authorizations for the CIM server. The configuration variable IZU_CIM_CONFIGURE is removed. Instead, IBM recommends that you perform this setup using the CFZSEC job, which is provided with CIM. For the steps needed to perform this action, see the chapter on CIM server quick setup and verification in z/OS Common Information Model User’s Guide SC33-7998.

In migrating your z/OSMF V1R12 configuration file and migration file to the latest format, z/OSMF removes the CIM-related values from these files. If CIM setup is required for a specific plug-in, the z/OSMF configuration process prompts you for the CIM-related groups, and adds these values to the security exec that is created for your configuration, so that users can be connected to the CIM-related groups.
For the specific configuration settings that are changed or removed in z/OSMF V1R13, and for recommendations on migrating an existing RACF setup for the CIM server, see the report that is generated from the `izumigrate.sh` script.

**Verify the setting for authorization mode**

In updating your configuration file from a previous release of z/OSMF, the `izumigrate.sh` script adds a setting for the authorization mode (IZU_AUTHORIZATION_MODE) and sets it to REPOSITORY. Later, during the configuration process, you can change this setting the SAF, if you prefer to operate z/OSMF in SAF Authorization Mode instead.

**Remove the SURROGAT class profiles for z/OSMF V1R12**

When your installation configured z/OSMF V1R12, the z/OSMF configuration process included RACF commands for creating the SURROGAT class profile `BB0.SYNC.<user ID>` for the administration user ID and for any other user IDs you might have authorized. You can remove these profiles as part of the migration to z/OSMF V1R13.

**Verify the user authorizations for the Workload Management task**

As described in “Updating z/OS for the Workload Management plug-in” on page 95, z/OSMF V1R13 supports several authorization levels for the Workload Management task. In z/OSMF V1R12, however, only one authorization level was supported. Thus, when migrating from z/OSMF V1R12 to z/OSMF V1R13, a mapping of authorization levels occurs.

The default authorization for the Workload Management task in V1R12 is to allow access for the z/OSMF Administrator role only. In V1R13, the z/OSMF Administrator role has access to all functions in the Workload Management task, and the z/OSMF User role has View access.

After a conversion from V1R12 to V1R13, z/OSMF Administrators will have all access, and z/OSMF Users will have View access.

If your z/OSMF Administrator has manipulated the default roles in Repository Authorization Mode, and later converts to SAF Authorization Mode, the conversion REXX exec will contain commented commands that define the adjustments made. For information about to creating a custom authorization for z/OSMF users to the appropriate SAF profiles, see “Controlling user authorizations for the Workload Management task” on page 96.

**Migrating from z/OSMF V1R11 to z/OSMF V1R13**

If you are migrating from z/OSMF V1R11 to z/OSMF V1R13, see the following topics for additional considerations:

- “Migrating the CIM server security setup from z/OSMF V1R11” on page 108
- “Ensure that no links exceed 4000 characters” on page 109
- “Remove the SURROGAT class profiles for z/OSMF V1R11” on page 109.
Migrating the CIM server security setup from z/OSMF V1R11

Previously, in z/OSMF V1R11, the z/OSMF configuration process included options for configuring the Common Information Model (CIM) server on your z/OS system. This setup work included customizing the z/OS system for the CIM server and creating sample authorizations for your security product. In z/OSMF V1R13, these options are removed. Instead, you are advised to configure the CIM server manually, according to the procedures and jobs described in the CIM publications.

CIM server configuration in z/OSMF V1R11: In z/OSMF V1R11, the z/OSMF configuration process included the option to perform the CIM related system customization, if desired. To request this setup in z/OSMF V1R11, you responded no (N) to the configuration script prompt "Has the Common Information Model (CIM) server been set up? [Y/N]", or specified N for the variable IZU_CIM_SETUP in your override file. Also, if you selected to configure the Incident Log task, the z/OSMF configuration process created the corresponding security authorizations for the CIM server.

What has changed in z/OSMF V1R13: Beginning in z/OSMF V1R13:

- z/OSMF no longer includes an option to set up the CIM server on your system; the configuration variable IZU_CIM_SETUP is removed. Instead, you must perform this setup using the CFZRCUST job, which is provided with CIM.
- z/OSMF no longer includes an option to create sample security authorizations for the CIM server during the configuration process. Instead, you must create the CIM-related security authorizations using the CFZSEC job, which is provided with CIM.

For the steps needed to perform these actions, see the chapter on CIM server quick setup and verification in z/OS Common Information Model User’s Guide SC33-7998.

If you allowed the z/OSMF configuration process to set up the CIM server in z/OSMF V1R11, be aware that the CIM server was set up to run as a z/OS UNIX process, not as a started task, as recommended in z/OS Common Information Model User’s Guide SC33-7998.

In migrating your z/OSMF V1R11 configuration file and migration file to the latest format, z/OSMF removes the CIM-related values from these files. Also, the z/OSMF configuration process no longer adds the CIM-related authorizations to the security exec that is created for your configuration.

For the specific configuration settings that are changed or removed in z/OSMF V1R13, and for recommendations on migrating an existing RACF setup for the CIM server, see the report that is generated from the izumigrate.sh script.

Verify the setting for authorization mode

In updating your configuration file from a previous release of z/OSMF, the izumigrate.sh script adds a setting for the authorization mode (IZU_AUTHORIZATION_MODE) and sets it to REPOSITORY. Later, during the configuration process, you can change this setting the SAF, if you prefer to operate z/OSMF in SAF Authorization Mode instead.
Ensure that no links exceed 4000 characters

Your installation can customize the z/OSMF navigation area with links to external sites for system management tools and information. In z/OSMF V1R11, you could specify a link location of up to 4096 characters. In z/OSMF V1R12, the character limit is decreased to 4000 characters.

If your installation customized z/OSMF V1R11 with additional links, examine the link locations to determine whether any exceed 4000 characters. As of z/OSMF V1R12, attempting to modify such links will result in error message IZUG603E.

For any links that exceed 4000 characters, determine whether a shorter Uniform Resource Locator (URL) can be substituted, and, if so, modify the link location accordingly through the Links task. A valid link location can be up to 4000 ASCII characters and must be a syntactically correct URL.

For information about adding links, see the z/OSMF online help for the Links task.

Remove the SURROGAT class profiles for z/OSMF V1R11

When your installation configured z/OSMF V1R11, the z/OSMF configuration process included RACF commands for creating SURROGAT class profiles for the z/OSMF administrator (BPX.SRV.ZOSMFAD.SURROGAT) and for each authorized user (BPX.SRV.<userid>.SURROGAT). As of R12, the Common Information Model (CIM) server no longer uses these profiles. You can remove them as part of the migration to z/OSMF V1R13.

Similarly, the z/OSMF configuration process previously included RACF commands for creating the SURROGAT class profile BBO.SYNC.<user ID> for the administration user ID and for any other user IDs you might have authorized. In z/OSMF V1R13, you can remove these profiles.

Considerations for reverting to a previous release of z/OSMF

Generally, after your installation migrates to a new release of z/OSMF, it is not advisable to revert (fall back) to a previous release of the product. Each new release of z/OSMF adds functions and enhancements that might not be available on an older release, or might not operate in the expected manner. Attempting to fall back to an older release can result in configuration script errors or a configuration that is difficult to manage. Before attempting a fallback, see this section for considerations.

The configuration process is unique in each release of the product. It is not possible to run the latest configuration scripts on a downlevel release of z/OSMF, nor is it possible to restore an older release of z/OSMF by transferring the z/OSMF data file system from the older release to a new IBM WebSphere Application Server OEM Edition for z/OS instance.

Though not recommended, reverting to an older release of z/OSMF is possible. If this capability is required at your installation, ensure that you create a backup of the older release file systems before migrating to the new release. Specifically you must save the following file systems:

- The z/OSMF data file system. This is the directory mount point that was specified on the IZU_DATA_DIR variable during the configuration process. See Table 7 on page 36.
The IBM WebSphere Application Server OEM Edition for z/OS configuration file system. Usually, this file system is mounted at /usr/lpp/zWebSphereOEM/V7R0, but your installation might have specified another location for it. Check the WebSphere response file for variable zConfigHfsName, which defaults to BBN.V7R0.CONFIG1.ZFS.

Here, you would also rename the backup configuration file and, if applicable, override file to the original names to use these files as before (see “Results” on page 105).

In the event that your installation needs to regress to an older level of z/OSMF, you can remount the saved file systems at their original mount points and begin using the older configuration. Understand that reverting to an older release in this manner means losing any functions or configuration changes specific to the new release.

If the original file systems are no longer available, falling back to an older release will require that you recreate the file systems. That is, by rerunning the WASOEM.sh -create script to create the WebSphere file system, and repeating the z/OSMF configuration steps, from the izusetup.sh -config script onward, to create the z/OSMF data file system.
Chapter 8. Multiple instances of z/OSMF

Your installation can choose to create more instances of z/OSMF, for example, to have a backup instance of z/OSMF available for switchover or testing purposes. This chapter describes the considerations for configuring, modifying, and using multiple z/OSMF instances. There are restrictions for the co-existence and co-operation of multiple instances of z/OSMF, so it is important to understand the limitations and considerations of this approach.

Planning for an additional instance of z/OSMF

Before creating another instance of z/OSMF, you should have already created primary instances of IBM WebSphere Application Server OEM Edition for z/OS and z/OSMF.

To create additional instances of z/OSMF on other systems, you can rerun the izusetup.sh script on those systems. Based on the security policies for your environment and the security requirements of specific deployed plug-ins, you can configure your backup instance of z/OSMF to use the same RACF user IDs and groups as your primary instance.

You should use unique configuration file names for each new instance that you create. The unique names enable the files to be persisted, and easily associated with the instance to which it applies.

Consider the following:

- If your primary instance of z/OSMF uses a shared data file system (that is, with a shared mount point and volume) and is read/write accessible from other systems in the sysplex, you will have fewer steps to follow to configure a backup instance of z/OSMF and to perform a switchover from the primary instance of z/OSMF to the backup. If you use a shared security database, the switchover procedure is further simplified because the backup instance can use the same user IDs and groups as your primary instance.

- If your primary instance of z/OSMF uses a non-shared data file system (one that is only read/write accessible from only the host z/OS system), switchover from the primary instance of z/OSMF to the backup will require that you unmount the data file system on the primary host z/OS system and mount it on the backup system.

Planning for a z/OSMF switchover

The act of transferring control from one system to another (a backup system) upon the failure of the primary system is called switchover. You perform a switchover manually, in contrast to a failover, which occurs automatically.

Performing a switchover will involve transferring your z/OSMF data file system from the failed instance to the backup instance. This is the directory mount point that was specified on the IZU_DATA_DIR configuration variable (by default, /var/zosmf/data).
Creating a backup instance of z/OSMF for switchover will require creating another instance of IBM WebSphere Application Server OEM Edition for z/OS on the backup system. You should configure this instance with identical settings as much as possible.


Restrictions on using additional instances

You can have only one instance of z/OSMF active in a system or sysplex at any given time. Multiple users can log into the same instance of z/OSMF using different computers, different browsers, or multiple instances of the same browser.

Though you can have only one instance of z/OSMF active in a sysplex, you can create additional instances of z/OSMF on other systems. You might do this, for example, for testing purposes, or for backup in case of system failure.

Observe the following restrictions for using additional instances of z/OSMF in your environment:

- You can have only one instance of z/OSMF per instance of IBM WebSphere Application Server OEM Edition for z/OS.
- The z/OSMF data file system can be used by only a single instance of z/OSMF in a sysplex at a given time.

To prevent the same z/OSMF data file system from being accessed by more than one instance of z/OSMF at a time, z/OSMF locks the data file system through a global resource serialization ENQ with QNAME ZOSMF. If you start a second instance of z/OSMF using the same data file system, that z/OSMF will not be usable. Users who attempt to access the second instance of z/OSMF will encounter a z/OSMF error web page (message IZUG680E). Further, all log messages from the second instance of z/OSMF are routed to the WebSphere log, rather than to the log in the z/OSMF data file system.

- Do not list the QNAME ZOSMF ENQ in the resource name list (RNL) in your installation’s GRSRNLxx member.
- Running multiple instances of z/OSMF simultaneously in a sysplex, using different z/OSMF data file systems, is not recommended. Consider, for example, that the Incident Log task is sysplex-wide in scope; it manages dumps in the sysplex dump directory. If users attempt to access the Incident Log task from different instances of z/OSMF at the same time, significant delays and resource contentions might result.

Scenarios for switchover

This section describes the following scenarios for using a backup instance of z/OSMF in your environment:

- “Switchover between z/OSMF V1R13 systems” on page 113
- “Switchover between mixed releases of z/OSMF” on page 114

In these scenarios, it is assumed that you have already have an operating instance of z/OSMF on your primary system (“SYS1”), based on the steps described in Chapter 4, “Configuring z/OSMF,” on page 61.
**Switchover between z/OSMF V1R13 systems**

In this scenario, the objective is to be able to bring up z/OSMF on a backup z/OSMF system ("SYS2") where it will use the same data file system from the primary z/OSMF system.

In this scenario:
- Two systems, SYS1 and SYS2, exist in the same sysplex. SYS1 is the primary system and SYS2 is the backup system.
- On the primary system, the data file system was created on a shared volume accessible by both SYS1 and SYS2.

To enable this type of switchover, your installation must ensure that the backup system is maintained as a “mirror” of the primary system. This includes having the same:
- Service levels
- File systems and mount points.

**Setting up the backup system in this scenario**

This section describes the steps for setting up a backup system. Follow these steps to ensure that a backup system is available for switchover when you need one.

1. Stop IBM WebSphere Application Server OEM Edition for z/OS on the primary system, if it is active.
2. If the data file system is not mounted at a shared mount point, the data file system must be unmounted. On the primary system, enter:
   ```bash
   /usr/sbin/unmount <IZU_DATA_DIR>
   ```
   where `<IZU_DATA_DIR>` is the mount point for the data file system.
3. Setup the backup system, that is, perform all of the steps to set up IBM WebSphere Application Server OEM Edition for z/OS and z/OSMF on SYS2. Use the configuration file from the primary system to configure z/OSMF on SYS2. If the data file system is not already mounted on a shared mount point, running configuration scripts on SYS2 will cause the data file system to be mounted.
4. Start IBM WebSphere Application Server OEM Edition for z/OS on the backup system and ensure that z/OSMF is operational.
   Now switch back to the primary system, as follows.
5. Stop IBM WebSphere Application Server OEM Edition for z/OS on the backup system, if it is active.
6. If the data file system is not mounted at a shared mount point, unmount it and remount it on the primary system. On the backup system, enter:
   ```bash
   /usr/sbin/unmount <IZU_DATA_DIR>
   ```
   where `<IZU_DATA_DIR>` is the mount point for the data file system.
7. On the primary system, enter:
   ```bash
   /usr/sbin/mount -f <IZU_DATA_FS_NAME> <IZU_DATA_DIR>
   ```
   where:
   - `<IZU_DATA_FS_NAME>` is the data file system name
   - `<IZU_DATA_DIR>` is the mount point for the data file system.
8. Start IBM WebSphere Application Server OEM Edition for z/OS on the primary system.
Procedure for switchover in this scenario

When a switchover is necessary, follow these steps:

1. Stop IBM WebSphere Application Server OEM Edition for z/OS on the primary system, if it is active.

2. If the data file system is not mounted on a shared mount point, you must unmount the data file system on the primary system and mount it on the backup system. On the primary system, enter:
   
   ```
   /usr/sbin/unmount <IZU_DATA_DIR>
   ```

   where `<IZU_DATA_DIR>` is the mount point for the data file system.

   On the backup system, enter:
   
   ```
   /usr/sbin/mount -f <IZU_DATA_FS_NAME> <IZU_DATA_DIR>
   ```

   where:
   - `<IZU_DATA_FS_NAME>` is the data file system name
   - `<IZU_DATA_DIR>` is the mount point for the data file system.


4. To verify, open a browser to z/OSMF on the backup system.

Switchover between mixed releases of z/OSMF

For switchover between z/OSMF on different releases of z/OSMF, understand that the configuration files are different. In each new release of z/OSMF, properties are added, removed, or changed in the configuration file, and the product can have more potential plug-ins. Running the `izusetup.sh` script in `-config` mode with input configuration file from the primary system will result in a modified configuration file on the backup system. As a result, it might not be possible for an older release of z/OSMF to serve as an exact backup for a newer release.

You must ensure that:

- Owners and groups assigned to the directories in the data file system on the primary system are applicable to the backup system.
- If your security database is not shared, the same users are authorized on the backup system.

To switchover to z/OSMF on the backup system, do the following:

1. Stop IBM WebSphere Application Server OEM Edition for z/OS on the primary system, if it is active.

2. If the data file system is not mounted on a shared mount point, unmount the data file system from the primary system and mount it on the backup system.
   
   a. On the primary system, enter:
      
      ```
      /usr/sbin/unmount <IZU_DATA_DIR>
      ```

   b. On the backup system, enter:
      
      ```
      /usr/sbin/mount -f <IZU_DATA_FS_NAME> <IZU_DATA_DIR>
      ```

      where:
      - `<IZU_DATA_FS_NAME>` is the data file system name
      - `<IZU_DATA_DIR>` is the mount point for the data file system.


4. To verify, open a browser to z/OSMF on the backup system.
Handling of tasks and links during a switchover to a lower level of z/OSMF

If your installation switches over to a lower level release of z/OSMF, the tasks and links are handled in the following manner:

- The tasks that are supported on the back-up system's level of z/OSMF will remain in the navigation area. Tasks that require the primary instance of z/OSMF will not be displayed in the navigation area. For the tasks that are preserved, these tasks retain the user assignments from the primary instance of z/OSMF.
- All installation-specified links are preserved on the back-up system’s level of z/OSMF. If the back-up system is z/OSMF V1R11, these are displayed under the Links category in the navigation area, regardless of whether your installation assigned the links to another category on the primary instance of z/OSMF.

On resumption of the primary instance of z/OSMF, the tasks and your installation-specified links are restored to their original assignments and placements in the navigation area.
Part 3. Administration

Administering z/OSMF includes the following topics:

- Chapter 9, “Post-configuration work for the z/OSMF administrator,” on page 119
- Chapter 10, “Performing administration tasks in z/OSMF,” on page 135
- Chapter 11, “Troubleshooting,” on page 143.
Chapter 9. Post-configuration work for the z/OSMF administrator

After you have configured a working instance of z/OSMF on your system, you have subsequent tasks to perform, such as authorizing users to z/OSMF. You might also want to further customize z/OSMF with more links and plug-ins, as required by your installation.

This section describes the following tasks:
- “Authorizing users to z/OSMF” on page 120
- “Using the verify function as needed” on page 123
- “Adding plug-ins to a z/OSMF configuration” on page 124
- “Updating plug-ins after service is applied” on page 127
- “Customizing the Welcome page for guest users” on page 128
- “Adding links through the izusetup.sh script” on page 131

Authorities needed after configuration

After the z/OSMF configuration process, you will require the authorities shown in Table 24 to perform subsequent work.

Table 24. Authorities needed after z/OSMF has been configured.

<table>
<thead>
<tr>
<th>Action to perform and where described</th>
<th>Invocation</th>
<th>Performed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Creating the commands to authorize a user ID” on page 120</td>
<td>izauthuser.sh -file izuconfig1.cfg -userid USERID</td>
<td>z/OSMF administrator</td>
</tr>
<tr>
<td>“Authorizing a user ID” on page 121</td>
<td>&lt;IZU_CONFIG_DIR&gt;/izuconfig1.USERID.rexx</td>
<td>Security administrator</td>
</tr>
<tr>
<td>“Using the verify function as needed” on page 123</td>
<td>izusetup.sh -file izuconfig1.cfg -verify option</td>
<td>z/OSMF administrator</td>
</tr>
<tr>
<td>“Updating plug-ins after service is applied” on page 127</td>
<td>izusetup.sh -file izuconfig1.cfg -service</td>
<td>z/OSMF administrator</td>
</tr>
<tr>
<td>“Customizing the Welcome page for guest users” on page 128</td>
<td>Not applicable.</td>
<td>z/OSMF administrator</td>
</tr>
<tr>
<td>“Adding links through the izusetup.sh script” on page 131</td>
<td>izusetup.sh -file filename.cfg -addlink &lt;pathname/link-properties-filename&gt;</td>
<td>z/OSMF administrator</td>
</tr>
</tbody>
</table>
Authorizing users to z/OSMF

This section describes the steps for authorizing an existing z/OS user ID to the z/OS components required for z/OSMF operations. This work includes running the izauthuser.sh script to create a REXX exec with RACF commands for authorizing the user, and running that exec.

These programs are described in the following topics:
- “Creating the commands to authorize a user ID” on page 121
- “Authorizing a user ID” on page 121

The resulting REXX exec is tailored for your z/OSMF configuration, based in part on your selection of the authorization mode to be used for z/OSMF. Observe the following considerations:
- If your installation selected SAF Authorization Mode (the default), you will need to examine the REXX exec, and choose an appropriate group for the user. As supplied by IBM, the REXX exec connects the user ID to the USER group, but includes commented commands for connecting the user ID to other groups, too.
- If your installation selected Repository Authorization Mode for this z/OSMF configuration, you have an additional step to complete for this user after running the REXX exec. The z/OSMF administrator must add the user in z/OSMF and assign the appropriate role through the Users task. For information, see “Performing administration tasks in Repository Authorization Mode” on page 137.

If you add more plug-ins to your z/OSMF configuration later, you must re-run the izauthuser.sh script and the generated rexx exec. Doing so can result in an "overlap" of RACF commands, for the previous set of plug-ins and the newly added plug-ins. Your security administrator should handle these situations accordingly.

The z/OSMF configuration process includes a resource called <zSAFProfilePrefix>.izuNOUsers, where <zSAFProfilePrefix> is the SAF profile prefix defined in the IBM WebSphere Application Server OEM Edition for z/OS configuration (BBNBASE by default). This resource is intended for z/OSMF internal use only; do not define this profile in the EJBRULE class, nor grant users access to it.

Creating the commands to authorize a user ID

This section describes script izauthuser.sh, which allows you to create a REXX exec with RACF commands for authorizing a user ID to the z/OS components used in z/OSMF operations.

About this script

This script creates a REXX exec with RACF commands for authorizing a user ID to the z/OS components used in z/OSMF operations.

Running this script

Authority

Run this script from the z/OSMF administrator user ID that you created previously (ZOSMFAD, by default).
 Environment
Run the script in either an OMVS or telnet/rlogin session. You cannot run it from ISHELL.

 Location
The script resides in the following directory:
<IZU_CODE_ROOT>/bin

where <IZU_CODE_ROOT> is the product file system. By default, this is /usr/lpp/zosmf/V1R13.

 Invocation
From your shell session, run the script, as follows:
izuauthuser.sh -file izuconfig1.cfg -userid USERID

 Where:
• izuconfig1.cfg is the configuration file that you created previously in "Step 1: Create the initial configuration" on page 65.
• USERID is the existing user ID for which the RACF commands are to be created.

 Results
On completion, this script creates sample RACF commands in the following file:
<IZU_CONFIG_DIR>/izuconfig1.USERID.rexx

where <IZU_CONFIG_DIR> is the configuration file system. By default, this is /etc/zosmf.

You can view the script output messages in the following log file:
<IZU_LOGFILE_DIR>/izuauthuser_<mddyy>_<hhmmss>.log

where <IZU_LOGFILE_DIR> is the log file directory for your installation. By default, this is /var/zosmf/configuration/logs/.

 Authorizing a user ID
This section describes the REXX exec izuconfig1.USERID.rexx. In short, this exec contains sample RACF commands for authorizing a user ID to the z/OS components used in z/OSMF operations.

 About this exec
This REXX exec contains sample RACF commands that your installation's security administrator can use to authorize a user ID to the z/OS components used in z/OSMF operations.

The content of this REXX exec is tailored based on your z/OSMF configuration. If you configured z/OSMF with the Incident Log task and the Workload Manager task, for example, the resulting REXX exec will include the necessary RACF commands for authorizing a user ID to those tasks.

If your installation uses a security management product other than RACF, your installation must create equivalent commands for your security product.
Before running the exec

These commands should be reviewed by your security administrator and modified as needed for your installation's environment.

Running this exec

Have your installation's security administrator review the RACF commands in this exec, modify them as necessary, and run the exec to issue the commands.

Authority
   This exec is run by your installation's security administrator.

Environment
   Run the script in either an OMVS or telnet/rlogin session. You cannot run it from ISHELL.

Location
   The exec resides in the configuration file system (IZU_CONFIG_DIR). By default, this is /etc/zosmf.

Invocation
   From an OMVS session, do the following:
     1. Make the IZU_CONFIG_DIR directory your active directory. For example:
        cd /etc/zosmf
     2. Run the exec, as follows:
        ./izuconfig1.cfg

Tip: By default, no log file is created. If you want a log file, you can use a z/OS UNIX command, such as tee, to direct the output from this exec to a log file. If so, you could direct this output to the z/OSMF log file directory for your installation (IZU_LOGFILE_DIR). By default, this is /var/zosmf/configuration/logs/. For example:

    izuconfig1.cfg.USERID.rexx | tee
    /var/zosmf/configuration/logs/izuconfig1.cfg.USERID.rexx.output

For techniques, see z/OS UNIX System Services User’s Guide SA22-7801.

Results

On completion, this exec creates the security definitions for the user ID on the z/OS system. If your installation is running z/OSMF in Repository Authorization Mode, the z/OSMF administrator must later complete this authorization on the product level by adding the user and assigning the appropriate role in z/OSMF. For information, see “Performing administration tasks in Repository Authorization Mode” on page 137.
Using the verify function as needed

After you have configured a working instance of z/OSMF on your system, you can optionally verify your configuration by running the `izusetup.sh` script with the `-verify` option. You can perform this action as often as needed, whenever you want to verify your z/OSMF configuration.

To verify your configuration, run the `izusetup.sh` script with the `-verify` option, as described in “Step 3: Verify the RACF security setup” on page 72. To select the scope of the verification, include one of the options shown in Table 25 with the `-verify` option.

**Table 25. Script options for verification**

<table>
<thead>
<tr>
<th>Script option</th>
<th>Scope of verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Verifies that all of the selected plug-ins were deployed. Also, if you selected to configure the Incident Log plug-in, this option runs the installation verification program (IVP) for verifying the z/OS system setup for the Incident Log task.</td>
</tr>
<tr>
<td>core</td>
<td>Verifies that the core functions were initialized.</td>
</tr>
<tr>
<td>log</td>
<td>Verifies that the Incident Log plug-in was deployed. This option also runs the installation verification program for verifying the z/OS system setup for the Incident Log task.</td>
</tr>
<tr>
<td>racf</td>
<td>Verifies the RACF security setup for all of the configured tasks and functions.</td>
</tr>
</tbody>
</table>

For example:

```
izusetup.sh -file izuconfig1.cfg -verify all
```

where `izuconfig1.cfg` is the configuration file that you created previously in “Step 1: Create the initial configuration” on page 65. If you omit the directory path, the script uses the z/OSMF configuration directory `<IZU_CONFIG_DIR>`, by default.

The script checks that all necessary configuration steps were carried out.

On completion, you can view the script output messages in the following log file:

```
<IZU_LOGFILE_DIR>/izusetup_verify.mm.dd.yy.hh.mm.ss.tt.log
```

where `<IZU_LOGFILE_DIR>` is the log file directory for your installation. By default, this is `/var/zosmf/configuration/logs/`.

If your installation has configured the Incident Log plug-in, this script can help you verify the setup of z/OS system components. If you run the script with the options all, log, or racf, the script the creates a report indicating any areas that might require further action on your part. The report resides in the following location:

```
<IZU_LOGFILE_DIR>/izuincidentlogverify.report
```

where `<IZU_LOGFILE_DIR>` is the log file directory for your installation. By default, this is `/var/zosmf/configuration/logs/`.

For more information, see “Reviewing the results of the izuincidentlogverify.report file” on page 162.
Adding plug-ins to a z/OSMF configuration

After you have configured a working instance of z/OSMF on your system, you might choose to modify the configuration later by adding more plug-ins. If so, you can use the `izusetup.sh` script to add the plug-ins, repeating the steps you followed earlier to configure the z/OSMF product.

After a plug-in is configured, you can remove it from z/OSMF only by repeating the configuration process and not selecting that plug-in.

Preparing for new plug-ins

For any plug-ins to be added, ensure that you have performed the appropriate z/OS system set-up actions and gathered the required information. See the applicable sections of “System prerequisites for the z/OSMF plug-ins” on page 24 and “Planning worksheets for z/OSMF” on page 35.

To add plug-ins to z/OSMF, you will run the `izusetup.sh` script with a series of options, repeating the steps you followed earlier to configure the z/OSMF product. The script resides in the `/bin` subdirectory of the z/OSMF product file system. This location is set through the `IZU_CODE_ROOT` variable in your global settings; the default is `/usr/lpp/zosmf/V1R13/bin`.

To run the script, you require a user ID with superuser authority. Run the script in either an OMVS or telnet/rlogin session. You cannot run it from ISHELL.

The script uses your current configuration file as input.

Steps for adding plug-ins to z/OSMF

Configure z/OSMF as you normally would, but specify the new plug-ins for your configuration. You can add plug-ins in response to the script prompts, or through an override file.

To add plug-ins to z/OSMF, follow these steps:

1. **If you are using an override file:** If you use an override file when configuring z/OSMF, you can specify the new plug-ins as properties in your override file. Here, you would mark the plug-ins to be added with the character `A`. Alternatively, you can skip this step and allow the script to prompt you for your plug-in selections.

   Figure 21 shows an override file that was used to configure z/OSMF previously. In this example, only the Incident Log plug-in was included in the configuration.

   ```plaintext
   IZU_IL_CONFIGURE=Y
   IZU_CA_CONFIGURE=N
   IZU_WLM_CONFIGURE=N
   IZU_RMF_CONFIGURE=N
   IZU_CP_CONFIGURE=N
   IZU_DM_CONFIGURE=N
   IZU_WISPF_CONFIGURE=N
   ```

   **Figure 21. Sample override file**

   The example in Figure 22 on page 125 shows the same override file updated to add the Capacity Provisioning task to a z/OSMF configuration. For
documentation purposes, the installation retained the previous setting — IZU_CP_CONFIGURE=N — in a commented line in the override file.

```plaintext
IZU_IL_CONFIGURE=Y
IZU_CA_CONFIGURE=N
IZU_WLM_CONFIGURE=N
IZU_RMF_CONFIGURE=N
#
# commenting out the previous setting for the Capacity Provisioning task:
# IZU_CP_CONFIGURE=N
#
# New setting for Capacity Provisioning task follows...
IZU_CP_CONFIGURE=A
IZU_DM_CONFIGURE=N
IZU_WISPF_CONFIGURE=N
```

**Figure 22. Sample override file**

Configuring z/OSMF with the override file shown in Figure 22 would indicate that you want to add the Capacity Provisioning plug-in to your z/OSMF configuration.

2. Run the `izusetup.sh` script, as follows:

```bash
izusetup.sh -file izuconfig1.cfg -config
[-overridefile filename.ovr] [-fastpath] -add
```

where `izuconfig1.cfg` is the configuration file that was used during the initial configuration of z/OSMF. You will overwrite this file.

You can include the `-fastpath` option to have the `izusetup.sh` script run without any interactive prompting. Instead, the script uses the values from the configuration file and the override file. Omitted values will cause the script to end with errors.

If you run the script in interactive mode, and have specified “A” values in the override file for the plug-ins to be added, the script prompts you to either accept what was specified in the override file, or modify your plug-in selections.

If you omit the override file, the script prompts you for the plug-ins to be added. You are prompted only for plug-ins that are not already deployed in your configuration. Respond to the prompt with one or more of the following plug-in identifiers:

1. Incident Log plug-in
2. Configuration Assistant plug-in
3. Workload Management plug-in
4. Resource Monitoring plug-in
5. Capacity Provisioning plug-in
6. Software Deployment plug-in
7. ISPF plug-in
N None (no plug-ins). You might use this option if you change your mind about adding plug-ins.

For multiple selections, separate each plug-in identifier with a comma.

If the script displays a prompt for the DASD Management plug-in, do not select it. This plug-in is not available for use.

On completion, the `izusetup.sh` script creates a REXX exec with RACF commands for creating the security definitions for your installation. The exec name is a concatenation of your configuration file name, the plug-ins you selected, and ".rexx". If you use "izuconfig1.cfg" as your configuration file name, and add two plug-ins, the exec is created as:

`izuconfig1.cfg.add.<plug-in-1>.<plug-in-2>.rexx`
The exec is stored in the IZU_CONFIG_DIR directory.

For reference on the izusetup.sh script and the z/OSMF configuration process, see “Step 1: Create the initial configuration” on page 65.

3. **Run security commands for the plug-ins.** The REXX exec izuconfig1.cfg.rexx contains sample RACF commands that your installation's security administrator can use to secure the plug-ins. Have your security administrator review the contents of the exec before running it.

With the IZU_CONFIG_DIR directory as your active directory, run the exec, as follows:

```
./izuconfig1.cfg.add.xxx.rexx
```

where xxx is the short name of the plug-in. If you are adding multiple plug-ins, the exec name will include the short name for each plug-in, for example:

```
izuconfig1.cfg.add.IL.CA.WLM.RMF.DM.rexx
```

**Tip:** If you want a log file, you can use a z/OS UNIX command, such as tee, to direct the output from this exec to a log file. For example, you could direct this output to the z/OSMF log file directory for your installation (IZU_LOGFILE_DIR). By default, this is /var/zosmf/configuration/logs/.

On completion, this exec creates the security definitions needed for the plug-in configuration.

For reference, see “Step 2: Run the security commands” on page 69.

4. **Verify security for the plug-ins.** If your installation uses RACF as its security management product, perform this step. Otherwise, skip this step and, instead, take the appropriate steps to verify your security setup.

Run the izusetup.sh script, as follows:

```
izusetup.sh -file izuconfig1.cfg -verify racf
```

For reference, see “Step 3: Verify the RACF security setup” on page 72.

5. **Prime the data file system.** Run the izusetup.sh script, as follows:

```
izusetup.sh -file izuconfig1.cfg -prime -add
```

For reference, see “Step 4: Prime the z/OSMF data file system” on page 73.

6. **Deploy the plug-ins.** From the z/OSMF administrator user ID (ZOSMFAD, by default), run the izusetup.sh script, as follows:

```
izusetup.sh -file izuconfig1.cfg -finish -add
```

This script might take some time to complete. As it runs, the script writes messages to the script log file. For reference, see “Step 5: Complete the setup” on page 75.

Optionally, you can verify the results of this step by running the izusetup.sh script with the -verify option for the deployed plug-ins; see “Using the verify function as needed” on page 123.

### Additional setup for plug-ins

Depending on which plug-ins you deploy, you might have additional steps to perform. For information, see Chapter 5, “Additional steps for setting up your z/OS system,” on page 81.
Updating plug-ins after service is applied

After applying PTFs to z/OSMF, you might be required to run the `izusetup.sh` script with the `-service` option to refresh your deployed plug-ins. Use the `-service` option when directed to do so by the instructions in the ++HOLD action of a PTF, or at the direction of IBM Support.

About this script

As input to the script, you will specify the z/OSMF configuration file for your current setup. The script reads the configuration file to determine which plug-ins are deployed on your system, and updates the EAR files for those plug-ins.

For each plug-in, the script compares the build version of the currently deployed plug-in with the build version of the plug-in that is supplied with the PTF. If the PTF contains a different version of the plug-in, the script undeploys the existing plug-in and deploys its replacement in the instance of IBM WebSphere Application Server OEM Edition for z/OS on your system. The script also refreshes the online help information for the plug-in.

If no updates from the PTF are applicable to your deployed plug-ins, running this script will have no adverse effect.

Before running this script

Before running the script, check the PTF for instructions to follow when the service is installed. Usually, you can run this script regardless of whether WebSphere is running or stopped.

This script might take several minutes or more to complete. If the script times out, the problem might be related to a CPU time limit on your z/OS system. Consider overriding the CPU time limit for this invocation of the script. Your system includes a number of controls for limiting CPU usage; use the appropriate command, consistent with the standard practices at your installation.

Running this script

Authority

Run this script from the z/OSMF administrator user ID that you created previously (ZOSMFAD, by default).

Environment

Run the script in either an OMVS or telnet/rlogin session. You cannot run it from I$HELL.

Storage allocation

Your user ID should have at least two gigabytes (2 GB) of storage allocated for its use. For information, see "Ensuring that your user ID has enough storage" on page 64.

Location

The script resides in the following directory:

`<IZU_CODE_ROOT>/bin`

where `<IZU_CODE_ROOT>` is the product file system. By default, this is `/usr/lpp/zosmf/V1R13`. 

Chapter 9. Post-configuration work for the z/OSMF administrator 127
Invocation

From your shell session, run the script, as follows:
izusetup.sh -file izuconfig1.cfg –service

where izuconfig1.cfg is the name of the configuration file used to save your configuration settings. The configuration file is stored in the directory specified on the IZU_CONFIG_DIR configuration variable. If you installed z/OSMF as part of a ServerPac order, the configuration file is named serverpac.cfg.

Results

You can view the script output messages in the following log file:
<IZU_LOGFILE_DIR>/izusetup_service.mm-dd.yyyy.hh.mm.ss.sss.log

where <IZU_LOGFILE_DIR> is the log file directory for your installation. By default, this directory is /var/zosmf/configuration/logs/.

In some cases, you might need to restart IBM WebSphere Application Server OEM Edition for z/OS after running the script; check the instructions for the PTF.

To verify the updated build levels of the plug-ins, display the About page for z/OSMF. See “Finding information about z/OSMF” on page 152.

Customizing the Welcome page for guest users

Your installation can customize the content of the z/OSMF Welcome page for non-authenticated guest users. You might do so, for example, to provide users with information they should read before logging in to z/OSMF, such as instructions specific to your company. You can even add a small image or graphic, such as your company logo. After the guest user authenticates, the Welcome page is replaced with the standard z/OSMF Welcome page.

What can be customized

You can customize the following areas of the Welcome page:

**Header area**
- Horizontal area above the main work area

**Footer area**
- Horizontal area below the main work area

**Image area**
- Small area at the right end of the footer.

Figure 23 on page 129 shows the areas of the z/OSMF Welcome page that can be customized.
As shown in Figure 23, the header and footer areas are styled to appear raised from the Welcome page. If you supply an image file, it is included at the right end of the footer area. In Figure 23, the IBM logo is shown in this position.

**Steps for customizing the Welcome page**

A sample Welcome page properties file is supplied with z/OSMF:

```
<IZU_CODE_ROOT>/samples/customWelcome.properties
```

where `<IZU_CODE_ROOT>` is the product file system. By default, this is `/usr/lpp/zosmf/V1R13`.

To customize the Welcome page, follow these steps:

1. **Copy the sample Welcome properties file to the correct location.** Copy the sample Welcome properties file to the z/OSMF data file system directory. You specified this directory on the IZU_DATA_DIR configuration variable (by default, the directory is `/var/zosmf/data`).

   It is recommended that you copy the file using the z/OSMF administrator user ID that you created previously during the configuration process. Doing so ensures that the files are stored with the correct ownership and permissions, as follows:
   - File owner is the z/OSMF administrator user ID (ZOSMFAD, by default)
   - Owning group is the z/OSMF administrator group (IZUADMIN, by default)
   - File permissions are a minimum of 440.

   Your Welcome page properties file must be named `customWelcome.properties`. This name is case sensitive.
If you create a symlink for the properties file, ensure that the file exists and is readable. Otherwise, the file is ignored.

2. **Edit the new Welcome properties file with your text.** As shown in Figure 24, the Welcome properties file contains the following input fields for the customizable areas:

```
header=
footer=
```

*Figure 24. Content of the Welcome page properties file*

You can specify your text for the header area and footer area, using an editor of your choice. In each area, you can specify up to 128 characters of content, including alphanumeric characters (A-Z a-z 0-9), blanks, mathematical symbols (+ - = \ ~ | ), punctuation marks (? , . ! ; ' " / ] ), and the following special characters: %, $, #, @, ^, *, and _. If you exceed this limit, this area is truncated at 128 characters.

Specify your input in the form of the ASCII, EBCDIC or Unicode character sets. Do not specify HTML coding; it is ignored. To use Japanese language characters, enter the characters in Unicode. Each Unicode character (\uxxxx) is treated as one character.

As an example, Figure 25 shows the Welcome page properties file that was used to customize the Welcome page in Figure 23 on page 129.

```
header=This is a header
footer=This is a footer
```

*Figure 25. Example of a Welcome page properties file*

3. **Add an image file, if required.** If you include an image file, such as your company logo, it must be named customLogo and have one of the following image formats: .png, .jpeg, .jpg, .gif, or .bmp. The required name and file type is case sensitive. Other names, if specified, are ignored. If you provide multiple image types, the priority order is: .png, .jpeg, .jpg, .gif, and .bmp.

The image size is limited to the area allotted on the Welcome page, which is about 120x40 pixels. A larger image will be scaled down to that size. A smaller image is not scaled up to that size.

Store the image file in the z/OSMF data file system directory, with the same ownership and permissions as done for the Welcome properties file in Step 1.

If the image file you supply is empty or corrupted, z/OSMF displays the following alternate text in place of the image:

```
Custom Company Logo
```

4. **View your changes.** Refresh your browser to display the customized Welcome page.
Adding links through the izusetup.sh script

Generally, when you want to add a link to z/OSMF, you should use the Links task in the z/OSMF navigation area. In some situations, however, you might be asked at the direction of a vendor to add a link to z/OSMF through the izusetup.sh script. If so, follow the steps in this section.

You can add only one link for each invocation of the izusetup.sh script.

To modify or remove a link after it is added, you must use the Links task in the z/OSMF navigation area. For information, see “Defining links for z/OSMF” on page 135.

Before running the script

Ensure that IBM WebSphere Application Server OEM Edition for z/OS is running. Otherwise, the new link is not added until after IBM WebSphere Application Server OEM Edition for z/OS is started.

To start IBM WebSphere Application Server OEM Edition for z/OS, enter the appropriate START command. For more information about starting and stopping IBM WebSphere Application Server OEM Edition for z/OS, see IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide, GA32-0631.

Steps for adding a link to z/OSMF

A sample link properties file is supplied with z/OSMF:

<IZU_CODE_ROOT>/samples/sampleLink.properties

where <IZU_CODE_ROOT> is the product file system. By default, this is /usr/lpp/zosmf/V1R13.

To add a link to the z/OSMF navigation area, follow these steps:

1. **Make a copy of the sample link properties file.** Copy the sample link properties file to a read/write directory.

2. **Edit the new link properties file with your text.** As shown in Figure 26, the link properties file contains the following input fields for a link:

   ```
   LinkName=
   LinkURL=
   LinkNavigationCategory=
   LinkAuthorizedRoles=
   LinkSafSuffix=
   LinkLaunchWorkArea=
   ```

   **Figure 26. Content of the link properties file**

   In your link properties file, define the link using these input fields:

   **LinkName**
   Specify a name for the link, as it should be displayed in the z/OSMF navigation area. Specify a value of up to 30 characters, including alphanumeric characters (A-Z a-z 0-9), blanks, mathematical symbols (+ - = | ~ ( ) { } \), punctuation marks (? , ! ; : ' ” / ] ), and the following special characters: %, $, #, ^, *, and _. Any leading or trailing white space is ignored.
Specify your input in the form of the ASCII, EBCDIC or Unicode character sets. To use Japanese language characters, enter the characters in Unicode. Each Unicode character (\uxxxx) is treated as one character.

The name you select must be unique among the existing links defined in z/OSMF. It is recommended that you choose a name that will be easily understood by users. Avoid names that might be confused with other links or tasks in z/OSMF.

**LinkURL**

Specify the location for the link (a URL), which is a valid Internet or intranet address, for example:

```
http://www.ibm.com
```

The URL can be up to 4000 characters, including alphanumeric characters (A-Z a-z 0-9), blanks, mathematical symbols (+ - = | ~ ( ) [ ] \), punctuation marks (? . ! ; : ’ ” / [ ]), and the following special characters: %, $, #, @, ^, *, and _. Any leading or trailing white space is ignored.

z/OSMF performs limited syntax checking of the specified URL. Ensure that the link location is a syntactically correct URL. Generally, a URL includes a protocol (such as http://), a host name (www.hostname.com), and, often, a resource such as a directory path and file.

**LinkNavigationCategory**

Specify the navigation area category to which the link is to be assigned. You can assign the link to any valid category in the z/OSMF navigation area. The link is sorted alphabetically with the other links and tasks in the category.

To indicate the category, specify one of the following values:

1  z/OSMF Administration
2  Problem Determination
3  Links
4  Configuration
5  Software
7  z/OS Classic Interfaces
9  Performance

You can specify one category only. Any leading or trailing white space is ignored.

**LinkAuthorizedRoles**

Specify the z/OSMF roles for which users are authorized to use the link. You can limit access to users with one or more of the following roles:

- z/OSMF Guest
- z/OSMF Authenticated Guest
- z/OSMF User
- z/OSMF Administrator

Enter the role name exactly as depicted here. To specify multiple roles names, separate each name with a comma. Any leading or trailing white space is ignored.

If you specify a role incorrectly, the role is ignored. If you specify no roles at all, or omit this property, the script adds the link to the table displayed in the Links task with no roles assigned to it.
**LinkSafSuffix**

Specify the system authorization facility (SAF) resource name suffix to be used for managing user authorizations to the link. To create a unique resource name for the link, z/OSMF appends this value to the WebSphere SAF profile prefix (by default, BBNBASE), followed by ZOSMF:LINK. Specify a unique resource name suffix, for example: BBNBASE:ZOSMF.LINK.mylink

You can specify a suffix of up to 220 alphanumeric characters (A-Z a-z 0-9) and the following special characters: underscore (_), dash (-), period (.). The use of a period in a resource name is treated as a qualifier. As such, the first character after a period must be A-Z or a-z.

When z/OSMF is operated in SAF Authorization Mode, ZOSMF:LINK.* is the default generic profile for protecting access to links.

You must provide a unique SAF resource name suffix for each link, even if your z/OSMF configuration is running in Repository Authorization Mode. z/OSMF uses the resource name for locating and identifying links.

**LinkLaunchWorkArea**

Specify how the link is to open in the user’s z/OSMF session, as follows:

- To have the link open in the user’s session as a separate window or tab, set this value to FALSE. The link will open in the user’s browser as a new window or tab, based on the user’s browser settings.
- To have the link open as a tab in the z/OSMF work area, like a z/OSMF task, set this value to TRUE.

Any other value is ignored and FALSE is used by default.

If you choose to have the link open as z/OSMF tab, verify that the link will work as intended in the z/OSMF work area. You might find that some links display better in a separate browser window or tab. Also, some external web sites might cause the user’s browser window to be re-sized or even redirect the browser to a new destination, rather than opening in the z/OSMF work area. Therefore, it is strongly recommended that you verify the general usage of the link in the z/OSMF work area before directing users to use the link.

Figure 27 shows an example of a completed link definition.

<table>
<thead>
<tr>
<th>LinkName=IBM</th>
</tr>
</thead>
<tbody>
<tr>
<td>LinkURL=<a href="http://www.ibm.com">http://www.ibm.com</a></td>
</tr>
<tr>
<td>LinkNavigationCategory=3</td>
</tr>
<tr>
<td>LinkAuthorizedRoles=z/OSMF Guest, z/OSMF User</td>
</tr>
<tr>
<td>LinkSafSuffix=IBM_COM</td>
</tr>
<tr>
<td>LinkLaunchWorkArea=false</td>
</tr>
</tbody>
</table>

Figure 27. Example of a link definition

3. **Add the link to z/OSMF.** From the z/OSMF administrator user ID (ZOSMFAD, by default), run the izusetup.sh script, as follows:

   ```bash
   izusetup.sh -file filename.cfg -addlink <pathname/link-properties-filename>
   ```

Figure 28. Syntax for adding a link to z/OSMF
where link-properties-filename is your link properties file.
This script might take some time to complete.

**Processing your request**

As it processes, the script writes messages to standard output and to the script log file:
<IZU_LOGFILE_DIR>/izusetup_addlink.mm.dd.yy.hh.mm.ss.tt.log

where <IZU_LOGFILE_DIR> is the log file directory for your installation. By default, this is /var/zosmf/configuration/logs/.

Check the messages to determine whether a problem occurred during -addlink processing. If so, you must resolve the problem before the link can be added.

If the WebSphere server is down, you must restart the WebSphere server to complete the processing of your request; see message IZU398I.

**Results**

On completion, the script issues message IZUG397I, which directs you to check the z/OSMF runtime log file (IZUGx.log) for an indication of whether the link was added. For more information, see “Working with z/OSMF runtime log files” on page 152.

More information about usage considerations is provided in “Defining links for z/OSMF” on page 135.
Chapter 10. Performing administration tasks in z/OSMF

z/OSMF includes one user ID that is authorized to access z/OSMF as the product administrator. With this user ID, a person designated by your installation to act as the z/OSMF administrator can log into z/OSMF and perform administration tasks, as needed.

The responsibilities of the z/OSMF administrator depend on the authorization mode that your installation selects for z/OSMF. In Repository Authorization Mode, the z/OSMF Administrator holds the following responsibilities:

- Assigning users to roles through the Users task
- Assigning tasks to roles through the Roles task
- Managing links through the Links task
- Controlling user access to links through the Roles task.

In SAF Authorization Mode, user and role assignments are managed entirely through the groups and profiles defined in your security product. The z/OSMF Administrator is responsible only for managing links through the Links task in the z/OSMF navigation area. In this mode, the z/OSMF Administrator does not manage user authorizations, and thus, the Users task and the Roles task are not displayed in the navigation area.

To display the z/OSMF administration tasks, expand the z/OSMF Administration category in the navigation area. To perform an administration task, select the appropriate task from the following list:

- **z/OSMF Links.** Select this task to manage your z/OSMF links. For an overview, see "Defining links for z/OSMF."
- **z/OSMF Application Linking Manager.** Select this task to manage associations between the z/OSMF tasks. For an overview, see "Linking z/OSMF tasks and external applications" on page 136.

The Users and Roles tasks are available in Repository Authorization Mode only. For an overview, see "Performing administration tasks in Repository Authorization Mode" on page 137.

### Defining links for z/OSMF

Your installation can customize z/OSMF with links to external sites for system management tools and information. This allows you to have a single launch point for all of your z/OS management web applications.

The process of defining a link to z/OSMF includes:

- Specifying the link name and its location (a URL)
- Providing a system authorization facility (SAF) resource name to be used for managing user authorizations to the link.
- Selecting a z/OSMF category for the link.
- Specifying how the link opens in the user’s browser session: As a new browser window or tab, or as a tab in the z/OSMF work area.
- Managing access to the link for guest users.
To display the Links task, expand the z/OSMF Administration category in the navigation area and select Links to begin a sequence of steps for defining links for z/OSMF. You can add links to any category in the navigation area.

Note: Some useful links were provided with the installation of z/OSMF. In the Japanese language version of z/OSMF, these links are not translated.

For more assistance with the Links task, see the online help for this task.

Authorizing users to links

How users are authorized to links, and whether the authorization is performed in your security management product or through the Links task, depends on the authorization mode that is in effect for your installation, as follows:

- In SAF Authorization Mode, a link in the z/OSMF navigation area is treated as a resource. Your installation must determine whether access to a link should be limited to certain users or unrestricted. Users are authorized to links by your security administrator, who creates groups and profiles for accessing link in your security management product.
- In Repository Authorization Mode, a link is assigned to a role by the z/OSMF Administrator through the Links task.

Preservation of links through migration and fallback

Installing a new release of z/OSMF will preserve any installation-specific links that you have defined.

If you fall back from your current level of z/OSMF to a previous level, observe the following considerations:

- If you fall back to a z/OSMF V1R11 system, your link definitions are retained, but are displayed in the Links category, regardless of which categories were specified for the links.
- If you fall back to a z/OSMF V1R12 or V1R11 system, links always open in a z/OSMF window, even if you specified another launch behavior for the link.

Linking z/OSMF tasks and external applications

To perform z/OS management tasks, typically, you interact with several different interfaces, such as the TSO command line, graphical user interfaces, and web-style interfaces. To help you link or connect your z/OSMF tasks and external applications, z/OSMF provides the Application Linking Manager task.

Key components

The key components of the Application Linking Manager task include the:

- **Event requestor.** z/OSMF task or external application that requests the launch of a specific function within another task or external application
- **Event.** Action requested by the event requestor. It includes the type of event and the event parameters.
- **Event type.** Object that connects an event requestor to an event handler. It identifies the handlers that can process an event and the possible parameters that can be supplied with an event.
- **Event handler.** z/OSMF task or external application that can process the event parameters and display the requested information.
Figure 29 depicts the relationship of these components in the application linking process.

![Diagram of application linking process]

Figure 29. Key components in the application linking process

The process begins with a user action, such as clicking a link. In response to this action, the event requestor creates an event and sends it to the Application Linking Manager. The Application Linking Manager searches the set of known event types for the type identified by the event. If a match is found, the Application Linking Manager searches for event handlers that are registered for this event type. If only one handler is found, it is launched. Otherwise, the user is prompted to select the handler to launch. The Application Linking Manager provides the handler with the parameters that were supplied with the event. The event handler processes the parameters and displays the requested information.

**Key features**

To open the Application Linking Manager task, in the navigation area, expand the z/OSMF Administration category and select Application Linking Manager. The task provides a web-based, user interface that you can use to:

- Define new event types, and view and delete existing event types.
- Define new handlers; view, enable, disable, and delete existing handlers; and make a handler the default handler.

For more assistance with this task, see the online help for the Application Linking Manager task.

**Programming interface**

The Application Linking Manager task also provides an application programming interface (API) that you can use to complete the aforementioned actions. For more details about the API, see Chapter 13, “Using the Application Linking Manager interface services,” on page 211.

**Performing administration tasks in Repository Authorization Mode**

This topic describes the administration tasks that are available if your installation has selected to run z/OSMF in Repository Authorization Mode.

To display the z/OSMF administration tasks, expand the z/OSMF Administration category in the navigation area.

Figure 30 on page 138 shows the Welcome page that is displayed to the z/OSMF Administrator in Repository Authorization Mode.
To perform an administration task, select the appropriate task from the following list:

- z/OSMF Application Linking Manager. Select this task to manage associations between the z/OSMF tasks.
- z/OSMF Links. Select this task to manage your z/OSMF links.
- z/OSMF Roles. Select this task to view and modify z/OSMF roles.
- z/OSMF Users. Select this task to define new z/OSMF users and to modify or delete existing z/OSMF users.

In Repository Authorization Mode, user authorizations are defined by the z/OSMF administrator in z/OSMF and enabled on the host system by your security administrator. This earlier form of authorization is replaced by SAF Authorization Mode in z/OSMF V1R13, but remains supported as an alternative form of authorization.

When defining roles and users to z/OSMF through the z/OSMF administration tasks, the z/OSMF administrator must ensure that a user's authority on z/OSMF is sufficient within the user's existing authority on the z/OS host system. If not, the user's authorization on the z/OS system takes precedence over the user's authorization in z/OSMF.

**Defining links in Repository Authorization Mode**

Using the Links task, the z/OSMF Administrator can customize the z/OSMF navigation area with additional links.
To display the Links task, expand the z/OSMF Administration category in the navigation area and select Links to begin a sequence of steps for defining links for z/OSMF. You can add links to any category in the navigation area.

To define links for z/OSMF, your user ID must be assigned to a role that is permitted to define links. By default, only the z/OSMF Administrator role can define links.

For information about the Links task, see “Defining links for z/OSMF” on page 135.

Enabling roles in Repository Authorization Mode

Enabling roles in z/OSMF involves the separate actions of selecting tasks for the role (through the Roles task) and assigning users to the role (through the Users task).

Figure 31 shows the main page for the Roles task.

<table>
<thead>
<tr>
<th>IBM z/OS Management Facility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome</td>
</tr>
<tr>
<td>Roles</td>
</tr>
</tbody>
</table>

Use this panel to view and modify z/OSMF roles.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>z/OSMF Administrator</td>
<td>User can perform all tasks defined within z/OSMF</td>
</tr>
<tr>
<td>z/OSMF Authenticated Guest</td>
<td>User is logged into z/OSMF, however, no role is associated with the user's user ID</td>
</tr>
<tr>
<td>z/OSMF Guest</td>
<td>User is not logged into z/OSMF</td>
</tr>
<tr>
<td>z/OSMF Storage Administrator</td>
<td>User can perform all storage tasks defined within z/OSMF</td>
</tr>
<tr>
<td>z/OSMF User</td>
<td>User can perform tasks that are not defined as z/OSMF administration tasks</td>
</tr>
</tbody>
</table>

z/OSMF filters the list of tasks shown in the navigation area to match the authorization of the assigned role for the current user. If a role is not authorized to work with certain tasks, those tasks are not displayed in the navigation area for users assigned to the role.
To work with roles for z/OSMF, your user ID must be assigned to a z/OSMF role that is permitted to the Roles task. By default, only the z/OSMF Administrator role can work with roles.

When defining roles in z/OSMF through the z/OSMF administration tasks, the z/OSMF administrator must ensure that a user’s authority in z/OSMF is sufficient within the user’s authority on the z/OS host system. If not, the user’s authorization on the z/OS system takes precedence over the user’s authorization in z/OSMF.

Understand that z/OSMF does not prevent you from modifying the role or the user definition with which you are currently logged on to z/OSMF. If you remove the Roles task from the role definition to which your user id is assigned, for example, you lose the authority to continue working with the Roles task. Here, z/OSMF performs the change and issues messages to:

- Confirm the modification of the role definition
- Indicate that you are not authorized to use the Roles task.

To work with roles in z/OSMF, expand the z/OSMF Administration category in the navigation area and select Roles. Doing so will begin a sequence of steps for defining which tasks are assigned to a z/OSMF role. For assistance with this task, see the online help for the Roles task.

Managing guest users in Repository Authorization Mode

Your installation can manage the access of guest users to z/OSMF tasks through the Roles task by modifying the roles z/OSMF Guest and z/OSMF Authenticated Guest.

A non-authenticated guest user can access the z/OSMF Welcome task and access the z/OSMF provided links. An authenticated guest can access everything a non-authenticated guest can, and also view the online help.

It is not possible to designate a user as a non-authenticated or authenticated guest user, for example, through the Users task.

Defining users in Repository Authorization Mode

On the Users page, you define a user by specifying the user ID, user name, and role. By specifying a role for the user, you authorize this person to perform the tasks that are associated with that role.

Figure 32 on page 141 shows the main page for the Users task.
To define users for z/OSMF, your user ID must be assigned to a z/OSMF role that is permitted to the Users task. By default, only the z/OSMF Administrator role can define users.

For any new users to be added, verify that your installation’s security management product (for example, RACF) will permit the user to access the system resources needed to perform a particular task. If necessary, contact your installation’s security administrator to authorize the user.

For help with establishing the required security setup for the user, your installation’s security administrator can refer to the configuration scripts that are provided with z/OSMF. The scripts contain sample RACF commands for authorizing users and groups to system resources. For information about the z/OSMF configuration process, see Chapter 4, “Configuring z/OSMF,” on page 61.

The z/OSMF configuration process creates an initial administrator user ID. With this user ID, the administrator can log into z/OSMF and add more users and administrators as needed, through the Users task.

To work with user definitions in z/OSMF, click on the z/OSMF Administration category in the navigation area and select Users. Doing so will begin a sequence of steps for defining one or more users to z/OSMF. For more assistance with this task, see the online help.
Chapter 11. Troubleshooting

This chapter provides troubleshooting tips for common problems. Included are procedures and methods for performing problem determination and for determining the status of the different components.

This chapter is organized into major topics, as follows:
- "Resources for troubleshooting"
- "Tools and techniques for troubleshooting" on page 144
- "Common problems and scenarios" on page 155

Resources for troubleshooting

z/OSMF is composed of a number of system "layers," each maintaining a different set of diagnostic information. Some errors that are intercepted at the lowest system levels can surface at the user interface layer. Some errors appear as messages in a CIM log, and others might be issued as standard z/OS messages to the system logs (SYSLOG or OPERLOG).

Table 26 shows a summary of the diagnostic tools and data available for each of the layers in the z/OSMF stack and references for locating the information.

Table 26. Summary of tools and information for troubleshooting problems with z/OSMF

<table>
<thead>
<tr>
<th>Component or task</th>
<th>Tools to assist with troubleshooting</th>
<th>Where described</th>
<th>Associated messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workstation and web browser</td>
<td>Environment checker tool</td>
<td>&quot;Verifying your workstation with the environment checker&quot; on page 144.</td>
<td>N/A</td>
</tr>
<tr>
<td>z/OSMF core functions and system management tasks</td>
<td>• The About page</td>
<td>• Finding information about z/OSMF on page 152</td>
<td>IBM z/OS Management Facility Messages SA38-0654.</td>
</tr>
<tr>
<td></td>
<td>• z/OSMF log files and tracing</td>
<td>• Working with z/OSMF runtime log files on page 152</td>
<td>For Configuration Assistant, messages and pop-ups are supplied with the task.</td>
</tr>
<tr>
<td></td>
<td>• z/OSMF log files and tracing</td>
<td>• Problems when using Configuration Assistant on page 174.</td>
<td></td>
</tr>
<tr>
<td>IBM WebSphere Application Server OEM Edition for z/OS</td>
<td>• WebSphere FFDC log files (sysout, HFS)</td>
<td>• Enabling tracing and logging for z/OSMF on page 153.</td>
<td>• IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide GA32-0631</td>
</tr>
<tr>
<td></td>
<td>• WebSphere tracing</td>
<td></td>
<td>• IBM z/OS Management Facility Messages SA38-0654.</td>
</tr>
<tr>
<td>CIM server and CIM providers</td>
<td>• CIM server logging</td>
<td>These options are defined in the CIM server configuration properties and set through the cimconfig command; see z/OS Common Information Model User’s Guide SC33-7998.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CIM server trace</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CIM provider trace</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Common event adapter (CEA)</td>
<td>System commands: • MODIFY CEA</td>
<td>z/OS MVS System Commands, SA22-7627.</td>
<td>z/OS MVS System Messages for information about: • WTO messages • CTRACE • Reason codes.</td>
</tr>
<tr>
<td></td>
<td>• MODIFY AXR</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• TRACE CT</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For information about resolving problems with IBM WebSphere Application Server OEM Edition for z/OS, see IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide GA32-0631.
Tools and techniques for troubleshooting

This section describes the tools and techniques available for troubleshooting problems with IBM z/OS Management Facility (z/OSMF).

Verifying your workstation with the environment checker

To work with z/OSMF, your web browser and workstation require a number of settings for proper functioning. z/OSMF includes an environment checker tool to help you verify these settings. The environment checker tool inspects your web browser and workstation operating system for compliance with z/OSMF requirements and recommended settings.

Before running the tool

Check to ensure that your workstation is set up correctly for z/OSMF. See “Preparing your workstation for z/OSMF” on page 46.

Ensure that your browser is enabled for JavaScript. For instructions, see Table 28 on page 146 or Table 29 on page 148, as appropriate.

Running the tool

To run the tool, do the following:

1. Open a web browser to the environment checker tool:

   https://hostname:port/zosmf/IzuUICommon/environment.jsp

   where:
   - hostname is the hostname or IP address of the system on which z/OSMF is installed
   - port is the secure application port.

   To find the hostname and port, see the link for z/OSMF in message IZUG349I. This message was written to the log file that was created when you ran the izusetup.sh script with the -finish option, as described in “Step 5: Complete the setup” on page 75. This log file is in the format:

   <IZU_LOGFILE_DIR>/izusetup_finish.mm.dd.yy.hh.mm.ss.tt.log

   where <IZU_LOGFILE_DIR> is the log file directory for your installation. By default, this directory is /var/zosmf/configuration/logs/.

2. Follow the instructions for your particular browser in the online help for the tool.
Understanding the results of the tool

Table 27 describes the layout of the environment checker report.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment Option</td>
<td>Browser setting that was examined by the environment checker tool.</td>
</tr>
<tr>
<td>Settings as of date-time</td>
<td>Findings from the most recent invocation of the tool. This column indicates potential problems with your browser.</td>
</tr>
</tbody>
</table>

In the column heading, the date and time (date-time) is represented in ISO 8601 format, a standard provided by the International Organization for Standardization (ISO). In this format:

- Calendar date is represented in year-month-day format (yyyy-mm-dd).
- Time of day (T) is based on the 24-hour clock: hh:mm:ss:mmm.
- Z indicates zero offset from coordinated universal time (UTC).

In the report, the status of each setting is indicated, as follows:

- **Items marked with a critical icon X**
  Setting is not correct for z/OSMF. You must fix this problem before continuing with z/OSMF.

- **Items marked with a warning symbol !**
  Setting is not optimal for z/OSMF. It is recommended that you update the setting before continuing with z/OSMF.

- **No error indication**
  Setting is correct for z/OSMF.

For the steps to resolve a problem, see the appropriate entry in the tool's online help. After updating a setting, use the browser reload button to run the environment checker again. Repeat this process until you have resolved all of the errors and warnings.

When using the Internet Explorer 7 browser, you might experience slow responsiveness if you open multiple tabs, work with large WLM service definitions, or use the Resource Monitoring task for long periods of time. If so, consider using another supported browser to avoid this problem.

Some users run Microsoft Windows Internet Explorer Version 8 with the Compatibility View feature enabled, which allows web sites to appear as they do when viewed with Internet Explorer Version 7. If so, the environment checker identifies the browser as "Internet Explorer V7 " for the environment option Browser Version and Name. This behavior is normal. For information about enabling Compatibility View in Internet Explorer, see Knowledge Base article 956197, which is available on the Microsoft Support web site: [http://support.microsoft.com/kb/956197](http://support.microsoft.com/kb/956197).

If you are using Microsoft Internet Explorer to work with WLM service definitions, ensure that automatic prompting for file downloads is enabled for the web link (a URL) to the active z/OSMF instance. See "Enabling automatic prompting for file downloads" on page 151.
Recommended settings for the Mozilla Firefox browser

Table 28 shows the recommended settings for the Mozilla Firefox browser.

Table 28. Recommended settings for Firefox

<table>
<thead>
<tr>
<th>Environment Option</th>
<th>Response</th>
</tr>
</thead>
</table>
| JavaScript         | To work with z/OSMF, your browser must have JavaScript enabled.  
To enable JavaScript, do the following:  
1. From the Tools menu, click Options > Content tab.  
2. Ensure that the JavaScript check box is selected.  
3. Click OK. |
| Cookies            | To work with z/OSMF, your browser must have cookies enabled—if not for all sites, then at least for the z/OSMF site at your installation.  
To enable cookies for use by any site, do the following:  
1. From the Tools menu, click Options > Privacy tab.  
2. Ensure that the Accept cookies from sites check box is selected.  
3. Click OK.  
To enable cookies for only the z/OSMF site, clear the Accept cookies from sites check box. Then, do the following:  
1. Click Exceptions.  
2. Enter the URL for the z/OSMF site at your installation.  
3. Click Allow > Close > OK. |
| Pop-up Windows     | For proper functioning with z/OSMF, your browser must be enabled for pop-up windows.  
To enable your browser for pop-up windows, do the following:  
1. From the Tools menu, click Options > Content tab.  
2. Clear the Block pop-up windows check box.  
3. Click OK.  
To enable pop-up windows for the z/OSMF site only, ensure that the Block pop-up windows check box is selected. Then, do the following:  
1. Click Exceptions.  
2. Enter the URL for the z/OSMF site at your installation.  
3. Click Allow > Close > OK. |
| Frames             | To work with z/OSMF, your browser must have frames enabled.  
To enable your browser for frames, do the following:  
1. In the browser input area, enter the following URL: about:config.  
2. If a warranty warning message appears, click the I’ll be careful, I promise! button to continue.  
3. In the Filter field, enter frames.  
4. Click browser.frames.enabled to set the Value field to true.  
5. Close the browser to save the changes. |
Table 28. Recommended settings for Firefox (continued)

<table>
<thead>
<tr>
<th>Environment Option</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screen Resolution</td>
<td>For optimal viewing with z/OSMF, your workstation requires a minimum screen resolution of 1024 by 768 pixels. To increase the screen resolution, do the following: 1. Right-click on the desktop and select Properties &gt; Settings tab. 2. Move the slider to select a screen resolution of at least 1024 by 768 pixels. 3. Click OK.</td>
</tr>
</tbody>
</table>

| Browser Content Dimensions | For optimal viewing with z/OSMF, your browser requires a usable content display area of at least 800 by 600 pixels. A number of factors can affect the size of your browser’s usable content display area, such as Windows desktop appearance settings and the inclusion of toolbars for browser plug-ins. To check the desktop appearance settings, do the following: 1. Right-click on the desktop and select Properties to open the Display Properties dialog box. 2. Click the Appearance tab. 3. Click Advanced. 4. From the Item list, select Active Title Bar and verify that it is no larger than necessary (the default is 25 pixels). Similarly, check the setting for Scrollbar (the default is 17 pixels). 5. Click OK > OK. To remove unnecessary toolbars, do the following: 1. From the View menu in Firefox, click Toolbars. 2. For any unnecessary toolbars, clear the associated check box. As an alternative, you can maximize the browser window, thus eliminating the toolbars, by pressing the F11 function key. To restore the window to its previous size, press F11 again. |

| Add-ons | For optimal performance with z/OSMF, disable the Firebug add-on in your browser settings. To disable the Firebug add-on, do the following: 1. From the Tools menu, click Add-ons > Extensions tab. 2. Select the Firebug add-on and click the Disable option. 3. Restart the browser to have the changes take effect. |
Table 28. Recommended settings for Firefox (continued)

<table>
<thead>
<tr>
<th>Environment Option</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plug-ins</td>
<td>Some plug-ins, such as JavaScript debuggers, can affect browser performance. For optimal performance with z/OSMF, include only required plug-ins with your browser. In the environment checker report, the Settings column shows the installed plug-ins for your browser. To verify this list, do the following: 1. In the browser input area, enter the following URL: about:plugins. 2. Compare the list of installed plug-ins to the list shown in the environment checker report to determine whether any add-ons should be disabled. To disable a plug-in, do the following: 1. From the Tools menu, click Add-ons &gt; Plugins tab. 2. Scroll down the list to locate the plug-in. 3. Select the plug-in and click the Disable option. 4. Restart the browser to have the changes take effect.</td>
</tr>
</tbody>
</table>

Recommended settings for the Windows Internet Explorer browser

Table 29 shows the recommended settings for the Microsoft Windows Internet Explorer browser. If you are using the Workload Management task, see also “Enabling automatic prompting for file downloads” on page 151.

Table 29. Recommended settings for Internet Explorer

<table>
<thead>
<tr>
<th>Environment Option</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>JavaScript</td>
<td>To work with z/OSMF, your browser must have JavaScript enabled. To enable JavaScript, do the following: 1. From the Tools menu, click Internet Options &gt; Security tab. 2. Click Custom Level. 3. Scroll down to Scripting, then Active Scripting. 4. Click Enable. 5. Click OK &gt; OK.</td>
</tr>
</tbody>
</table>
**Table 29. Recommended settings for Internet Explorer (continued)**

<table>
<thead>
<tr>
<th>Environment Option</th>
<th>Response</th>
</tr>
</thead>
</table>
| Cookies            | To work with z/OSMF, your browser must have cookies enabled—if not for all sites, then at least for the z/OSMF site at your installation.  
To enable cookies for use by any site, do the following:  
1. From the *Tools* menu, click **Internet Options > Privacy** tab.  
2. Click **Advanced**.  
3. Select the **Override automatic cookie handling** check box.  
4. Select **Accept** for *First-party Cookies* and *Third-party Cookies*.  
5. Click **OK > OK**.  
To enable cookies for only the z/OSMF site, clear the **Override automatic cookie handling** check box and select **Block** for *First-party Cookies* and *Third-party Cookies*. Then, do the following:  
1. From the *Tools* menu, click **Internet Options > Privacy** tab.  
2. Click **Sites**.  
3. Enter the URL for the z/OSMF site at your installation.  
4. Click **Allow**.  
5. Click **OK > OK**. |
| Pop-up Windows      | For proper functioning with z/OSMF, your browser must be enabled for pop-up windows.  
To enable your browser for pop-up windows, do the following:  
1. From the *Tools* menu, click **Internet Options > Privacy** tab.  
2. Clear the **Turn on Pop-up Blocker** check box.  
3. Click **OK**.  
To enable pop-up windows for the z/OSMF site only, ensure that the **Turn on Pop-up Blocker** check box is selected. Then, do the following:  
1. Select **Settings**.  
2. Enter the URL for the z/OSMF site at your installation.  
3. Click **Add**.  
4. Click **Close > OK**. |
| Frames              | To work with z/OSMF, your browser must have frames enabled.  
To enable your browser for frames, do the following:  
1. From the *Tools* menu, click **Internet Options > Security** tab.  
2. Click **Custom Level**.  
3. Scroll down to **Miscellaneous**, then *Launching programs and files in an IFRAME*.  
4. Click **Enable**.  
5. Click **OK**. |
### Table 29. Recommended settings for Internet Explorer (continued)

<table>
<thead>
<tr>
<th>Environment Option</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screen Resolution</td>
<td>For optimal viewing with z/OSMF, your workstation requires a minimum screen resolution of 1024 by 768 pixels. To increase the screen resolution, do the following: 1. Right-click on the desktop and select <strong>Properties &gt; Settings</strong> tab. 2. Move the slider to select a screen resolution of at least 1024 by 768 pixels. 3. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Browser Content Dimensions</td>
<td>For optimal viewing with z/OSMF, your browser requires a usable content display area of at least 800 by 600 pixels. A number of factors can affect the size of your browser's usable content display area, such as Windows desktop appearance settings and the inclusion of toolbars for browser plug-ins. To check the desktop appearance settings, do the following: 1. Right-click on the desktop and select <strong>Properties</strong> to open the <strong>Display Properties</strong> dialog box. 2. Click the <strong>Appearance</strong> tab. 3. Click <strong>Advanced</strong>. 4. From the <strong>Item</strong> list, select <strong>Active Title Bar</strong> and verify that it is no larger than necessary (the default is 25 pixels). Similarly, check the setting for <strong>Scrollbar</strong> (the default is 17 pixels). 5. Click <strong>OK &gt; OK</strong>. To remove unnecessary toolbars, do the following: 1. From the <strong>View</strong> menu, click <strong>Toolbars</strong>. 2. For any unnecessary toolbars, clear the associated check box. As an alternative, you can maximize the browser window, thus eliminating the toolbars, by pressing the F11 function key. To restore the window to its previous size, press F11 again.</td>
</tr>
<tr>
<td>Add-ons</td>
<td>For optimal performance with z/OSMF, it is recommended that you include only required add-ons with your browser. To disable an add-on, do the following: 1. From the <strong>Tools</strong> menu, click <strong>Manage Add-ons &gt; Enable or Disable Add-ons</strong>. 2. Scroll down the list to view the add-ons. 3. To disable an add-on, select it and click the <strong>Disable</strong> button. 4. Click <strong>OK</strong>. 5. Restart the browser to have the changes take effect.</td>
</tr>
</tbody>
</table>
Table 29. Recommended settings for Internet Explorer (continued)

<table>
<thead>
<tr>
<th>Environment Option</th>
<th>Response</th>
</tr>
</thead>
</table>
| Plug-ins           | Some plug-ins, such as JavaScript debuggers, can affect browser performance. For optimal performance with z/OSMF, it is recommended that you include only required plug-ins with your browser. In the environment checker report, the **Settings** column shows the installed plug-ins for your browser. To verify this list, do the following:  
1. From the **Tools** menu, click **Manage Add-ons > Enable or Disable Add-ons**.  
2. Scroll down the list to view the add-ons.  
3. To disable an add-on, select it and click the **Disable** button.  
4. Click **OK**.  
5. Restart the browser to have the changes take effect. |

Enabling automatic prompting for file downloads
If you are using Microsoft Internet Explorer to work with WLM service definitions, ensure that automatic prompting for file downloads is enabled for the web link (a URL) to the active z/OSMF instance. If the feature is disabled, when you attempt to display the **File Download** dialog box, the browser window refreshes and all of your selections and unsaved changes are discarded. To enable automatic prompting for file downloads, use the following procedure.

**Procedure**
1. From the **Tools** menu, click **Internet Options > Security** tab.  
2. Select **Trusted sites**.  
3. Click **Sites**.  
4. If the URL to the active z/OSMF instance is listed in the Add this web site to the zone field, click **Add**. Otherwise, enter the URL, and then click **Add**.  
5. Click **Close**.  
6. Click **Custom level**.  
7. In the Settings field, scroll to the Downloads section, and ensure that Automatic prompting for file downloads is enabled.  
8. Click **OK**.  
9. Click **OK**.
Finding information about z/OSMF

z/OSMF includes an About page to display the product version details that can be useful to IBM Support during the diagnosis of a problem.

About this task

To access the About page for z/OSMF, do the following:

Procedure

1. Select the Welcome task in the navigation area. The Welcome page opens.
2. Click the About link located in the upper right-hand corner of the Welcome page. Details about the product build level, and the configured plug-ins and their versions, are displayed in a new browser window. If no plug-ins are configured, this area is empty.

Working with z/OSMF runtime log files

During normal operations, z/OSMF collects its runtime data (log messages and trace messages) in log files. z/OSMF runtime data is created on the server (server side) or sent to the server by the client (client side). Both types of messages are written to the z/OSMF runtime log files.

z/OSMF creates the log files in the product logs directory, which is, by default, /var/zosmf/data/logs. z/OSMF names the log files IZUGn.log, where n is a numeral from 0 to 9.

z/OSMF creates log files in a “cascading” manner. The most current log file is always named IZUG0.log. When this log file reaches its predefined limit, z/OSMF saves it as IZUG1.log and begins writing to a new IZUG0.log file. When the IZUG0.log file is again full, z/OSMF saves it as IZUG1.log after renaming the existing IZUG1.log file to IZUG2.log. z/OSMF continues this process, saving each log file under the next available name, up to a maximum of ten log files. Thereafter, z/OSMF discards the oldest log file (IZUG9.log) whenever a new log file is to be created.

The z/OSMF runtime log files are written in English only, and are tagged as ASCII, using the ISO8859-1 code page. You can view the log files in ASCII format through ISPF option 3.17, using the VA action (View an ASCII file). Other viewing options, such as OBROWSE, or tools such as vi, emacs, or grep, might require that you first convert the files to EBCDIC. To have ASCII files converted to EBCDIC automatically prior to browsing, set the z/OS UNIX System Services environment variable _BPXK_AUTOCVT to “ON”.

To work with the logs, you require the z/OSMF administrator user ID. Changing the level of logging and activating trace are performed through the same operation. For the steps, see “Enabling tracing and logging for z/OSMF” on page 153.

For examples of z/OSMF runtime log data, and a description of the log file format, see Appendix G, “Examples of working with z/OSMF runtime logs,” on page 267.

Managing log lock files

When z/OSMF initializes, the log file handler creates a file named IZUG0.log.lck. This file represents a “lock” on the log data. Usually, lock files are cleaned up automatically as part of application shutdown. If WebSphere Application Server
ends abnormally, however, the lock files might remain. If so, the log file handler append numbers to the normal lock file name to find a file that is free.

If the server ends abnormally, inspect the log directory and delete the lock files. If additional locks and log files were created, you can sort the files in the directory by timestamp to determine which files are the most recent. Back up these files if you want to preserve them, then clear the logs directory to conserve space.

If client data cannot be written to the server

If a communication problem prevents the client’s critical error log data from being written to the z/OSMF logs directory, the unlogged client data is displayed to the end user in a separate browser window. This failover action allows for the client data to be retained until the communication with the z/OS system can be restored. In some situations, IBM Support might request this data for diagnostic purposes. If the browser window is closed, the client data is not retained.

If the product logs directory cannot be accessed

If a problem occurs with the product logs directory, for example, the directory is not writable or z/OSMF encounters an error on initialization, z/OSMF writes its log data in the WebSphere servant log instead.

Other log files in z/OSMF

Do not confuse the z/OSMF runtime log file with the script log files that are created during the z/OSMF configuration process. In contrast to runtime data, configuration log data is written to a file in the z/OSMF configuration file system, which is, by default /etc/zosmf. If a problem occurs with the configuration log file, the log data is written instead to the directory specified by $TMPDIR, if this environment variable is set. Otherwise, the configuration log data is written to the /tmp directory.

Enabling tracing and logging for z/OSMF

For diagnostic purposes, you might be asked by IBM Support to enable tracing and logging for z/OSMF. You can configure the WebSphere server to start in a trace-enabled state, or you can enable tracing and logging dynamically for the running server. The trace output is written to files in the z/OSMF logs directory.

Activating tracing and changing the level of logging are performed through the same operation.

This section contains the following topics:
- “Determining the current level of tracing and logging” on page 154
- “Enabling tracing and logging at server startup” on page 155
- “Enabling tracing and logging on a running server” on page 155.

Understand that tracing carries a performance cost. Do not activate tracing for z/OSMF unless directed to do so by IBM Support.

Determining the current level of tracing and logging

You might be asked by IBM Support to determine the current level of tracing and logging for your z/OSMF configuration. To do so, you use the command MODIFY
DISPLAY with the options TRACE, JAVA. To run this command, your user ID must be permitted to enter operator commands.

Enter the command from the operator console. The command output is displayed in the operator console and in the z/OS system log.

The command has the following format:

```
f server-name,display,trace,java
```

where server-name identifies the WebSphere server for your z/OSMF configuration, as follows:

- If your installation starts the WebSphere server as a started task, specify the job name that was used to start the server. Usually, the job name is the same as the server short name, which is specified on the variable zServerShortName in the WebSphere response file, which your installation created earlier when installing IBM WebSphere Application Server OEM Edition for z/OS. By default, the response file is /etc/zWebSphereOEM/V7R0/conf/CONFIG1/CONFIG1.responseFile, and zServerShortName is BBNS001.

- If your installation starts the WebSphere server without a specified job name, server-name is the name of the member in your procedure library that is used to start the WebSphere server controller. This value is the same as the value for variable zControlProcName in the WebSphere response file. By default, zControlProcName is BBN7ACR.

For more information about starting and stopping the WebSphere server, see IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide GA32-0631.

For example, the following command displays the trace settings for the BBNS001 server: `f bbns001,display,trace,java`

Figure 33 shows an example of the command output.

```
F BBNS001,DISPLAY,TRACE,JAVA
BB000196I TRACE INFORMATION FOR SERVER BBNC001/BBNS001
BB000501: CTL(STC18988):**=warning:com.ibm.ws.management.applica
BB008188I END OF OUTPUT FOR COMMAND DISPLAY,TRACE,JAVA
```

Figure 33. Sample results from the MODIFY DISPLAY, TRACE operator command

IBM Support uses the command output to determine the current level of tracing and logging for your z/OSMF configuration.

### Enabling tracing and logging at server startup

The WebSphere diagnostic trace configuration settings are used to configure tracing and logging for z/OSMF. These settings, which are read when the WebSphere server is started, determine the initial trace state for the server.

If there is a problem with starting the server, you might be asked by IBM Support to configure the server to start in a trace-enabled state. If so, you can use izuupdate.sh script to perform this step. The script is described in Appendix E, “Modifying advanced settings for the z/OSMF configuration,” on page 263.
Enabling tracing and logging on a running server

You might be asked by IBM Support to enable tracing and logging for z/OSMF dynamically. If so, use the command MODIFY with the TRACEJAVA option to set the appropriate tracing specification. To run this command, your user ID must be permitted to enter operator commands.

The command has the following format:

\[ f \text{ server-name,tracejava='trace_specification'} \]

where:

- **server-name**
  - Is the WebSphere server for your z/OSMF configuration. For the value to use, see “Determining the current level of tracing and logging” on page 153.

- **trace_specification**
  - Is the level of tracing to be used. This value is provided by IBM Support.

Enter the command from the operator console. The command output is displayed in the operator console and in the z/OS system log.

Your changes take effect immediately and remain in effect while the WebSphere server is running. Your changes are discarded when the server is restarted, and the previous settings are used. To have your changes saved across server restarts, you must use the **izuupdate.sh** script, as described in Appendix F, “Modifying advanced settings for the z/OSMF configuration,” on page 263.

---

Common problems and scenarios

z/OSMF is based on a stack of components, starting with the application running in the user’s workstation web browser and extending to the lower level z/OS functions and components that deliver much of the underlying function. This section discusses troubleshooting topics, procedures and tools for recovering from a set of known issues.

Troubleshooting topics are included for the following problems and scenarios:

- “Problems during configuration” on page 156
- “Problems identified by the Incident Log installation verification program (IVP)” on page 161
- “Problems when accessing the user interface” on page 168
- “Problems when using Configuration Assistant” on page 174
- “Problems when using the Incident Log task” on page 176
- “Problems when using the ISPF task” on page 175
- “Problems when attempting to send data” on page 178

---

Problems during configuration

This topic provides troubleshooting tips for resolving problems related to the configuration and setup of z/OSMF.

Troubleshooting topics are included for the following problems and scenarios:

- “izusetup.sh script cannot locate CEA parmlib member” on page 156
- “izusetup.sh script cannot activate CEA parmlib member” on page 156
izusetup.sh script fails or CIM server abends” on page 157
“izusetup.sh script fails when issuing an operator command, such as DUMP” on page 158
“izusetup.sh script fails with an authorization failure for the z/OSMF administrator” on page 158
“izusetup.sh script fails with incomplete details in the log file” on page 159
“izusetup.sh script fails because cimivp times out” on page 160
“A z/OSMF script fails because no z/OS UNIX processes are available” on page 160.

A problem in the configuration of z/OSMF might be indicated by error messages from the common event adapter (CEA) component of z/OS. For a description of configuration-related CEA reason codes, which might be useful in diagnosing problems in your z/OSMF setup, see Appendix H, “Common event adapter (CEA) reason codes,” on page 269.

izusetup.sh script cannot locate CEA parmlib member

**Symptom:** While performing “Step 4: Prime the z/OSMF data file system” on page 73, the script `izusetup.sh -prime` fails with the following message:

```
IZUG207E: File <source parmlib>(CEAPRM00) does not exist.
```

**Possible Causes:** The script searches for the IBM-supplied member, CEAPRM00 in the source data set (`source parmlib`) that you specified earlier as input (see “Step 1: Create the initial configuration” on page 65). However, the source data set is:

1. Missing or is not cataloged
2. Missing the CEAPRM00 member
3. Protected through a RACF data set profile (for example, SYS1.*), but the `z/OSMF administrator` identity is not permitted to the profile.

By default, the source data set is SYS1.PARMLIB.

**Corrective Actions:** Ensure that the parmlib data set:

1. Exists and is cataloged
2. Contains the IBM-supplied member CEAPRM00
3. If protected through a RACF data set profile, the `z/OSMF administrator` identity is permitted to the data set profile. To grant this permission, use the following command, where `ZOSMFAD` is the user ID to be authorized to the data set profile SYS1.*:

```
PERMIT SYS1.* ID(ZOSMFAD) ACCESS(READ)
```

izusetup.sh script cannot activate CEA parmlib member

**Symptom:** When performing “Step 4: Prime the z/OSMF data file system” on page 73, the script `izusetup.sh -prime` fails. The z/OSMF log contains messages like the following:
**Possible Cause:** z/OSMF cannot activate the newly created CEAPRMxx parmlib member (by default, CEAPRM01). This error can occur if the configuration script copied the CEAPRMxx member to a target parmlib data set that is not in your installation's parmlib concatenation. You specified the target parmlib data set earlier when you ran the script described in “Step 1: Create the initial configuration” on page 65. By default, this is data set SYS1.PARMLIB.

**Corrective Action:** To resolve the problem, copy the CEAPRMxx member to your parmlib concatenation. Then, enter the following command to activate the new CEAPRMxx member, where xx represents the member suffix:

```
MODIFY CEA,CEA=xx
```

To verify that the new CEAPRMxx parmlib member is in effect, enter the MODIFY command, as follows:

```
MODIFY CEA,DISPLAY,PARMS
```

Ensure that the new member:
- Defines a high level qualifier for CEA, such as HLQ(CEA), and sets the SNAPSHOTS parameter to Y to allow CEA to create diagnostic snapshots of the system logs
- Sets the IBM branch and country code values for your installation
- Defines the storage value for parmlib (an SMS class or a string of volume names).

It is recommended that you edit your active IEASYSxx parmlib member to identify the CEAPRMxx parmlib member to use for the next IPL of the system. Specify the CEAPRMxx member suffix on the CEA=xx statement of IEASYSxx.

For more information about the CEAPRMxx parmlib member, see z/OS MVS Initialization and Tuning Reference SA22-7592.

**izusetup.sh script fails or CIM server abends**

**Symptoms:** While performing “Step 5: Complete the setup” on page 75, the script izusetup.sh -finish fails. Or, the CIM server abends when attempting to use CEA.

**Possible Cause:** LIBPATH is not set up correctly

**Corrective Action:** Add the path in which the CEA DLLs are installed to LIBPATH. Usually, this is /usr/lib.
izusetup.sh script fails when issuing an operator command, such as DUMP

Symptom: When performing ["Step 5: Complete the setup" on page 75] the script izusetup.sh -finish fails. SYSLOG contains messages related to authorization errors.

Possible Cause: The z/OSMF administrator lacks OPERCMDS access.

Corrective Action: If your installation protects MVS commands with the RACF class OPERCMDS, you must grant the proper authority to the z/OSMF administrator user ID.

- To grant DUMP command access to the z/OSMF administrator, enter the PERMIT command as follows. This authorization is required for the Incident Log verify step to complete.

  PERMIT MVS.DUMP CLASS(OPERCMDS) ID(ZOSMFAD) ACCESS(CONTROL)

- To allow the z/OSMF administrator to use all operator commands, enter the PERMIT command, as follows:

  PERMIT MVS.** CLASS(OPERCMDS) ID(ZOSMFAD) ACCESS(CONTROL)

- To grant the z/OSMF administrator access to particular operator commands, enter the PERMIT command with one or more of the profiles shown in Table 30, as appropriate for your installation.

<table>
<thead>
<tr>
<th>Resource profile</th>
<th>Access required</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVS.DISPLAY.LOGGER</td>
<td>READ</td>
</tr>
<tr>
<td>MVS.SETLOGR.LOGR</td>
<td>UPDATE</td>
</tr>
<tr>
<td>MVS.DISPLAY.SYMBOLS</td>
<td>ALTER</td>
</tr>
<tr>
<td>MVS.DISPLAY.XCF</td>
<td>READ</td>
</tr>
<tr>
<td>MVS.DUMP</td>
<td>CONTROL</td>
</tr>
</tbody>
</table>

izusetup.sh script fails with an authorization failure for the z/OSMF administrator

Symptom: While performing ["Step 5: Complete the setup" on page 75] the script izusetup.sh -finish fails with an authorization failure message for the z/OSMF administrator identity.

Possible Cause: Your installation uses the RACF PROTECT-ALL option to protect its data sets, but you did not define the CEA.* RACF profile.

Corrective Action: If your installation uses PROTECT-ALL, you must define a CEA.* data set profile to RACF and permit CEA and the z/OSMF administrator identity. For example:

ADDSD 'CEA.*,*' UACC(NONE)
PERMIT 'CEA.*,*' ID(CEA) ACCESS(ALTER)
PERMIT 'CEA.*,*' ID(ZOSMFAD) ACCESS(ALTER)
**izusetup.sh script fails with incomplete details in the log file**

**Symptom:** While performing the script `izusetup.sh -finish` on page 75, the script fails with the following message:

```
IZUG305E The script <script-name> failed with reason code nnn;
see log file <log-file-path-and-name>.
```

In this message, the reason code `nnn` indicates that an internal script, `wsadmin.sh`, encountered an error while processing. On examining the indicated log file, `izusetup_finish<timestamp>.log`, you find little additional information about the error.

**Corrective Action:** For more information about this error, check the contents of log file `wsadmin.traceout`, which is created by the internal script `wsadmin.sh`. This log file is located in the WebSphere configuration file system, the mount point of which is indicated by the `<IZU_APPSERVER_ROOT>` variable for your z/OSMF configuration, as follows:

```
<IZU_APPSERVER_ROOT>/AppServer/profiles/default/logs/wsadmin.traceout
```

Depending on the source of the error, more information might be available in the reason code documentation for z/OS UNIX System Services or Java.

**izusetup.sh script fails with "garbage characters" in the display or log file**

**Symptom:** While performing the script `izusetup.sh -finish` on page 75, the script fails with message IZUG295E indicating that the verification process has failed. This message is accompanied by unrecognized or "garbage" characters written to the z/OSMF log, the user's screen, or both. Figure 34 shows an example:

```
AN AE-EE/EEA---------8??>AAEEN-Æ-Æ-ÆE----ÆE-----ÆAEEE---ÆS;Æ-Æ-Æ
AE=ÆEE-----{[1]Æ-ÆE-
ÆE----Æ-----ÆE-----ÆAEEE--ÆE-----ÆEAE--ÆE-ÆAE---ÆE---ÆEAE--ÆE---ÆE
Æ-ÆE---ÆE-AE-----ÆEAE--ÆE---ÆEAE--ÆE---ÆEAE--ÆE---ÆEAE--ÆE---ÆE
Æ-ÆE---ÆE-AE-----ÆEAE--ÆE---ÆEAE--ÆE---ÆEAE--ÆE---ÆEAE--ÆE---ÆE

---IZUG295E: Verification process /usr/lpp/cim/bin/cimivp has failed.
IZUG211E: Script "./izusetup.sh" encountered errors; exiting script.
```

**Corrective Action:** Verify that the z/OSMF administrator profile is properly set up for the z/OS UNIX shell environment. By default, the file `profile.add`, which is shipped with the CIM server, provides the environment variables that you need to define for the administrator; see `/usr/lpp/cim/install/ profile.add`. If you are not using the defaults, you should modify the appropriate settings. Copy the contents of the `profile.add` file to the `.profile` file in the home directory of the z/OSMF administrator user ID. The `.profile` file should be owned by the z/OSMF administrator, and have read-write-execute access for the owner.

Then, run the `izusetup.sh -finish` script again.
izusetup.sh script fails because cimivp times out

**Symptom:** While performing [“Step 5: Complete the setup” on page 75](#) the script `izusetup.sh -finish` fails with a message indicating that the cimivp program has timed out.

**Corrective Action:** As part of its processing, the script `izusetup.sh -finish` runs the CIM installation verification program, cimivp. If the execution of cimivp times out, the problem might be a slow IP hostname resolution or a large number of managed resources to be queried, such as logical disks. The default timeout for cimivp is two minutes. To override this default, you can export the following variable in your z/OS UNIX shell environment:

```
CIM_IVP_TIMEOUT=nnn
```

where `nnn` is the number of seconds that cimivp is to wait for a response from the CIM server before it fails with a timeout. For example, to set the cimivp timeout to five minutes, enter the following export command:

```
export CIM_IVP_TIMEOUT="300"
```

Then, run the `izusetup.sh -finish` script again.

For more information about the cimivp program, see [z/OS Common Information Model User’s Guide](#).

A z/OSMF script fails because no z/OS UNIX processes are available

**Symptom:** A script fails with a message indicating that no z/OS UNIX processes are available for the user ID that was used to run the script.

**Possible Cause:** The user ID is exceeding the MAXPROCUSER setting for your system. MAXPROCUSER specifies the maximum number of z/OS UNIX processes that a single user can have active concurrently. Typically, an installation sets a system-wide limit through the MAXPROCUSER setting in the BPXPRMxx member of parmlib, and then sets higher limits for individual users and processes through PROCUSERMAX, a value in the OMVS segment. Though z/OSMF by itself does not add significantly to the number of z/OS UNIX processes for the user, the MAXPROCUSER setting can be reached when the user is also running a number of other processes on the system besides z/OSMF.

**Corrective Action:** Use the RACF ADDUSER or ALTUSER command (or an equivalent command for your security product) to specify a PROCUSERMAX value for the user ID that is higher than the MAXPROCUSER setting. Try adding 20 to the value that is currently specified through the MAXPROCUSER setting.

Suppose, for example, that your installation has specified a MAXPROCUSER value of 80 in the BPXPRMxx member. Here, you would set the PROCUSERMAX value for this user ID to 100, to allow a greater number of processes for the user ID. The following example assumes that you are running the script from the z/OSMF administrator user ID:

```
ALTUSER ZOSMFAD OMVS(PROCUSERMAX(100))
```
If the problem persists, repeat this process by increasing the PROCUSERMAX value by an additional 20, taking care not to exceed any limits that are appropriate for your installation; check with the security administrator.

Problems identified by the Incident Log installation verification program (IVP)

This topic provides troubleshooting tips for system setup problems identified by the Incident Log task installation verification program (IVP). Included are procedures and methods for performing problem determination and for troubleshooting the status of the different system components.

Using the installation verification program

The Incident Log installation verification program (IVP) checks the z/OS system setup to determine actions that might have been missed during z/OSMF configuration.

About the installation verification program

The IVP checks for the following conditions, all of which are required for successful operation of the Incident Log task:

- CEA component is available
- System REXX component is available
- User is authorized for the Incident Log resources associated with CEA and CIM
- Sysplex dump directory is available and accessible
- AMATERSE program is enabled to run
- System REXX execs are available and operational
- System Logger is available
- Operations log (OPERLOG) and logrec snapshots are accessible
- Dump analysis and elimination (DAE) is active and its symptom data set is available.

Appendix B, “z/OS system setup for the Incident Log task,” on page 231 contains sections on how to perform each of these z/OS setup tasks manually.

Running the installation verification program

To run the Incident Log IVP, your user ID must be permitted to enter operator commands. To add this authority, enter the RACF PERMIT command, as follows:

```
PERMIT MVS.** CLASS(OPERCMDS) ID(userid) ACCESS(CONTROL)
```

You can invoke the IVP program as a batch job using the following JCL:
Reviewing the results of the izuincidentlogverify.report file

On completion, the script creates a report file called izuincidentlogverify.report, which is stored in the following location:

<IZU_LOGFILE_DIR>/izuincidentlogverify.report

where <IZU_LOGFILE_DIR> is the log file directory for your installation. By default, this is /var/zosmf/configuration/logs/.

To verify the configuration of the Incident Log task, z/OSMF creates a test SVC dump on the system and performs a series of tests on the dump. For each test, the izuincidentlogverify.report file shows either SUCCESS or an error message. Each error message corresponds to a possible cause and one or more corrective actions for the problems described by this report.

For your reference, the format of the IVP report is shown in Appendix J, “Format of the installation verification program report,” on page 289.

For information about the errors and corrective actions you can take, see Table 31, “Responding to system setup errors indicated in the izuincidentlogverify.report file.”

Table 31. Responding to system setup errors indicated in the izuincidentlogverify.report file

<table>
<thead>
<tr>
<th>Problem indicated by the IVP</th>
<th>Corrective action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEA address space is not running.</td>
<td>Start the CEA address space; see “Ensuring that CEA is active” on page 245.</td>
</tr>
<tr>
<td>System REXX address space is not running.</td>
<td>Start the System REXX address space; see “Ensuring that System REXX is set up and active” on page 247.</td>
</tr>
<tr>
<td>User is not authorized.</td>
<td>Authorize the user to the indicated security class profile-class; see “User is not authorized” on page 164.</td>
</tr>
<tr>
<td>Unable to locate an incident in the sysplex dump directory.</td>
<td>Check the sysplex dump directory setup; see “Unable to locate an incident in the sysplex dump directory” on page 164.</td>
</tr>
<tr>
<td>Unable to open the sysplex dump directory.</td>
<td>Check the sysplex dump directory setup; see “Unable to open the sysplex dump directory” on page 165.</td>
</tr>
<tr>
<td>SYS1.MIGLIB is not APF-authorized.</td>
<td>APF-authorize the SYS1.MIGLIB data set; see “Authorizing the SYS1.MIGLIB data set” on page 249.</td>
</tr>
</tbody>
</table>
### Resolving problems identified by the installation verification program

This topic provides corrective actions for system setup problems identified by the Incident Log installation verification program (IVP).

Troubleshooting topics are included for the following problems and scenarios:
- “CEA address space is not running” on page 164
- “System REXX address space is not running” on page 164
- “User is not authorized” on page 164
- “Unable to locate an incident in the sysplex dump directory” on page 164
- “Unable to open the sysplex dump directory” on page 165
- “SYS1.MIGLIB is not APF-authorized” on page 165
- “Another resource is using the sysplex dump directory” on page 165
- “Unable to generate prepared data set” on page 166
- “User is not SAF authorized” on page 166
- “System logger not available” on page 166
- “Unable to find the active DAE data set name” on page 166

### Table 31. Responding to system setup errors indicated in the izuincidentlogverify.report file (continued)

<table>
<thead>
<tr>
<th>Problem indicated by the IVP</th>
<th>Corrective action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Another resource is using the sysplex dump directory.</td>
<td>Check the sysplex dump directory usage; see “Another resource is using the sysplex dump directory” on page 165.</td>
</tr>
<tr>
<td>Unable to generate the prepared data set.</td>
<td>Verify that the System REXX exec library is accessible, the SYSREXX address space is active, and that the compiled REXX exec CEACDMPP exists and is accessible to System REXX. See “Ensuring that System REXX is set up and active” on page 247.</td>
</tr>
<tr>
<td>User is not SAF authorized.</td>
<td>Grant the user the system authority to view the log files; see “User is not SAF authorized” on page 166.</td>
</tr>
<tr>
<td>System logger is not available.</td>
<td>Check the system logger setup; see “System logger not available” on page 166.</td>
</tr>
<tr>
<td>Unable to find the active DAE data set name.</td>
<td>Check the dump analysis and elimination (DAE) setup; see “Configuring dump analysis and elimination” on page 242.</td>
</tr>
<tr>
<td>System REXX environment cannot process the request.</td>
<td>Ensure that runtime support for compiled REXX is set up properly; see “System REXX cannot process the request” on page 166.</td>
</tr>
<tr>
<td>Unable to allocate the prepared data set to be tersed.</td>
<td>The function that prepares an incident’s materials to be sent through FTP was not able to allocate the data set to be tersed; see “Unable to allocate the prepared data set to be tersed” on page 167.</td>
</tr>
<tr>
<td>Unable to find the OPERLOG snapshot.</td>
<td>Check the system logger setup for the operations log (OPERLOG); see “Unable to find the OPERLOG snapshot” on page 167.</td>
</tr>
<tr>
<td>Sysplex dump directory has no space allocated.</td>
<td>Allow more space for incidents; see “Sysplex dump directory has no space allocated” on page 167.</td>
</tr>
<tr>
<td>Unable to allocate new data set.</td>
<td>When preparing incident materials to be sent through FTP, z/OSMF could not allocate a new data set to contain the tersed diagnostic snapshot. See “Unable to allocate new data set” on page 167.</td>
</tr>
<tr>
<td>No diagnostic data available.</td>
<td>Specify a larger time interval for error log snapshots; see “No diagnostic data available” on page 167.</td>
</tr>
<tr>
<td>Internal error encountered. CEA return code: return-code CEA reason code: reason-code</td>
<td>Look for system messages indicating why the failure occurred in the CIM trace associated with the failed return code; see “Internal error encountered. CEA return code: CEA reason code:” on page 168.</td>
</tr>
</tbody>
</table>
• “System REXX cannot process the request” on page 166
• “Unable to allocate the prepared data set to be tersed” on page 167
• “Unable to find the OPERLOG snapshot” on page 167
• “Sysplex dump directory has no space allocated” on page 167
• “Unable to allocate new data set” on page 167
• “No diagnostic data available” on page 167
• “Internal error encountered. CEA return code: CEA reason code: ” on page 168

CEA address space is not running

Possible Cause: The common event adapter (CEA) address space is not active.

Corrective Action: Start the CEA address space. For information, see “Ensuring that CEA is active” on page 245.

System REXX address space is not running

Possible Cause: The System REXX address space (AXR) is not active.

Corrective Action: Start the System REXX address space. For information, see “Ensuring that System REXX is set up and active” on page 247.

User is not authorized

Possible Cause: Most likely, a problem occurred when running the script to define a z/OSMF user.

Corrective Action: Authorize the user to the indicated security class profile-class. Check the izuauthuser.sh script, which is used to authorize the user; see “Creating the commands to authorize a user ID” on page 120. Ensure that the user has the appropriate permission to the CEA classes required for using the Incident Log task; see Table 47 on page 229.

Unable to locate an incident in the sysplex dump directory

Possible Cause: IPCS could not locate the sysplex dump directory data set. The dump directory is a shared VSAM data set with a default name of SYS1.DDIR. The installation can rename the data set and communicate that name through the BLSCUSER parmlib member.

Corrective Action: Check the sysplex dump directory setup:
1. Try locating the sysplex dump directory through ISPF 3.4
2. Verify that the name of the sysplex dump directory is the same as specified in the BLSCUSER member
3. Try rerunning BLSCDDIR to create the SYS1.DDIR data set.
4. Run a job to check the contents of the sysplex dump directory.

Figure 36 on page 165 shows an example of a job that you can use to create an IPCS report of the contents of the sysplex dump directory.
Unable to open the sysplex dump directory

Possible Causes include the following:

- Data set not found. The volume is offline or otherwise unavailable.
- Abend occurred during processing. The data set has I/O errors.

Corrective Action: Check the sysplex dump directory setup:

1. Verify that the data set is available. It might be allocated by DUMPSRV.
2. An IPCS user has allocated the sysplex dump directory.
3. The z/OSMF user was not authorized to access the sysplex dump directory.
4. If you renamed the sysplex dump directory to be a name other than SYS1.DDIR, update BLSCUSER with the new name, as described in "Establishing a larger sysplex dump directory" on page 244.
5. Check SYSLOG and OPERLOG for messages about the sysplex dump directory data set or volume.

For more information, see “Creating the sysplex dump directory” on page 243.

SYS1.MIGLIB is not APF-authorized

Possible Cause: The SYS1.MIGLIB data set, which contains the AMATERSE program, is not APF-authorized.

Corrective Action: APF-authorize the SYS1.MIGLIB data set. For information, see “Authorizing the SYS1.MIGLIB data set” on page 249.

Another resource is using the sysplex dump directory

Possible Cause: Another program is accessing the sysplex dump directory (by default SYS1.DDIR) exclusively and must free it. Programs that obtain exclusive (ENQ) access to the data set include DUMPSRV post-dump processing and common event adapter (CEA) when using IPCS service routines.

Corrective Actions: Check the sysplex dump directory usage:
1. Enter the command D GRS and check for contention on the sysplex dump directory data set.
2. If an IPCS user is holding the ENQ exclusively, consider cancelling that user's TSO session.
3. If CEA is holding the ENQ exclusively, enter the following command to end the CEA usage of the directory data set: MODIFY CEA, DROP IPCS
4. Try the request again later.

For more information, see "Creating the sysplex dump directory" on page 243.

Unable to generate prepared data set

Possible Cause: There was a SYSREXX processing failure when preparing diagnostic data to send through FTP. Or, the prepare request failed because the logrec data set is empty (CEA reason code 378).

Corrective Action: Verify that the System REXX exec library is accessible and the SYSREXX address space is active. Verify that the compiled REXX exec CEACDMPP exists and is accessible to System REXX. See "Ensuring that System REXX is set up and active" on page 247.

User is not SAF authorized

Possible Cause: The user is not authorized to view information about the OPERLOG snapshot. The name of the data set (snapshot) appears in the buffer returned with the message.

Corrective Action: The security administrator must authorize the user of the service to the high level qualifier of this data set, which is specified in the CEAPRMxx parmlib member.

System logger not available

Possible Cause: The CEA component cannot access the OPERLOG or logrec snapshot log stream when preparing incident data to be sent.

Corrective Action: Enter the command D LOGGER and verify that system logger is active. For information about system logger and the log streams, see:
- "Defining a couple data set for system logger" on page 233
- "Enabling the operations log (OPERLOG)" on page 235
- "Defining and activating the LOGREC log stream" on page 237.

Unable to find the active DAE data set name

Possible Cause: Dump analysis and elimination (DAE) is not active.

Corrective Action: Check the DAE setup. For information, see "Configuring dump analysis and elimination" on page 242.

System REXX cannot process the request

Possible Cause: The System REXX environment cannot process an exec. This problem usually indicates that the runtime support for compiled REXX has not been set up.
Corrective Action: The REXX library or the REXX Alternate library data set must be added to the LINKLIST concatenation or LPA. For more information, see IBM Compiler and Library for REXX on zSeries: User’s Guide and Reference, SH19-8160.

Unable to allocate the prepared data set to be tersed

Possible Cause: When preparing the dump or a log snapshot data set to be sent through FTP, the resulting data set is allocated and processed by the AMATERSE program. The dynamic allocation failed.

Corrective Action: Check message CEZ0500E for the dynamic allocation messages. For more information about these situations, see z/OS MVS System Messages.

Unable to find the OPERLOG snapshot

Possible Cause: The OPERLOG snapshot was not created. When accessing the OPERLOG snapshots, the system logger service IXGCONN received a bad return or reason code, indicating that the OPERLOG snapshot does not exist. It is possible that system logger is not active.

Corrective Action: Check the system logger setup:
1. Verify that the user has authorization to the OPERLOG DASD log stream.
2. Enter the command DISPLAY LOGGER,LOGSTREAM and verify the name of the OPERLOG snapshots (defined when configuring the DASD log streams).

For more information, see “Enabling the operations log (OPERLOG)” on page 235.

Sysplex dump directory has no space allocated

Possible Cause: The sysplex dump directory (SYS1/DDIR) has no space available to record new SVC dumps.

Corrective Action: Increase the size of the sysplex dump directory by doing one or both of the following:
1. Delete unneeded incidents from z/OSMF
2. Create a larger sysplex dump directory and copying the contents of the older data to the new directory data set. For more information, see “Establishing a larger sysplex dump directory” on page 244.

Unable to allocate new data set

Possible Cause: When preparing incident materials to be sent through FTP, z/OSMF could not allocate a new data set to contain the tersed diagnostic snapshot.

Corrective Action: Look for system messages indicating why the failure occurred in the CIM trace associated with the failed return code. For assistance, contact IBM Support.

No diagnostic data available

Possible Cause: The error log did not accumulate any data within the time interval specified in the CEAPRxx member.
Corrective Action: To specify a larger time interval for error log snapshots, modify the CEAPRMxx member statements as shown in Figure 37.

Note:
- The maximum value for a logrec summary is four hours.
- As part of its processing, the IVP creates a test SVC dump on the system. The test dump is not an ABEND type of incident, and therefore might not post any data in the error log. If this is the only problem reported by the IVP, you can ignore this problem.

```
DUMPCAPTURETIME
{
  SLIP(OPERLOG(01:00:00) LOGREC(01:00:00)
    LOGRECSUMMARY(04:00:00))
  DUMP(OPERLOG(01:00:00) LOGREC(01:00:00)
    LOGRECSUMMARY(04:00:00))
  ABEND(OPERLOG(01:00:00) LOGREC(01:00:00)
    LOGRECSUMMARY(04:00:00))
}
```

Figure 37. Specifying a larger time interval for error log snapshots

**Internal error encountered. CEA return code: CEA reason code:**

Possible Cause: An internal error occurred.

Corrective Action: Look for system messages indicating why the failure occurred in the CIM trace associated with the failed return code. See "CEA reason codes related to the Incident Log task" on page 270. For assistance, contact IBM Support.

**Problems when accessing the user interface**

This topic provides troubleshooting tips for resolving problems related to the user interface of z/OSMF.

Troubleshooting topics are included for the following problems and scenarios:
- "Browser cannot connect to z/OSMF"
- "Missing initialization message or JSP processing error when attempting to use z/OSMF from browser" on page 169
- "Certificate error in Mozilla Firefox Version 3" on page 170
- "Cannot log into z/OSMF" on page 173
- "Message or help information is not available" on page 173
- "A script takes too long to run or is not responding" on page 174

**Browser cannot connect to z/OSMF**

When logging into z/OSMF for the first time, your browser either does not connect, or waits indefinitely. Verify that the browser has network connectivity to the host on which the IBM WebSphere Application Server OEM Edition for z/OS instance is running. If your network connectivity is functioning properly, there might be an issue with the digital certificates used for SSL connections.

Missing initialization message or JSP processing error when attempting to use z/OSMF from browser

**Symptoms:** The following symptoms occur in this sequence:

1. You start IBM WebSphere Application Server OEM Edition for z/OS on the system where z/OSMF is installed, but see no message on the operator log about whether z/OSMF started successfully or failed.
2. You attempt to access the z/OSMF URL but encounter a "JSP Processing Error" with HTTP code 500, along with some text like the following with supporting messages:
   
   JSPG0049E: /NavigationTree.jsp failed to compile

3. You examine the z/OSMF logs and find that they are empty or have no new messages since starting IBM WebSphere Application Server OEM Edition for z/OS. No .lck file exists either, which suggests that the logs are not active.
4. You examine IBM WebSphere Application Server OEM Edition for z/OS servant logs and search for "IZUG" looking for message codes. While none exist, you notice that the search reveals the following:
   
   UTLS0002E: The shared library IzuSrvLibs contains a classpath entry which does not resolve to a valid jar file, the library jar file is expected to be found at /usr/lpp/zosmf/V1R13/lib/izugjni.jar.

**Possible Cause:** A failure of the JSP to compile typically means that one or more of the required classes could not be found. Most likely, this is a problem with a referenced shared library.

Failures with the shared libraries typically mean either of two things:
- Shared libraries class path entries are incorrect.
- Class path entries point to missing JAR files.

In this situation, the WebSphere message shows which paths were not found.

**Investigation:** Use the following procedure to determine the cause of this error.

1. Examine the contents of the directory where the JARs are supposed to exist:
   
   # ls /usr/lpp/zosmf/V1R13/lib
   
   ls: FSUM6785 File or directory "/usr/lpp/zosmf/V1R13/lib" is not found

2. The directory does not exist, so inspect which file systems are mounted.
   
   [Figure 38 on page 170](#) shows an example.
In Figure 38, notice that the display is missing the product file system, which should be mounted at the location specified on the IZU_CODE_ROOT configuration variable.

**Corrective Action:** Mount the necessary file system in the correct location and restart IBM WebSphere Application Server OEM Edition for z/OS.

**Certificate error in Mozilla Firefox Version 3**

When logging into z/OSMF for the first time, you might notice that the Mozilla Firefox Version 3 browser displays the error message: Secure Connection Failed (Figure 39).

The error message occurs because the browser does not recognize the self-signed Certificate Authority (CA) certificate configured in the application server hosting the z/OSMF application.
To resolve the certificate error message, you can use either of the following methods:

- “Adding the CA certificate to the security exceptions list”
- “Importing the CA certificate into your browser” on page 172

These methods are described in the sections that follow.

**Adding the CA certificate to the security exceptions list**

You can allow your browser to bypass the Secure Connection Failed message for z/OSMF.

Do the following:

1. On the error page, click **Or you can add an exception**.
2. Click **Add Exception**. The **Add Security Exception** dialog is displayed.
3. Click **Get Certificate**.
4. Click **View** to display a window that describes the problem with your z/OSMF site. Figure 40 shows an example.

![Figure 40. Connection failure message in Firefox Version 3](image)

Examine the **Issued To** fields. Verify that the information identifies the WebSphere application server that is hosting z/OSMF. The value for **Common Name (CN)** should match the host name for your installation of z/OSMF.

Examine the **Issued By** fields. Verify that the certificate was issued by the certificate authority (CA) that was used to generate the server certificate. By default, IBM WebSphere Application Server OEM Edition for z/OS uses the certificate authority **WAS CertAuth for Security Domain**.

To see the other fields of the certificate, select the **details** tab.

5. After you have verified the certificate, close the dialog. If you leave the **Permanently store this exception** check box selected, Firefox stores the certificate information to prevent the error from being displayed again for the z/OSMF site.

6. Click **Confirm Security Exception** to trust the z/OSMF site.
Your browser will now connect to the z/OSMF application.

**Importing the CA certificate into your browser**

You can import the CA certificate into your browser. Doing so involves exporting the IBM WebSphere Application Server OEM Edition for z/OS certificate from RACF, transferring the CA certificate to your workstation, and importing the CA certificate into your browser.

The CA certificate is determined by the WebSphere configuration file that you used to create the IBM WebSphere Application Server OEM Edition for z/OS instance. The file provides the controller id (zControlUserid=WSCRU1) and the SAF keyring name (zDefaultSAFKeyringName=WASKeyring.BBNBASE).

To import the CA certificate into your browser, do the following:

1. List the keyring for the controller user ID using the RACDCERT command, for example:

   ```
   RACDCERT ID(WSCRU1) LISTRING(*)
   ```

   Figure 41 shows an example of the output from the RACDCERT command.

<table>
<thead>
<tr>
<th>Certificate Label Name</th>
<th>Cert Owner</th>
<th>USAGE</th>
<th>DEFAULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebSphereCA</td>
<td>CERTAUTH</td>
<td></td>
<td>NO</td>
</tr>
<tr>
<td>Verisign Class 3 Primary CA</td>
<td>CERTAUTH</td>
<td></td>
<td>NO</td>
</tr>
<tr>
<td>Verisign Class 1 Primary CA</td>
<td>CERTAUTH</td>
<td></td>
<td>NO</td>
</tr>
<tr>
<td>RSA Secure Server CA</td>
<td>CERTAUTH</td>
<td></td>
<td>NO</td>
</tr>
<tr>
<td>Thawte Server CA</td>
<td>CERTAUTH</td>
<td></td>
<td>NO</td>
</tr>
<tr>
<td>Thawte Premium Server CA</td>
<td>CERTAUTH</td>
<td></td>
<td>NO</td>
</tr>
<tr>
<td>Thawte Personal Basic CA</td>
<td>CERTAUTH</td>
<td></td>
<td>NO</td>
</tr>
<tr>
<td>Thawte Personal Freemail CA</td>
<td>CERTAUTH</td>
<td></td>
<td>NO</td>
</tr>
<tr>
<td>Thawte Personal Premium CA</td>
<td>CERTAUTH</td>
<td></td>
<td>NO</td>
</tr>
<tr>
<td>Verisign International Svr CA</td>
<td>CERTAUTH</td>
<td></td>
<td>NO</td>
</tr>
</tbody>
</table>

   Figure 41. Digital ring information for the controller user ID

   Verify that the configured SAF keyring is shown for the controller user ID. Note the keyring name and the certificate label (WebSphereCA, in this case).

2. Export the CA certificate using the RACDCERT command, for example:

   ```
   RACDCERT EXPORT(LABEL(' WebSphereCA')) ID(WSCRU1) CERTAUTH DSN('WASOEM.CERT.AUTH.DER') FORMAT(CERTDER)
   ```

3. Transfer this file in binary format to your workstation. Keep the .der extension when you transfer the file.

4. To import the certificate into the Firefox browser, do the following:

   a. From the Tools menu, click Options > Advanced tab.
   b. Click View Certificates.
   c. Select the Authorities tab.
d. Click Import.
e. From the Select File menu, navigate to the folder to which you transferred the CA certificate.
f. Select the certificate file and click Open.
g. In the dialog box, select the Trust this CA to identify web sites check box. You can also click View to examine the certificate.
h. To import the certificate to your browser, click OK.

Your browser will now open to the z/OSMF interface.

**Cannot log into z/OSMF**

If you receive an error while attempting to log into z/OSMF, try troubleshooting with the following steps.

**Procedure**

1. Verify that your user ID is correct and then try logging in. If you are still not able to log in, continue to the next step.
2. Ensure that the password associated with your user ID is correct. If you are still not able to log in, continue to the next step.
3. It is possible that the password for your user ID has expired. Try creating a new password for the user ID and then log in.
4. If you are attempting to log in with a password phrase (pass phrase), your installation’s security product might need to be updated to allow mixed case passwords. In a system with RACF, for example, your security administrator can use the SETROPTS PASSWORD(MIXEDCASE) option to allow mixed-case passwords at your installation. After this change is made, your installation must restart IBM WebSphere Application Server OEM Edition for z/OS. For more information, see z/OS Security Server RACF Security Administrator’s Guide SA22-7683. Also, see the WebSphere Application Server for z/OS Information Center.
5. Ensure that the appropriate script has been run for your user ID; see “Authorizing users to z/OSMF” on page 120.

**What to do next**

If none of these steps resolve the problem, contact your system programmer for assistance.

End user messages for authentication errors are often general by design, to avoid providing malicious users with valuable information, such as whether a particular user ID is valid. More specific information about this error might be available to your system programmer in the form of messages written to the operator console or to the operator log. Typically, these problems are caused by incorrect passwords or user IDs that have been revoked.

**Message or help information is not available**

**Symptom:** The help information for messages or pages is not available.

**Possible Cause:** The help files are missing or not readable, or new help files were installed and z/OSMF was not restarted.

The z/OSMF help files must reside at the location `<IZU_CONFIG_DIR>/helps/eclipse/plugins/zosmf.properties`. By default, the `<IZU_CONFIG_DIR>`
directory is /etc/zosmf. If your installation set the IZU_CONFIG_DIR configuration variable to a value other than /etc/zosmf, you must create a symlink from /etc/zosmf to the location specified for IZU_CONFIG_DIR.

**Administrator Action:** Use the following procedure to resolve this error.
1. Verify that the following file is present and readable: `<IZU_CONFIG_DIR>/helps/eclipse/plugins/zosmf.properties`
2. Verify that symlinks exist in the /etc/zosmf/helps subdirectory. The symlinks should refer to the product file system (configuration variable IZU_CODE_ROOT).
3. If your installation selected a different directory for the IZU_CONFIG_DIR configuration variable, verify that the symlink /etc/zosmf exists and refers to the location you chose.
4. Verify that the EJBROLE resource class is defined properly; it is case sensitive.

**A script takes too long to run or is not responding**
When using z/OSMF, you might encounter the long-running script dialog, which means that a script is taking a long time to run or that a script has stopped responding. From the dialog, you can decide either to stop executing the script or to continue executing it. If you stop executing the script, the function on that web page that is dependent upon the script might not function properly. If you continue executing the script, the dialog will re-display each time the number of statements executed or the amount of time executing a script exceeds the browser's threshold.

To decrease the number of times the long-running script dialog is displayed, you can increase the maximum amount of time a script is allowed to execute or you can increase the maximum number of statements that can be executed. Whether you are modifying the amount of time or the number of statements is dependent upon the browser. For example, the Firefox threshold is based on time; while the Internet Explorer threshold is based on the number of statements.

For more information about unresponsive or long-running scripts, see the appropriate support web site for your browser:

**Firefox**
- See the following Mozilla web site for information you might find useful: [http://support.mozilla.com/en-US/kb/Warning+Unresponsive+script](http://support.mozilla.com/en-US/kb/Warning+Unresponsive+script)

**Internet Explorer**
- See the following Microsoft web site for information you might find useful: [http://support.microsoft.com/kb/175500](http://support.microsoft.com/kb/175500)

**Problems when using Configuration Assistant**
This section provides a procedure you can use to send troubleshooting documentation to IBM Support.

**Steps for sending information to IBM Support**
In case of a failure in Configuration Assistant, use this procedure to provide troubleshooting documentation to IBM Support.
Procedure
1. In the Configuration Assistant task in z/OSMF, use the menu option **Actions > Tools > Collect Problem Determination Information**. A zip file of troubleshooting information is created.
2. Send the zip file to IBM Support.

Problems when using the ISPF task

This topic provides troubleshooting tips for common problems that might occur while using the ISPF task.

Troubleshooting topics are included for the following problems and scenarios:
- "Unexpected behavior occurs in the ISPF user session after the user logs on again."
- "Log-on or log-off through the ISPF task takes too long." on page 176
- "Log-on through the ISPF task takes too long, even though the system is enabled for reconnectable user sessions." on page 176.

Unexpected behavior occurs in the ISPF user session after the user logs on again.

**Symptom:** User logs off from an ISPF session. On logging on again, the user encounters an unexpected behavior, such as one of the following:
- z/OSMF ISPF environment is not reset
- Logon proc is not run
- Region size is not restored
- Session behaves unexpectedly in some other manner.

**Probable cause:** The user required a new session, but the ISPF task reconnected the user to an existing session. To save time and system resources, the ISPF task can reconnect a user to an existing session, rather than creating a new session. This reconnect capability requires that some aspects of the user session be preserved after logoff (the session is not completely ended). In some cases, this processing can pose a problem for users who require that their sessions be completely ended and cleaned up during logoff.

**Corrective Action:** The user can force z/OSMF to create a new session, rather than reconnect to an existing session, by changing one of the logon settings. For example, changing the screen size or region size slightly would result in a new session being created.

If this problem occurs frequently or for multiple z/OSMF users, consider deactivating the reconnect capability for the ISPF task. You can do so through parmlib member, CEAPRMxx, which is used to specify options for the common event adapter (CEA) component of z/OS. In CEAPRMxx, the following statements control the reconnect capability for the ISPF task:
- **RECONTIME** limits the number of reconnectable sessions
- **RECONSESSION** limits the time that sessions can remain in a reconnectable state.

To deactivate the reconnect capability for the ISPF task, set one or both of these values to zero, as indicated in the commented section of IBM-supplied member, CEAPRM00. For more information about CEAPRM00, see **z/OS MVS Initialization and Tuning Reference** SA22-7592.
Log-on or log-off through the ISPF task takes too long.

Possible Cause: The extra time is used by the system during logon processing to perform a complete log-on for the user. Or, to log-off the user and clean-up the user address space.

Corrective Action: Enable the use of reconnectable sessions for ISPF task users. Doing so can allow for potentially faster logon processing when existing user sessions are eligible for re-use.

Enabling reconnectable user sessions involves modifying the CEA component on your system through parmlib member CEAPRMxx. See the descriptions of statements TSOASMGR, RECONSESSIONS, and RECONTIME in z/OS MVS Initialization and Tuning Reference SA22-7592. If reconnectable user sessions are already enabled, consider increasing either the RECONSESSIONS or RECONTIME values.

Log-on through the ISPF task takes too long, even though the system is enabled for reconnectable user sessions.

Symptom: User selects the ISPF task, but the resultant log-on takes too long, even though the z/OS system is enabled for reconnectable user sessions.

Possible Cause: On a system enabled for reconnectable user sessions, the ISPF task checks for a session to which the user can reconnect. No eligible session was found, however, possibly because the session has expired, based on one or more system limits. Without an available reconnectable session, the ISPF task creates a new session for the user. The additional processing increases the time for the log-on request to complete.

Another possibility is that the ISPF task has discarded its reconnectable user sessions as part of normal clean-up. This processing occurs when the ISPF task is idle (has no active users) for at least 15 minutes. After the clean-up is completed, a subsequent user of the ISPF task will always receive a new session.

Corrective Action: You can increase the number of reconnectable sessions allowed on your system and the time that sessions can remain connectable. See the descriptions of the RECONTIME and RECONSESSION statements of parmlib member CEAPRMxx in z/OS MVS Initialization and Tuning Reference SA22-7592. Regardless of these settings, the ISPF task discards its reconnectable sessions when it is idle for 15 minutes.

Problems when using the Incident Log task

This topic provides troubleshooting tips for common problems that might occur while using the Incident Log task.

Troubleshooting topics are included for the following problems and scenarios:

- “User cannot access the Incident Log task” on page 177
- “User encounters message ICH408I” on page 177
- “CEA address space is blocking the use of the sysplex dump directory” on page 177
- “CEA cannot allocate a data set for dump prepare or snapshot” on page 178
- “Diagnostic log streams and other incident data for deleted incidents are not being deleted over time” on page 178
User cannot access the Incident Log task

**Symptom:** On selecting the Incident Log task, the user receives an error message indicating a lack of authorization to CEA.

**Probable cause:** During the configuration of z/OSMF, the configuration script defines the resource CEA.CEAPDWB*. However, the resource CEA.* was already defined by your installation. Because CEA.CEAPDWB* takes priority over CEA.*, no z/OSMF users are authorized to make CIM requests.

**Corrective Action:** Give z/OSMF users access to CEA.CEAPDWB*. If you have CEA security definitions configured, you might already have the CEA.* resource defined.

User encounters message ICH408I

ICH408I USER(user ) GROUP(group ) NAME(user ) 031
CATALOG.SYVPLEX.MASTER CL(DATASET ) VOL(volser)
INSUFFICIENT ACCESS AUTHORITY
FROM CATALOG.*.MASTER (G)
ACCESS INTENT(UPDATE ) ACCESS ALLOWED(NONE )

**Possible Cause:** A user with insufficient authority is attempting to update the master catalog while creating the data diagnostic files. As a result, an Incident Log task request to FTP materials cannot compress (terse) the diagnostic snapshot data set.

**Corrective Action:** Allow the user to create catalog entries, as follows:

- To authorize a user to create entries in the master catalog:

  RALTER GLOBAL DATASET ADDMEM('CATALOG.**'/UPDATE)
  ADDSD 'CATALOG.**' UACC(UPDATE)
  SETR GLOBAL(DATASET) REFRESH

- To authorize a user to create entries in a user catalog:

  DEFINE ALIAS(NAME(CEA) RELATE(<usercatalog name>)

CEA address space is blocking the use of the sysplex dump directory

**Possible Cause:** CEA holds an exclusive ENQ to serialize on the sysplex dump directory data set while processing a z/OSMF request. Usually, the ENQ is released in microseconds. But sometimes an I/O error could result in holding the ENQ for longer time periods, therefore blocking DUMPSRV from updating the dump directory with information about a new dump, or your installation from doing maintenance on the sysplex dump directory data set.

**Corrective Action:** Use the z/OS system console command F CEA, DROPIPCS to disconnect CEA from the IPCS sysplex dump directory data set.
CEA cannot allocate a data set for dump prepare or snapshot

Possible Cause: CEA alias is not cataloged properly.

Corrective Action: If your installation has a user catalog setup instead of using the MASTER catalog, you might need to define the CEA alias to the user catalog. For example:

```
DEFINE ALIAS(NAME(CEA) RELATE(YOUR_CATALOG_NAME))
```

Diagnostic log streams and other incident data for deleted incidents are not being deleted over time

Possible Cause: If you modified the HLQ parameter value in the CEAPRMxx parmlib member, CEA no longer detects the previously-stored diagnostic data files stored under the old high level qualifier.

Corrective Action: Carefully remove the data manually. The data exists in both log stream and data set format. Use caution as to not remove any needed data.

Remove data sets and log streams manually.

To list the available log streams, enter the following z/OS system console command:

```
D LOGGER,L
```

Most log streams with the status of AVAILABLE are the result of diagnostic snapshots taken at the time of the dump. The old high level qualifier appears in the log streams that were created earlier by CEA.

To delete log streams, enter the following command:

```
SETLOGR FORCE,DELETE,LSN=logstreamname
```

To remove data sets, do the following:
- List the data sets having the same HLQ as the available log streams.
- Delete the data sets.

Problems when attempting to send data

When you invoke the Send Diagnostic Data wizard from the Incident Log task, the information supplied in the page is used to produce one FTP job for each diagnostic data file being sent. Thus, if an incident has a dump data set and three log snapshot files, four FTP jobs are created (and the FTP Job Status table will have four entries). To debug the FTP jobs, you need access to the job output. This is most often obtained by using SDSF to examine the spooled output from the job.

FTP job status codes and other information

The Incident Log allows you to display the status of the FTP jobs. On the FTP Job Status page, you can display the status of all FTP jobs associated with a particular incident or the FTP jobs associated with diagnostic data.

For a description of each FTP job status condition and the actions you can take to resolve errors in the jobs, see the online help for the FTP Job Status page.
Part 4. Programming

This section describes the programming interfaces for z/OSMF

Introduction

z/OSMF supports the use of Representational State Transfer (REST) APIs, which are public APIs that your application can use to work with system resources and extract system data. As with implementations of REST services on other platforms, the z/OSMF APIs allow for easy-to-use HTTP services that are language- and platform-independent, stateless, scalable, and easily parsed.

The format for the z/OSMF APIs requests and responses is based on the HTTP/1.1 protocol. Conceptually, your application (the client) issues requests to the target system (z/OS) in the form of request messages. Each request message consists of a request line, optionally followed by request headers (HTTP headers), an empty line, and an optional message body. The request line includes the HTTP method, such as GET, a Universal Resource Identifier (URI) and, where appropriate, parameters that further qualify the request. For requests that return data, the services define an expected response in the form of a JavaScript Object Notation (JSON) object or another type of response data.

It is assumed that users of these services are familiar with the JSON standard and coding practices. The following references provide additional helpful information:

- Hypertext Transfer Protocol 1.1: [http://www.w3.org/Protocols/rfc2616/rfc2616.html](http://www.w3.org/Protocols/rfc2616/rfc2616.html)
- Multipurpose Internet Mail Extensions (MIME) media types: [http://www.iana.org/assignments/media-types/index.html](http://www.iana.org/assignments/media-types/index.html)
- Introducing JSON: [http://www.json.org](http://www.json.org)

Programming interfaces described in this document

This document describes the following programming interfaces:

- Chapter 12, “Using the z/OS jobs REST interface,” on page 181
- Chapter 13, “Using the Application Linking Manager interface services,” on page 211
Chapter 12. Using the z/OS jobs REST interface

The z/OS jobs REST interface is an application programming interface (API) implemented through industry standard Representational State Transfer (REST) services. This interface allows a client application to perform operations with batch jobs on a z/OS system.

With the z/OS jobs REST interface, an application can use REST services to perform the following operations with batch jobs:
- Obtain the status of a job
- List the jobs for an owner, prefix, or job ID
- List the spool files for a job
- Retrieve the contents of a job spool file
- Submit a job to run on z/OS
- Cancel a job
- Change the job class of a job
- Cancel a job and purge its output.

Software requirements

Using the z/OS jobs REST interface requires one of the following minimum levels of JES on your z/OS system: JES2 V1R13 or JES3 V1R13.

Processing overview

The z/OS jobs REST interface services can be invoked by any HTTP client application, running on the z/OS local system or a remote system.

Your program (the client) initiates an HTTP request to the z/OS jobs REST interface. If the interface determines that the request is valid, it performs the requested service. After performing the service, the z/OS jobs REST interface creates an HTTP response. If the request is successful, this response takes the form of an HTTP 2nn response and, if applicable, a result set that is passed back to your program. Depending on which service was requested, the result set might be returned in a format that requires parsing by your program, for example, a JSON object. In other cases, results might be returned in another format, such as plain text or binary data. If the request is not successful, the response consists of a non-OK HTTP response code with details of the error provided in the form of a JSON object.

The contents of the JSON objects are described in "JSON document specifications" on page 202.

Resource URLs

The URLs of the z/OS jobs REST interface have the format shown in Figure 42:

https://{host}:{port}/zosmf/restjobs/jobs/{resource}?{parm}

Figure 42. Format of resource URLs for z/OS jobs REST interface.

where:
HTTP methods

The z/OS jobs REST interface provides the following HTTP methods:

GET
Retrieves information about jobs running on the z/OS system.

PUT
Updates job information on the z/OS system, or sets attributes and performs actions on jobs.

DELETE
Removes jobs from the z/OS system.

Some situations might require the use of the POST method; see “Usage considerations” on page 183.

Supported HTTP versions

z/OS jobs REST interface supports requests in either of the following protocols:
HTTP/1.0 or HTTP/1.1

Content types

The data sent or returned by the HTTP methods has one of the following content types:

- Application/octet-stream ("Content-Type: application/octet-stream") is used for data sent or returned in an uninterpreted format, such as a job being submitted, or binary data or records obtained from a z/OS job spool file.
- JSON ("Content-Type: application/json") is used for sent data and returned data; for the detailed format of each JSON object, see the description for each operation.
- Plain text ("Content-Type: plain/text").

Error handling

For errors that occur during the processing of a request, the z/OS jobs REST interface returns an appropriate HTTP status code to the calling client. An error is indicated by a 4nn code or a 5nn code. For example, "HTTP/1.1 400 Bad Request" or "HTTP/1.1 500 Internal Server Error".

In addition, the z/OS jobs REST interface returns a JSON ErrorReport document with information about the problem. You can use this information to diagnose the problem or provide it to IBM Support, if required. The JSON ErrorReport document returned for HTTP request failures might also include additional messages and a stack trace. For the contents of the ErrorReport document, see “ErrorReport document” on page 204.

Error logging

An INFO level log message is issued when an HTTP error response is to be sent. The log message includes the exception.
Required authorizations

Generally, your user ID requires the same authorizations for using the z/OS jobs REST interface services as when you perform these operations through a TSO/E session on the system. For example, submitting a job through the z/OS jobs REST interface requires that your user ID be authorized to run jobs on the system and be able to access any protected resources that the job might require.

In addition, your user ID requires authorization to the WebSphere SAF profile prefix on the target z/OS system, as follows:

- READ access to `<WebSphere-SAF-profile-prefix>` in the APPL class.
- READ access to the `<WebSphere-SAF-profile-prefix>.izuUsers` profile in the EJBROLE class.

By default, the WebSphere SAF profile prefix is BBNBASE.

Besides these authorizations, the following services require that your user ID be authorized to the Common Information Model (CIM) server and permitted to the JES2-JES3Jobs CIM provider:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cancel a job</td>
<td>PUT</td>
</tr>
<tr>
<td>Change the class of a job</td>
<td>PUT</td>
</tr>
<tr>
<td>Cancel a job and purge its output</td>
<td>DELETE</td>
</tr>
</tbody>
</table>

CIM provides jobs (CFZSEC and CFZRCUST) to help you configure the CIM server, including security authorizations and file system customization. For information, see the chapter on CIM server quick setup and verification in Common Information Model User's Guide SC33-7998.

Where applicable, additional authorization requirements are noted in the descriptions of the individual z/OS jobs REST interface services.

Usage considerations

Observe the following considerations when using the z/OS jobs REST interface services:

- The z/OS jobs REST interface services run as unauthorized programs on z/OS.
- As with any z/OSMF task, the z/OS jobs REST interface services compete for z/OSMF resources with users of the z/OSMF web browser interface. Thus, concurrent high usage of the z/OS jobs REST interface services can affect response time for users of the z/OSMF web browser interface.
- During periods of concurrent high usage of the z/OS jobs REST interface services, an application can experience connection failures, such as connection refused, connection timed out, or connection reset. In these cases, the application should try the request again. The number of retry attempts needed will depend on how much work is being requested of the server. It might be necessary for your installation to modify the workload and reduce the arrival rate of requests.
- Some browsing environments do not support all of the HTTP methods, such as HTML 4 or XHTML 1, or might block applications from accessing response content having non-successful HTTP response status codes (4nn and 5nn). As a workaround, your application can use the following custom HTTP request headers:
**Requested-Method:**
GET, PUT, and DELETE requests can be “tunneled” through a **POST** method using this custom HTTP header.

**Bypass-Status:**
If set to true, all response status codes are set to 200, and the custom HTTP response header **Actual-Status** is included in the returned data. To determine the original status code, your application must check the **Actual-Status** header.

### How this chapter is organized

**Table 32. Operations provided through the z/OS jobs REST interface services.**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Method</th>
<th>Where described</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain the status of a job</td>
<td>GET</td>
<td>&quot;GET method: Obtain the status of a job&quot; on page 185</td>
</tr>
<tr>
<td>List the jobs for an owner, prefix, or job ID</td>
<td>GET</td>
<td>&quot;GET method: List the jobs for an owner, prefix, or job ID&quot; on page 187</td>
</tr>
<tr>
<td>List the spool files for a job</td>
<td>GET</td>
<td>&quot;GET method: List the spool files for a job&quot; on page 189</td>
</tr>
<tr>
<td>Retrieve the contents of a job spool file</td>
<td>GET</td>
<td>&quot;GET method: Retrieve the contents of a job spool file&quot; on page 191</td>
</tr>
<tr>
<td>Submit a job to run on z/OS</td>
<td>PUT</td>
<td>&quot;PUT method: Submit a job&quot; on page 194</td>
</tr>
<tr>
<td>Cancel a job</td>
<td>PUT</td>
<td>&quot;PUT method: Cancel a job&quot; on page 196</td>
</tr>
<tr>
<td>Change the class of a job</td>
<td>PUT</td>
<td>&quot;PUT method: Change the class of a job&quot; on page 198</td>
</tr>
<tr>
<td>Cancel a job and purge its output</td>
<td>DELETE</td>
<td>&quot;DELETE method: Cancel a job and purge its output&quot; on page 200</td>
</tr>
</tbody>
</table>
GET method: Obtain the status of a job

You can use the GET method to obtain the status of a batch job on z/OS.

URL format

The following figure shows the format of the URL for this request.

https://host:port/zosmf/restjobs/jobs/jobname/jobid

where jobname/jobid identifies the job name and job ID for which status is requested.

Query parameters

None.

Required authorizations

See “Required authorizations” on page 183.

Usage considerations

Observe the following considerations for this request:
- This request can be directed to a secondary JES subsystem. To do so, use the following request format:

https://host:port/zosmf/restjobs/jobs/-JESB/jobname/jobid

where JESB is the name of the secondary JES subsystem.

Expected response

On completion, the z/OS jobs REST interface returns an HTTP response with a JSON Job document. For the contents, see “Job document” on page 202.

For errors, z/OS jobs REST interface returns an appropriate HTTP status code and error information as a JSON ErrorReport document. See “ErrorReport document” on page 204.

Example

The following request obtains the status for the job G1JAVA1B, job ID JOB00023:

GET /zosmf/restjobs/jobs/G1JAVA1B/JOB00023 HTTP/1.1

A sample response is shown in Figure 43 on page 186.
HTTP/1.1 200 OK
Date: Thu, 12 Jan 2012 05:39:28 +0000
Content-Type: application/json
Connection: close

{
   "jobid":"JOB00023","jobname":"G1JAVA1B","subsystem":null,"owner":"G1JAVA1",
   "status":"OUTPUT","type":"JOB","class":"A","retcode":"CC 0000",
   "url":"https://host:port/zosmf/restjobs/jobs/G1JAVA1B\JOB00023",
   "files-url":"https://host:port/zosmf/restjobs/jobs/G1JAVA1B\JOB00023/files"
}

Figure 43. Example: Returned job status
GET method: List the jobs for an owner, prefix, or job ID

You can use the GET method to list the jobs for an owner, prefix, or job ID.

URL format

The following figure shows the various formats of the URL for this request, depending on the data to be requested.

```
https://host:port/zosmf/restjobs/jobs
https://host:port/zosmf/restjobs/jobs?owner=owner
https://host:port/zosmf/restjobs/jobs?prefix=prefix*
https://host:port/zosmf/restjobs/jobs?owner=owner&prefix=prefix*
https://host:port/zosmf/restjobs/jobs?jobid=jobid
https://host:port/zosmf/restjobs/jobs?max-jobs=nnn
```

Query parameters

You can specify one or more of the following optional query parameters on this request:

- **owner**
  User ID of the job owner whose jobs are being queried; the default is the z/OS user ID. Folded to upper case; cannot exceed eight characters.

- **prefix**
  Job name prefix; defaults is '*'. Folded to upper case; cannot exceed eight characters.

- **jobid**
  Job ID. Folded to upper case; cannot exceed eight characters.

- **max-jobs**
  Maximum number of jobs returned. The value must be between 1 and 1000, inclusive. If this parameter is not specified, or is specified incorrectly, the default value of 1000 is used.

Observe the following conventions:
- You can use zero or more of the query parameters in the request.
- You use '?' to separate the first query parameter from the resource.
- To specify multiple query parameters in combination, use an ampersand (&).
- Wildcard characters '*' (multiple characters) and '?' (single character) are permitted in the owner and prefix query parameter values.

Required authorizations

See "Required authorizations" on page 183.

Usage considerations

Observe the following considerations for this request:
- This request can be directed to a secondary JES subsystem. To do so, use the following request format:
where JESB is the name of the secondary JES subsystem in these examples.

- The ordering of the jobs returned is not predictable.
- If the maximum number of jobs is returned, no indication is provided for whether more jobs remain to be retrieved.

**Expected response**

On completion, the z/OS jobs REST interface returns an HTTP response with an array of matching jobs, each as a JSON Job document. For the contents, see "Job document" on page 202.

For errors, z/OS jobs REST interface returns an appropriate HTTP status code and error information as a JSON ErrorReport document. See "ErrorReport document" on page 204.

**Example**

In the following example, the GET method is used to list the jobs that are owned by G1JAVA1 and have a prefix beginning with G1JAVA:

```
GET /zosmf/restjobs/jobs?owner=G1JAVA1&prefix=G1JAVA* HTTP/1.1
```

A sample response is shown in Figure 44.

```
HTTP/1.1 200 OK
Date: Thu, 12 Jan 2012 05:39:28 +0000 GMT
Content-Type: application/json
Connection: close

[
  
  "jobid": "JOB00023", "jobname": "G1JAVA1B", "subsystem": null, "owner": "G1JAVA1", "status": "OUTPUT", "type": "JOB", "class": "A", "retcode": "CC 0000", "url": "https://host:port/zosmf/restjobs/jobs/G1JAVA1B/JOB00023", "files-url": "https://host:port/zosmf/restjobs/jobs/G1JAVA1B/JOB00023/files"},
  
]
```

**Figure 44. Example: Returned list of the jobs for an owner and job ID prefix**
GET method: List the spool files for a job

You can use the GET method to list the spool files for a batch job on z/OS.

URL format

The following figure shows the format of the URL for this request.

https://host:port/zosmf/restjobs/jobs/jobname/jobid/files

where jobname/jobid identifies the job name and job ID for which the spool files are to be listed.

Query parameters

None.

Required authorizations

See “Required authorizations” on page 183.

Usage considerations

Observe the following considerations for this request:

- This request can be directed to a secondary JES subsystem. To do so, use the following request format:

  https://host:port/zosmf/restjobs/jobs/-JESB/jobname/jobid/files

  where JESB is the name of the secondary JES subsystem.

Expected response

On completion, the z/OS jobs REST interface returns an HTTP response with an array of zero or more JSON JobFile documents. For the contents, see “JobFile document” on page 203.

For errors, z/OS jobs REST interface returns an appropriate HTTP status code and error information as a JSON ErrorReport document. See “ErrorReport document” on page 204.

Example

The following request lists the spool files for the job G1JAVA1B, job ID JOB00023:

GET /zosmf/restjobs/jobs/G1JAVA1B/JOB00023/files HTTP/1.1

A sample response is shown in Figure 45 on page 190.
HTTP/1.1 200 OK
Date: Thu, 12 Jan 2012 05:39:28 +0000 GMT
Content-Type: application/json
Connection: close

[{
  "jobid": "JOB00023", "jobname": "G1JAVA1B", "subsystem": null, "id": 1,
  "stepname": "JESE", "procstep": null, "class": "H",
  "ddname": "JESMSGLG", "record-count": 14, "byte-count": 1200,
  "records-url": "https://host:port/zosmf/restjobs/jobs/G1JAVA1B/JOB00023/1/records"},
{
  "jobid": "JOB00023", "jobname": "G1JAVA1B", "subsystem": null, "id": 2,
  "stepname": "JESE", "procstep": null, "class": "H",
  "ddname": "JESJCL", "record-count": 10, "byte-count": 526,
  "records-url": "https://host:port/zosmf/restjobs/jobs/G1JAVA1B/JOB00023/2/records"},
{
  "jobid": "JOB00023", "jobname": "G1JAVA1B", "subsystem": null, "id": 3,
  "stepname": "JESE", "procstep": null, "class": "H",
  "ddname": "JESYSMSG", "record-count": 14, "byte-count": 1255,
  "records-url": "https://host:port/zosmf/restjobs/jobs/G1JAVA1B/JOB00023/3/records"},
{
  "jobid": "JOB00023", "jobname": "G1JAVA1B", "subsystem": null, "id": 4,
  "stepname": "STEP57", "procstep": "COMPILE", "class": "H",
  "ddname": "SYSUT1", "record-count": 6, "byte-count": 741,
  "records-url": "https://host:port/zosmf/restjobs/jobs/G1JAVA1B/JOB00023/4/records"},
{
  "jobid": "JOB00023", "jobname": "G1JAVA1B", "subsystem": null, "id": 5,
  "stepname": "STEP57", "procstep": "COMPILE", "class": "A",
  "ddname": "SYSPRINT", "record-count": 3, "byte-count": 209,
  "records-url": "https://host:port/zosmf/restjobs/jobs/G1JAVA1B/JOB00023/5/records"}
]

Figure 45. Example: Returned list of spool files
GET method: Retrieve the contents of a job spool file

You can use the GET method to retrieve the contents of a job spool file on z/OS.

**URL format**

The following figure shows the format of the URL for this request.

```plaintext
https://host:port/zosmf/restjobs/jobs/jobname/jobid/files/nnn/records
```

where:
- `jobname/jobid` identifies the job name and job ID for which the spool files are to be listed
- `nnn` is the ID for the spool file from which the contents are to be retrieved.

**Query parameters**

You can specify translation for the returned data through the mode parameter. The following values are valid for mode:

- **text**
  - The z/OS jobs REST interface translates records from the server codepage to the client codepage and returns the records with Content-Type: plain/text. Trailing spaces are removed and newline characters are used as record separators. This value is the default if you omit the mode parameter.

- **binary**
  - The z/OS jobs REST interface performs no translation and returns the records with Content-Type: application/octet-stream.

- **record**
  - The z/OS jobs REST interface performs no translation and returns the records with Content-Type: application/octet-stream. The z/OS jobs REST interface prefixes each record with a 4-byte (big endian) length.

Specifying the mode parameter with any other value, or no value, results in the default: mode=text.

**Custom headers**

You can use the following optional custom header:

- **Record-Range**
  - Use this header to retrieve a range of records from a spool file. The format is as follows: `SSS-EEE` where `SSS` identifies the start record and `EEE` identifies the end record to be retrieved. Both values are relative offsets (0-based). When `EEE` is set to 0, records through the end of the spool file are retrieved.

For an example of how this custom header is used, see “Examples” on page 192.

**Required authorizations**

See “Required authorizations” on page 183.

In addition, your user ID requires READ access to the JESSPOOL profile for the spool data set. If no profile exists, only the user who created the spool data set can access, modify, or delete it. For information about spool data set security.
considerations, see *z/OS JES Application Programming, SA23-2240*.

**Usage considerations**

The response does not include the Content-Length header. Because the server streams the data rather than buffering it in memory, it is usually not possible for the server to determine the total content length of the data before completing the transfer. For similar reasons, the response does not include the Content-Range header, either.

**Restrictions**

You cannot direct this request to a secondary JES subsystem. Attempting to do so results in a "not implemented" service error.

**Expected response**

On completion, the z/OS jobs REST interface returns an HTTP response with content type defined by the mode query parameter.

For errors, z/OS jobs REST interface returns an appropriate HTTP status code and error information as a JSON ErrorReport document. See "ErrorReport document" on page 204.

**Examples**

In the following example, the GET method is used to retrieve the contents of spool file 1 for the job G1JAVA1B, job ID JOB00023:

```
GET /zosmf/restjobs/jobs/G1JAVA1B/JOB00023/files/1/records HTTP/1.1
```

A sample response is shown in Figure 46.

```
HTTP/1.1 200 OK
Date: Thu, 12 Jan 2012 05:39:28 +0000 GMT
Content-Type: text/plain
Connection: close

JES2 JOBLOG -- SYSTEM EIMG -- NODE DCEIMGW

15.49.11 JOB00023 --- TUESDAY, 10 JAN 2012 ----
15.49.11 JOB00023 IRR010I USERID G1JAVA1 IS ASSIGNED TO THIS JOB.
15.49.11 JOB00023 ICH70001I G1JAVA1 LAST ACCESS AT 15:48:25 ON TUESDAY, JANUARY 10, 2012
15.49.11 JOB00023 $HASP373 INSTALL STARTED - INIT 2 - CLASS A - SYS EIMG
15.49.11 JOB00023 IEF403I INSTALL - STARTED - TIME=15.49.11
15.49.16 JOB00023 IEF404I INSTALL - ENDED - TIME=15.49.16
15.49.16 JOB00023 $HASP395 INSTALL ENDED

------ JES2 JOB STATISTICS ------
10 JAN 2012 JOB EXECUTION DATE
71 CARDS READ
287 SYSOUT PRINT RECORDS
0 SYSOUT PUNCH RECORDS
13 SYSOUT SPOOL KBYTES
0.08 MINUTES EXECUTION TIME
```

*Figure 46. Example: Returned spool file content*

In the following example, the GET method is used to retrieve a range of records (the first 250) using the Record-Range custom header:
A sample response is shown in Figure 47.

GET /zosmf/restjobs/jobs/G1JAVA1B/JOB00023/files/8/records HTTP/1.1
Record-Range: 0-249

HTTP/1.1 200 OK
Date: Thu, 12 Jan 2012 05:39:28 +0000GMT
Content-Type: text/plain
Connection: close
...(the first 250 records)

Figure 47. Example: Returned spool file content (a range of records)
PUT method: Submit a job

You can use the PUT method to submit a job to run on z/OS.

URL format

The following figure shows the format of the URL for this request.

https://host:port/zosmf/restjobs/jobs

Standard headers

Use the following standard HTTP header with this request:

Content-Type
One of the following values, as appropriate:
- Set to text/plain when the optional header Intrdr-Mode is set to TEXT, or is omitted.
- Set to application/octet-stream when optional header Intrdr-Mode is set to RECORD or BINARY.

Custom headers

Optionally, you can include one of the following custom HTTP headers with this request:

Intrdr-Class
A single character that specifies the internal reader class; the default is A.

Intrdr-Recfm
A single character that specifies the internal reader record format; one of F or V; the default is F. If you specify a value other than F or V, the default is used instead.

Intrdr-Lrecl
An integer value specifying the internal reader logical record length; the default is 80. If you specify a non-integer value, the default is used instead.

Intrdr-Mode
A keyword that specifies the format of the input job: TEXT, RECORD, or BINARY. The default is TEXT.
- If BINARY is specified, Intrdr-Recfm must be F.
- If RECORD or BINARY is specified, Content-Type must be set to application/octet-stream.

Query parameters

Not applicable.

Input to this request

- Internet media type: text/plain or application/octet-stream
- HTTP request with optional headers followed by job to be submitted.

Required authorizations

See "Required authorizations" on page 183.
In addition, your user ID must be authorized to run jobs on the system and be able to access any protected resources that the job might require. For information about the security considerations for job submission, see z/OS JES2 Initialization and Tuning Guide, SA22-7532, or z/OS JES3 Initialization and Tuning Guide, SA22-7549.

Restrictions

You cannot direct this request to a secondary JES subsystem. Attempting to do so results in a “not implemented” service error.

Expected response

On completion, the z/OS jobs REST interface returns an HTTP response with a JSON Job document. For the contents, see “Job document” on page 202.

For errors, z/OS jobs REST interface returns an appropriate HTTP status code and error information as a JSON ErrorReport document. See “ErrorReport document” on page 204.

Example

The following request submits the job G1JAVA1J to run on z/OS:

---

PUT /zosmf/restjobs/jobs HTTP/1.1
Content-Type: text/plain
Intrdr-Class: A
Intrdr-Recfm: F
Intrdr-Lrecl: 80
Intrdr-Mode: TEXT

//G1JAVA1J JOB (),MSGCLASS=H
// EXEC PGM=IEFBR14

---

A sample response is shown in Figure 48.

```
HTTP/1.1 201 Created
Date: Thu, 12 Jan 2012 05:39:28 +0000GMT
Content-Type: application/json
Connection: close

{
  "jobid":"JOB00025","jobname":"G1JAVA1J","subsystem":null,"owner":"G1JAVA1","status":"INPUT","type":"JOB","class":"A","retcode":null,
  "url":"https:\/\/host:port\/zosmf\/restjobs\/jobs\/G1JAVA1J\/JOB00025",
  "files-url":"https:\/\/host:port\/zosmf\/restjobs\/jobs\/G1JAVA1J\/JOB00025\/files"
}
```

Figure 48. Example: Returned results of a job submission
PUT method: Cancel a job

You can use the PUT method to cancel a job on z/OS.

URL format

The following figure shows the format of the URL for this request.

https://host:port/zosmf/restjobs/jobs/jobname/jobid

where jobname/jobid identifies the job to be cancelled.

Query parameters

None.

Input to this request

- Internet media type: application/json
- HTTP request with JSON document containing the "request":"cancel" property.

Required authorizations

See "Required authorizations" on page 183.

In addition, your user ID must be authorized to cancel the job on the system. For information about the security considerations for job cancellation, see z/OS JES2 Initialization and Tuning Guide, SA22-7532, or z/OS JES3 Initialization and Tuning Guide, SA22-7549.

Restrictions

You cannot direct this request to a secondary JES subsystem. Attempting to do so results in a "not implemented" service error.

Expected response

On completion of this request, the z/OS jobs REST interface returns an HTTP response. This response is independent of whether the job is actually cancelled.

For errors, z/OS jobs REST interface returns an appropriate HTTP status code and error information as a JSON ErrorReport document. See "ErrorReport document" on page 204.

Example

The following request cancels the job G1JAVA1B, job ID JOB00023 on z/OS:
A sample response is shown in Figure 49

HTTP/1.1 202 Accepted
Date: Thu, 12 Jan 2012 05:39:28 +0000 GMT
Connection: close

Figure 49. Example: Returned results of a job cancellation
PUT method: Change the class of a job

You can use the PUT method to change the class of a job on z/OS.

URL format

The following shows the format of the URL for this request.

https://host:port/zosmf/restjobs/jobs/jobname/jobid

where jobname/jobid identifies the job for which the class is to be changed.

Query parameters

None.

Input to this request

- Internet media type: application/json
- HTTP request with JSON document containing the "class":"<new_job_class>" property.

Usage considerations

The specified job class is not validated on input. To verify the success of this request, your program can issue a GET request for the job status, and check the class value in the returned JSON Job document. See "GET method: Obtain the status of a job" on page 185.

Restrictions

You cannot direct this request to a secondary JES subsystem. Attempting to do so results in a "not implemented" service error.

Required authorizations

See "Required authorizations" on page 183.

Expected response

On completion of this request, the z/OS jobs REST interface returns an HTTP response. This response is independent of whether the requested operation completed.

For errors, z/OS jobs REST interface returns an appropriate HTTP status code and error information as a JSON ErrorReport document. See "ErrorReport document" on page 204.

Example

The following request specifies job class A for the job G1JAVA1B, job ID JOB00023, on z/OS:
A sample response is shown in Figure 50.

Figure 50. Example: Returned results of a job cancellation
DELETE method: Cancel a job and purge its output

You can use the DELETE method to cancel a job and purge its output.

URL format

The following figure shows the format of the URL for this request.

```
https://host:port/zosmf/restjobs/jobs/jobname/jobid
```

where jobname/jobid identifies the job to be canceled.

Query parameters

None.

Restrictions

You cannot direct this request to a secondary JES subsystem. Attempting to do so results in a "not implemented" service error.

Required authorization

See "Required authorizations" on page 183.

In addition, your user ID must be authorized to cancel the job on the system, which allows the user to delete the job SYSOUT data sets. For information about the security considerations for job cancellation, see z/OS JES2 Initialization and Tuning Guide, SA22-7532, or z/OS JES3 Initialization and Tuning Guide, SA22-7549.

Expected response

On completion, the z/OS jobs REST interface returns an HTTP response. This response is independent of whether the job is actually cancelled.

For errors, z/OS jobs REST interface returns an appropriate HTTP status code and error information as a JSON ErrorReport document. See "ErrorReport document" on page 204.

Example

The following request cancels the job G1JAVA1B, job ID JOB00023 and purges its output on z/OS:

```
DELETE /zosmf/restJobs/jobs/G1JAVA1B/JOB00023 HTTP/1.1
```

A sample response is shown in Figure 51 on page 201.
Figure 51. Example: Results of a job purge request
JSON document specifications

This section describes the contents of the JSON documents that are used with z/OS jobs REST interface requests.

The following JSON documents are described:

- "Job document"
- "JobFile document" on page 203
- "ErrorReport document" on page 204

Job document

Table 33 shows the contents of the JSON Job document.

Table 33. Contents of the JSON Job document

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobid</td>
<td>Job ID.</td>
</tr>
<tr>
<td>jobname</td>
<td>Job name.</td>
</tr>
<tr>
<td>subsystem</td>
<td>The primary or secondary JES subsystem. If this value is null, the job was processed by the primary subsystem.</td>
</tr>
<tr>
<td>owner</td>
<td>The z/OS user ID associated with the job.</td>
</tr>
<tr>
<td>status={</td>
<td>Job status. One of the following values:</td>
</tr>
<tr>
<td>INPUT</td>
<td>Job is in input processing.</td>
</tr>
<tr>
<td>ACTIVE</td>
<td>Job is running.</td>
</tr>
<tr>
<td>OUTPUT</td>
<td>Job is on the hardcopy output queue.</td>
</tr>
<tr>
<td>type={</td>
<td>Job type. One of the following values:</td>
</tr>
<tr>
<td>JOB</td>
<td>Batch job.</td>
</tr>
<tr>
<td>STC</td>
<td>Started task.</td>
</tr>
<tr>
<td>TSU</td>
<td>TSO/E user.</td>
</tr>
<tr>
<td>class</td>
<td>Job execution class.</td>
</tr>
</tbody>
</table>
Table 33. Contents of the JSON Job document (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>retcode={</td>
<td></td>
</tr>
<tr>
<td>ABENDUnnnn</td>
<td></td>
</tr>
<tr>
<td>ABEND Sxxx</td>
<td></td>
</tr>
<tr>
<td>CANCELED</td>
<td></td>
</tr>
<tr>
<td>CC nnnn</td>
<td></td>
</tr>
<tr>
<td>CONV ABEND</td>
<td></td>
</tr>
<tr>
<td>CONV ERROR</td>
<td></td>
</tr>
<tr>
<td>JCL ERROR</td>
<td></td>
</tr>
<tr>
<td>SEC ERROR</td>
<td></td>
</tr>
<tr>
<td>SYS FAIL</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>

Job completion code. One of the following values:

- **ABENDUnnnn**: Job ended with the user abend code *nnnn*.
- **ABEND Sxxx**: Job ended with the system abend code *xxx*.
- **CANCELED**: Job was canceled.
- **CC nnnn**: Job ended with the completion code *nnnn*.
- **CONV ABEND**: Converter ended abnormally when processing the job.
- **CONV ERROR**: Converter error when processing the job.
- **JCL ERROR**: Job encountered a JCL error.
- **SEC ERROR**: Job failed a security check.
- **SYS FAIL**: System failure.

If this value is null, the job has not yet completed.

<table>
<thead>
<tr>
<th>url</th>
<th>Resource URL based on original HTTP request.</th>
</tr>
</thead>
<tbody>
<tr>
<td>files-url</td>
<td>Resource URL for listing the spool files for the job.</td>
</tr>
</tbody>
</table>

JobFile document

Table 34 shows the contents of the JSON JobFile document.

Table 34. Contents of the JSON JobFile document

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jobid</td>
<td>Job ID.</td>
</tr>
<tr>
<td>jobname</td>
<td>Job name.</td>
</tr>
<tr>
<td>subsystem</td>
<td>The primary or secondary JES subsystem. If this value is null, the job was processed by the primary subsystem.</td>
</tr>
<tr>
<td>id</td>
<td>Data set number (key). This field is integer data type.</td>
</tr>
<tr>
<td>stepname</td>
<td>Stepname for the step that created this data set. This value might be null.</td>
</tr>
<tr>
<td>procstep</td>
<td>Procnname for the step creating this data set. This value might be null.</td>
</tr>
<tr>
<td>class</td>
<td>Class assigned to the spool file.</td>
</tr>
<tr>
<td>ddname</td>
<td>DDNAME for the data set creation.</td>
</tr>
<tr>
<td>record-count</td>
<td>Number of records in the spool file. The value might be 0. This field is integer data type.</td>
</tr>
<tr>
<td>byte-count</td>
<td>Number of bytes on spool consumed by the spool file. The value might be 0. This field is integer data type.</td>
</tr>
<tr>
<td>records-url</td>
<td>Resource URL for retrieving the spool file contents for the job.</td>
</tr>
</tbody>
</table>
**ErrorReport document**

Table 35 shows the contents of the JSON ErrorReport document.

**Table 35. Contents of the JSON ErrorReport document**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>category</td>
<td>Error category. This field is integer data type.</td>
</tr>
<tr>
<td>rc</td>
<td>Return code. This field is integer data type.</td>
</tr>
<tr>
<td>reason</td>
<td>Reason code. This field is integer data type.</td>
</tr>
<tr>
<td>message</td>
<td>Message that describes the error.</td>
</tr>
<tr>
<td>details</td>
<td>(optional) Array of strings containing additional message details.</td>
</tr>
<tr>
<td>stack</td>
<td>Stack trace of the exception.</td>
</tr>
</tbody>
</table>

For the meanings of the category, rc, and reason fields, see “Error reporting categories” on page 205.
**Error reporting categories**

This section describes the error categories and associated error codes that can be returned in the JSON ErrorReport document, described in "ErrorReport document" on page 204.

**Categories**

Table 36 shows the error categories that are defined for errors returned in z/OS jobs REST interface operations.

<table>
<thead>
<tr>
<th>Category</th>
<th>Ordinal Value</th>
<th>Description</th>
<th>Where the error details are described</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynalloc</td>
<td>1</td>
<td>BPXWDYN related dynamic allocation errors that are associated with the internal reader for job submission. The return code is specific to BPXWDYN. The reason code is always zero.</td>
<td>&quot;Category 1 — dynamic allocation error&quot;</td>
</tr>
<tr>
<td>VSAM API</td>
<td>3</td>
<td>Errors produced or detected by the Java/ JNI/ C/ HLASM/ VSAM layer.</td>
<td>&quot;Category 3 — VSAM API error&quot; on page 206</td>
</tr>
<tr>
<td>VSAM System</td>
<td>4</td>
<td>Errors produced or detected by VSAM. The return code and reason code are VSAM specific.</td>
<td>&quot;Category 4 — VSAM system error&quot; on page 206</td>
</tr>
<tr>
<td>VSAM ABEND</td>
<td>5</td>
<td>ABEND information resulting from VSAM failures.</td>
<td>&quot;Category 5 — VSAM ABEND error&quot; on page 206</td>
</tr>
<tr>
<td>Service</td>
<td>6</td>
<td>Errors produced or detected in the service layer.</td>
<td>&quot;Category 6 — service error&quot; on page 206</td>
</tr>
<tr>
<td>Unexpected</td>
<td>7</td>
<td>Unexpected errors detected.</td>
<td>&quot;Category 7 — Unexpected error&quot; on page 208</td>
</tr>
<tr>
<td>SSI</td>
<td>8</td>
<td>Errors produced or detected by the extended status function call of the MVS subsystem interface (SSI Function Code 80).</td>
<td>&quot;Category 8 — SSI error&quot; on page 208</td>
</tr>
<tr>
<td>CIM</td>
<td>9</td>
<td>Errors produced or detected by the CIM interface.</td>
<td>&quot;Category 9 — CIM error&quot; on page 209</td>
</tr>
</tbody>
</table>

**Category 1 — dynamic allocation error**

Table 37 shows the possible conditions for this error category.

<table>
<thead>
<tr>
<th>rc</th>
<th>reason</th>
<th>message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
<td>0</td>
<td>Error allocating internal reader, BPXWDYN rc=%d</td>
<td>The internal routine BPXWDYN failed while attempting to allocate the internal reader. For the meaning of return code n, see the error codes for BPXWDYN in z/OS Using REXX and z/OS UNIX System Services, SA22-7806.</td>
</tr>
</tbody>
</table>
### Category 3 — VSAM API error

Table 38 shows the possible conditions for this error category.

<table>
<thead>
<tr>
<th>rc</th>
<th>reason</th>
<th>message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>2</td>
<td>VSAM file is not open</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>Record length ( %d \geq \text{lrecl} %d )</td>
<td>Writing a record to a VSAM file failed because an incorrect record length was specified.</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>Could not write JCL to internal reader</td>
<td>An I/O exception occurred when writing JCL to the internal reader.</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>JesVsam get failed</td>
<td>Buffer too small to hold the VSAM record.</td>
</tr>
<tr>
<td>255</td>
<td>0</td>
<td>JesVsam native buffer malloc failed</td>
<td></td>
</tr>
</tbody>
</table>

### Category 4 — VSAM system error

Table 39 shows the possible conditions for this error category.

<table>
<thead>
<tr>
<th>rc</th>
<th>reason</th>
<th>message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(n)</td>
<td>(m)</td>
<td>varies</td>
<td>For descriptions of the specific return and reason codes, see the VSAM publications.</td>
</tr>
</tbody>
</table>

### Category 5 — VSAM ABEND error

Table 40 shows the possible conditions for this error category.

<table>
<thead>
<tr>
<th>rc</th>
<th>reason</th>
<th>message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(n)</td>
<td>(m)</td>
<td>varies</td>
<td>The values (n) and (m) indicate the ABEND return code and reason code.</td>
</tr>
</tbody>
</table>

### Category 6 — service error

Table 41 shows the possible conditions for this error category.

<table>
<thead>
<tr>
<th>rc</th>
<th>reason</th>
<th>message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>1</td>
<td>Incorrect Internal Reader mode: (%s) Must be one of TEXT</td>
<td>Request header Intrdr-Mode specified a value that is not valid. Valid values are TEXT, BINARY, or RECORD.</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Incorrect Internal Reader parameters: (%s). Fixed records are required for binary mode</td>
<td>The internal reader characteristics form a combination that is not valid. If you specify the value BINARY for the Intrdr-Mode request header, you must specify the value F for the Intrdr-Recfm request header.</td>
</tr>
</tbody>
</table>
Table 41. Category 6 errors (continued)

<table>
<thead>
<tr>
<th>rc</th>
<th>reason</th>
<th>message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>3</td>
<td>Request does not contain '%s' content</td>
<td>Job update requests must have a content type of application/json.</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>Value of %s query parameter is not valid</td>
<td>The query parameter identified in the message either contains incorrect characters or exceeds the allowable length. In the message, the query parameter is owner, prefix, or jobid.</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>Update request is not 'cancel'</td>
<td>The job update request value for the &quot;request&quot; property is not valid. The value must be &quot;cancel&quot;.</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>Request does not contain a valid job update request</td>
<td>The job update request input document does not specify a valid property. The valid properties are: &quot;request&quot; &quot;class&quot;</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>No match for method %s and pathInfo='%s'</td>
<td>The supplied servlet pathinfo does not match any expected string for the HTTP method that was specified.</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>POST requests not supported</td>
<td>For standard REST requests, the POST HTTP method is not allowed. To avoid this message, include the Requested-Method header to have the request sent through the POST verb.</td>
</tr>
<tr>
<td>4</td>
<td>9</td>
<td>Job submission error. Record length %d too long for JCL submission</td>
<td>The check for record mode job submission failed.</td>
</tr>
<tr>
<td>4</td>
<td>10</td>
<td>No job found for reference: '%s'</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>11</td>
<td>Record range '%s' is not valid for spool file record request</td>
<td>Request header Record-Range specified a value that is not valid. The content range value must be of the form: SSS-EEE where SSS and EEE are relative offsets and identify the first and last records to be read. When EEE is 0, the GET request reads to the end of the file.</td>
</tr>
<tr>
<td>4</td>
<td>12</td>
<td>Job '%s' does not contain spool file id %d</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>13</td>
<td>Job input was not recognized by system as a job</td>
<td>The job was submitted without a job statement or with unrecognized (non-JCL) content.</td>
</tr>
<tr>
<td>4</td>
<td>20</td>
<td>Service not implemented: %s</td>
<td>The request service has not been implemented. The variable text %s contains additional information.</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>Unable to query information about submitted job: %s</td>
<td>The job status for the submitted job could not be obtained within the timeout period (3 seconds).</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>EOF encountered before all requested bytes read</td>
<td>Internal read state error. The expected number of bytes were not available to be read before EOF</td>
</tr>
</tbody>
</table>
### Table 41. Category 6 errors (continued)

<table>
<thead>
<tr>
<th>rc</th>
<th>reason</th>
<th>message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>3</td>
<td>Range start is beyond end of spool file <code>%d</code> for job <code>%s</code></td>
<td>During a request to get a range of records for a spool file, the Record-Range header specified a record start value that is beyond the end of the spool file.</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>Cannot advance spool file more than <code>Integer.MAX_VALUE</code>. DD= <code>%s</code></td>
<td>During a request to get a range of records for a spool file, the Record-Range header specified a record start value greater than <code>2**31-1</code>.</td>
</tr>
<tr>
<td>12</td>
<td>1</td>
<td>Not authorized to access spool file</td>
<td>An authorization check failed trying to OPEN the requested spool file.</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>Not authorized to submit job</td>
<td>Failed an authorization check when attempting to open the internal reader to submit a job.</td>
</tr>
<tr>
<td>12</td>
<td>3</td>
<td>User not authorized to issue a CIM request</td>
<td>CIM detected an authentication or authorization failure during the request. To cancel a job, change a job class, or purge a job, the user must be authorized to use the CIM server and be permitted to the JES2-JES3Jobs CIM provider. CIM provides jobs (CFZSEC and CFZRCUST) to help you configure the CIM server, including security authorizations and file system customization. See the chapter on CIM server quick setup and verification in <a href="https://pic.dhe.com/psp/zos/pdfs/cic/zos_common_information_model_user_guide.pdf">z/OS Common Information Model User’s Guide SC33-7998</a>.</td>
</tr>
</tbody>
</table>

### Category 7 — Unexpected error

Table 42 shows the possible conditions for this error category.

### Table 42. Category 7 errors

<table>
<thead>
<tr>
<th>rc</th>
<th>reason</th>
<th>message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>1</td>
<td>Server error occurred</td>
<td>For details about the exception, see the stack property of the JSON ErrorReport document, which is described in <a href="https://pic.dhe.com/psp/zos/pdfs/cic/zos_common_information_model_user_guide.pdf">“ErrorReport document” on page 204</a>.</td>
</tr>
</tbody>
</table>

### Category 8 — SSI error

Table 43 shows the possible conditions for this error category.

### Table 43. Category 8 errors

<table>
<thead>
<tr>
<th>rc</th>
<th>reason</th>
<th>message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
<td>m</td>
<td>varies</td>
<td>The rc and reason (n,m) are set from the return code of the extended status function call of the MVS subsystem interface (SSI Function Code 80) and the subsystem options block (SSOB) return code, respectively. The details property of the JSON ErrorReport document contains a message with more information. See <a href="https://pic.dhe.com/psp/zos/pdfs/cic/zos_common_information_model_user_guide.pdf">“ErrorReport document” on page 204</a>.</td>
</tr>
</tbody>
</table>
## Category 9 — CIM error

Table 44 shows the possible conditions for this error category.

<table>
<thead>
<tr>
<th>rc</th>
<th>reason</th>
<th>message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>2</td>
<td>Incorrect jobname: &quot;%s&quot;</td>
<td>Prior to the CIM service call, the job name was found to be null or an empty string.</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>Incorrect jobid: &quot;%s&quot;</td>
<td>Prior to the CIM service call, the job ID was found to be null or an empty string.</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>Incorrect JES type</td>
<td>Prior to the CIM service call, an incorrect JES type (not JES2 or JES3) was detected.</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>Incorrect job class: &quot;%s&quot;</td>
<td>Prior to the CIM service call, the job class was found to be null or an empty string.</td>
</tr>
<tr>
<td>8</td>
<td>—</td>
<td>varies</td>
<td>CIM internal error. An error occurred during setup or invocation of the CIM service.</td>
</tr>
<tr>
<td>12</td>
<td>m</td>
<td>Error returned from CIM job {Cancel</td>
<td>Request Property Change} service</td>
</tr>
<tr>
<td>16</td>
<td>—</td>
<td>CIM connection failure</td>
<td>A connection exception was encountered while processing a request to cancel a job, change job class, or purge a job. This error can occur during periods of concurrent high usage of these interfaces. Most of the time, the reason for the failure is a simple connection refused due to overload of the server. The application should try the request again. The number of retry attempts needed depends on how much work is being requested of the server.</td>
</tr>
</tbody>
</table>
Chapter 13. Using the Application Linking Manager interface services

The Application Linking Manager task of z/OSMF includes an application programming interface (API), which is implemented through industry standard Representational State Transfer (REST) services. This interface allows a client application to define new event types, to list the registered handlers for an event type, and to register new handlers for an event type.

You can use a variety of tools to issue these HTTP requests; the examples in this section use cURL, which is a command-line application that runs in the z/OS UNIX System Services environment. For more information about cURL, see "https://www.ibm.com/systems/z/os/zos/features/unix/ported/suptlk/index.html".

Processing overview

The Application Linking Manager interface services can be invoked by any HTTP client application, running on the z/OS local system or a remote system.

Your program (the client) initiates an HTTP request to the Application Linking Manager interface. If the interface determines that the request is valid, it performs the requested service. After performing the service, the Application Linking Manager interface creates an HTTP response. If the request is successful, this response takes the form of an HTTP 200 (OK) response and, if applicable, an object containing a result set, which it passes back to your program. Results are returned in the form of a JSON object, which must be parsed by your program. If the request is not successful, the response consists of a non-OK HTTP response code and a JSON object.

Resource URLs

The URLs of the Application Linking Manager interface have the format shown in Figure 52:

```
https://{host}:{port}/zosmf/izual/rest/{resource}?{parm}
```

*Figure 52. Format of resource URLs for Application Linking Manager interface.*

where:

- "https://{host}:{port}" specifies the target system address and port
- "/zosmf/izual/rest" identifies the Application Linking Manager interface
- "{resource}?{parm}" represents the resource, such as an event type, and optionally one or more parameters, to qualify the request.

HTTP methods

The Application Linking Manager interface provides the following HTTP methods:

**POST**

Sends a registration request for an event type or handler.
GET
Retrieves a list of registered handlers for an event type.

DELETE
Unregisters an event type or handler.

Supported HTTP versions

The Application Linking Manager interface supports requests in either of the following protocols: HTTP/1.0 or HTTP/1.1.

Content types

The JSON content type ("Content-Type: application/json") is used for sent data and returned data; for the detailed format of each returned object, see the JSON object description for each operation.

Error handling

For errors that occur during the processing of a request, the Application Linking Manager interface returns an appropriate HTTP status code to the calling client. An error is indicated by a 4\textit{nn} code or a 5\textit{nn} code. Some errors might also include a returned JSON object that contains a message that describes the error.

The following HTTP status codes are valid:

"HTTP/1.1 200 OK"
Success.

"HTTP/1.1 400 Bad Request"
Request contained incorrect parameters.

"HTTP/1.1 401 Unauthorized"
Submitter of the request did not authenticate to z/OSMF or is not authorized to the Application Linking Manager task.

"HTTP/1.1 404 Bad URL"
Target of the request (a URL) was not found.

"HTTP/1.1 500 Internal server error"
Programming error.

Error logging

Errors from the Application Linking Manager interface services are logged in the WebSphere log or the z/OSMF log. You can use this information to diagnose the problem or provide it to IBM Support, if required.

Required authorizations

To submit requests through the Application Linking Manager interface services, your user ID requires authorization to the Application Linking Manager task, as follows:

- If your installation is operating z/OSMF in SAF Authorization Mode, your user ID requires READ access to the following resource profile in the ZMFAPLA class: <SAF-prefix>.ZOSMF.ADMINTASKS.APPLINKING
- If your installation is operating z/OSMF in Repository Authorization Mode, your user ID must be assigned to a role that can perform the Application Linking Manager task.
By default, the z/OSMF administrator user ID is authorized to the Application Linking Manager interface services.

Further, if you plan to use the Application Linking Manager interface services to list the registered event handlers for an event type, your user ID requires authorization to the WebSphere SAF profile prefix on the target z/OS system, as follows:

- READ access to `<WebSphere-SAF-profile-prefix>` in the APPL class.
- READ access to the `<WebSphere-SAF-profile-prefix>.izuUsers` profile in the EJBROLE class.

By default, the WebSphere SAF profile prefix is BBNBASE.

**Usage considerations**

Observe the following considerations when using the Application Linking Manager interface services:

- The Application Linking Manager interface services run as unauthorized programs on z/OS.
- Some browsing environments do not support all of the HTTP methods, such as HTML 4 or XHTML 1, or might block applications from accessing response content having non-successful HTTP response status codes (4nn and 5nn). As a workaround, your application can use the following custom HTTP request headers:

  **Requested-Method:**
  GET and DELETE requests can be "tunneled" through a POST method using this custom HTTP header.

  **Bypass-Status:**
  If set to true, all response status codes are set to 200, and the custom HTTP response header `Actual-Status` is included in the returned data. To determine the original status code, your application must check the `Actual-Status` header.

**Invoking a z/OSMF application link externally**

It is possible for an external application (a web application, for example, or a desktop application), to launch a z/OSMF event on a z/OS system. Here, the application issues a command comprised of the URL for the local instance of z/OSMF, combined with the appropriate event information.

The following is an example of such a request. In the example, `eventType-1` identifies the event type and `value-1` specifies the parameter input for the event handler.

```
https://...:9443/zosmf/?izual.eventType=<eventType-1>&parm1=<value-1>
```

This command launches z/OSMF in a new browser window on the issuer's system, and sends the event to z/OSMF after session startup. If the user is authenticated to z/OSMF, the handler is launched in the user's session. Otherwise, the user is prompted to authenticate before the handler can be launched.
How this chapter is organized

Table 45. Operations provided through the Application Linking Manager interface services.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Method</th>
<th>Where described</th>
</tr>
</thead>
<tbody>
<tr>
<td>Register an event type</td>
<td>POST</td>
<td>“POST method: Register an event type” on page 215</td>
</tr>
<tr>
<td>Register a handler for an event</td>
<td>POST</td>
<td>“POST method: Register an event handler” on page 218</td>
</tr>
<tr>
<td>type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>List the already-registered</td>
<td>GET</td>
<td>“GET method: Obtain a list of handlers for an</td>
</tr>
<tr>
<td>handlers for an event type</td>
<td></td>
<td>event type” on page 221</td>
</tr>
<tr>
<td>Unregister a handler</td>
<td>DELETE</td>
<td>“DELETE method: Unregister an event handler” on page 222</td>
</tr>
<tr>
<td>Unregister an event type</td>
<td>DELETE</td>
<td>“DELETE method: Unregister an event type” on page 223</td>
</tr>
</tbody>
</table>
POST method: Register an event type

You can use the POST method to define a new event type to z/OSMF.

URL format

The following figure shows the URL format for this request.

https://{host}:{port}/zosmf/izual/rest/eventtype

Standard headers

Use the following standard HTTP header with this request:

Content-Type: application/json

Custom headers

None.

Request content

Your request must include a JSON object that describes the event type to be registered, for example:

```
{
  id: "IBM.ZOSMF.EVENT_TYPE_ID",
  displayName: "Default English name",
  desc: "Default English description",
  owner: "ownerId",
  params: {"key1": "English description of the param"}
}
```

Figure 53. Registering an event type: request content

The following values are supported:

id Specify a unique identifier for the event type. It can contain up to 50 characters, including alphanumeric characters (A-Z, a-z, and 0-9), periods (.), and underscores (_). The event ID is required and must be unique.

displayName Specify the name of the event type. The name is required and can contain up to 50 characters.

desc Specify a description of the event type. The description is optional and can contain up to 200 characters.

owner Specify the ID of the first z/OSMF task or external application that registered the event type. Typically, event types are registered by or on behalf of event handlers. They can also be registered by or on behalf of event requestors. This field is required, and can contain up to 50 characters, including alphanumeric characters (A-Z, a-z, and 0-9), periods (.), and underscores (_).

params Specify the name and description of the parameters that event requestors
can supply with an event. Enter each parameter name and description combination on a separate line, and use a comma to separate the parameter name and description.

This area can contain up to 4,000 characters, including alphanumeric characters (A-Z, a-z, and 0-9), periods (.), underscores (_), and commas (,).

Required authorizations

See "Required authorizations" on page 212.

IBM-supplied event types

As shipped, z/OSMF comes the following event types pre-registered:

- Event type IBM.ZOSMF.CONFIGURE_NETWORK_POLICIES, which has the following attributes:

  id: IBM.ZOSMF.CONFIGURE_NETWORK_POLICIES
displayName: Configure network policies
desc: Used to configure z/OS Communications Server network policies
owner: IBM
params:
  <No parameters>

- Event type IBM.ZOSMF.VIEW_DATASET, which has the following attributes:

  id: IBM.ZOSMF.VIEW_DATASET
displayName: View DataSet
desc: Event for viewing a data set
owner: ISPF
params:
  name: dataSetName
description: The name of the data set

- Event type IBM.ZOSMF.VIEW_JOB_STATUS, which has the following attributes:

  id: IBM.ZOSMF.VIEW_JOB_STATUS
displayName: View Job Status
desc: Event for viewing the status of a job
owner: ISPF
params:
  Name: jobName
  Description: The name of the job to display the status for
  Name: jobId
  Description: The ID of the job to display the status for

Example of registering an event type

A sample request using the cURL command line application is shown in Figure 54 on page 217.
Expected response

On completion, the Application Linking Manager interface returns an HTTP response, which includes a status code indicating whether your request completed. Status code 200 indicates success. A status code of 4nn or 5nn indicates that an error has occurred. See "Error handling" on page 212.

The response also includes a JSON object with additional information about the results of the request. If your request is successful, the JSON object contains null data for the error and result fields, as shown in Figure 55.

```
{"error":null,"result":null}
```

Figure 55. Example: Returned results of a successful event registration

For an unsuccessful request, the JSON object contains an error message in the error fields, msgid and msgtext. The example in Figure 56 shows the results for an attempt to register an already-registered event with different parameters:

```
{
  "error":{
    "msgid":"IZUG690E",
    "msgtxt":"Event type "IBM.ZOSMF.VIEW_JOB_STATUS" is already defined, but different parameters are specified."
  },
  "result":null
}
```

Figure 56. Example: Returned results of an unsuccessful event registration
**POST method: Register an event handler**

You can use the POST method to define a new event handler to z/OSMF.

**URL format**

The following figure shows the URL format for this request.

```plaintext
https://{host}:{port}/zosmf/izual/rest/handler?eventTypeId=<eventTypeId>
```

where `<eventTypeId>` is the event type to be associated with a new handler.

**Standard headers**

Use the following standard HTTP header with this request:

*Content-Type: application/json*

**Custom headers**

None.

**Request content**

Your request must include a JSON object that describes the event handler to be registered.

The following values are supported:

- **type**
  For the handler type, specify `INTERNAL` for a z/OSMF task or `EXTERNAL` for an external application. If you specify `INTERNAL`, you must also specify values for `applID` and `taskID`.

- **id**
  For the z/OSMF task ID, enter the ID assigned to the z/OSMF task. The ID is required, and can contain up to 50 characters, including alphanumeric characters (A-Z, a-z, and 0-9), periods (.), and underscores (_).

- **applID**
  If type is set to `INTERNAL`, you must specify a value for `applID`. The valid value is `com.ibm.zoszmf.ispf`. If type is set to `EXTERNAL`, omit this value.

- **taskID**
  If type is set to `INTERNAL`, you must specify a value for `taskID`. The valid value is `ISPF`. If type is set to `EXTERNAL`, omit this value.

- **displayName**
  For the handler name, specify the name of the handler task or application. The name is required and can contain up to 50 characters.

- **URL**
  For the handler URL, specify the URL to be used for accessing the handler. The URL can contain up to 4,000 characters, including alphanumeric characters (A-Z, a-z, 0-9), blanks, mathematical symbols (+ - = | ~ ( ) [ ] \), punctuation marks (? ! ; : ’ “ / [ ] ), and the following special characters: %, $, #, @, ^, *, and _. The URL is required and must be URI-encoded as specified in RFC 2396. For more information about RFC 2396, see the Uniform Resource Identifiers (URI): Generic Syntax Web page.
options

The CONTEXT_SUPPORT option indicates what the handler will display when it processes events of this type. Specify either of the following values for CONTEXT_SUPPORT:

OPT_CONTEXT_SUPPORT_NONE
Handler is launched without context in a separate browser window and displays its homepage. When re-launched, the handler receives focus. This option is selected by default.

OPT_CONTEXT_SUPPORT_LAUNCH
Handler is launched with context in a separate browser window. When re-launched, the handler receives focus, but the context is not updated.

Required authorizations

See “Required authorizations” on page 212.

Expected response

On completion, the Application Linking Manager interface returns an HTTP response, which includes a status code indicating whether your request completed. Status code 200 indicates success. A status code of 4nn or 5nn indicates that an error has occurred. See “Error handling” on page 212.

IBM-supplied event handler registrations

As shipped, z/OSMF comes the following event handler registrations:

• Event handler Configuration Assistant, which has the following attributes:

  Event type ID: IBM.ZOSMF.CONFIGURE_NETWORK_POLICIES
  z/OSMF plug-in ID: CAV1R11
  z/OSMF task ID: Configuration Assistant
  Handler ID: CAV1R13_Configuration_Assistant
  Handler name: Configuration Assistant
  URL: /zosmf/ipsecgui/ca
  Handler type: z/OSMF task
  Enabled: Yes
  Launch context support: Launch without context

• Event handler ISPF Browse, which has the following attributes:

  Event type ID: IBM.ZOSMF.VIEW_DATASET
  z/OSMF plug-in ID: com.ibm.zoszmf.ispf
  z/OSMF task ID: ISPF
  Handler ID: IBM.ZOSMF.VIEW_DATASET_HANDLER
  Handler name: ISPF Browse
  URL: /zosmf/webispf/index.jsp?cmd=ISPSTART%20CMD
  (%25ISREPDF%20%24dataSetName%20%20)&%20ONEWAPPL(ISR)
  Handler type: z/OSMF task
  Enabled: Yes
  Launch context support: Launch with context and switch
Example of registering the SDSF ISPF application as an event handler

Assume that you want to register the SDSF application that is accessed through the z/OSMF ISPF task as an event handler for SDSF Job Status (event type IBM.ZOSMF.VIEW_JOB_STATUS). Your application would issue this request using the following format:

https://{host}:{port}/zosmf/izual/rest/handler?eventTypeId=IBM.ZOSMF.VIEW_JOB_STATUS ID?{JSON object}

where IBM.ZOSMF.VIEW_JOB_STATUS identifies the SDSF job status event, which causes the event handler to be invoked.

A sample request using the cURL command line application is shown in Figure 57:

curl -k --user zosmfad:zosmfad2 -H "Content-Type: application/json" -X POST -d '{"type": "INTERNAL", "openIn": "ZOSMF", "id": "com.ibm.zoszmf.ispf.ISPF.SDSF", "appId": "com.ibm.zoszmf.ispf", "taskId": "ISPF", "displayName": "SDSF","url": "https://{host}:{port}/zosmf/webispf?command="SELECT PSPM(ISFISP) PARM(ST FILTER(JOBNAME EQ $jobname JOBID EQ $jobid) FILTERMODE(AND) NP(S))""}" https://{host}:{port}/zosmf/izual/rest/handler?eventTypeId=IBM.ZOSMF.VIEW_JOB_STATUS | iconv -f ISO8859-1 -t IBM-1047

Figure 57. Example: Registering an event handler
GET method: Obtain a list of handlers for an event type

You can use the GET method to obtain a list of registered handlers for an event type.

**URL format**

The following figure shows the URL format for this request.

```
https://{host}:{port}/zosmf/izual/rest/handler?eventTypeId=<eventTypeId>
```

where `<eventTypeId>` is the event type to be queried for registered handlers.

**Standard headers**

Use the following standard HTTP header with this request:

```
Content-Type: application/json
```

**Custom headers**

None.

**Request content**

None.

**Required authorizations**

See "Required authorizations" on page 212.

**Expected response**

On completion, the Application Linking Manager interface returns an HTTP response, which includes a status code indicating whether your request completed. Status code 200 indicates success. A status code of 4nn or 5nn indicates that an error has occurred. See "Error handling" on page 212.

The response also includes a JSON object with additional information about the results of the request. If your request is successful, the JSON object contains null data for the error and result fields, as shown in Figure 58.

```
{"error":null,"result":null}
```

*Figure 58. Example: Returned results of a successful list handlers request*

For an unsuccessful request, the JSON object contains an error message in the error fields, `msgid` and `msgtext`. 
DELETE method: Unregister an event handler

You can use the DELETE method to remove an existing event handler registration from z/OSMF.

URL format

The following figure shows the URL format for this request.

```
https://{host}:{port}/zosmf/izual/rest/handler/<handlerId>?eventTypeId=<eventTypeId>
```

where the combination of `<handlerId>` and `<eventTypeId>` identifies the handler registration to be removed.

Standard headers

None.

Custom headers

None.

Request content

None.

Required authorizations

See "Required authorizations" on page 212.

Expected response

On completion, the Application Linking Manager interface returns an HTTP response, which includes a status code indicating whether your request completed. Status code 200 indicates success. A status code of 4nn or 5nn indicates that an error has occurred. See "Error handling" on page 212.
DELETE method: Unregister an event type

You can use the DELETE method to remove the definition of an event type from z/OSMF.

URL format

The following figure shows the URL format for this request.

https://{host}:{port}/zosmf/izual/rest/eventtype/<eventTypeId>

where <eventTypeId> identifies the event type to be removed.

Standard headers

None.

Custom headers

None.

Request content

None.

Required authorizations

See “Required authorizations” on page 212.

Expected response

On completion, the Application Linking Manager interface returns an HTTP response, which includes a status code indicating whether your request completed. Status code 200 indicates success. A status code of 4nn or 5nn indicates that an error has occurred. See “Error handling” on page 212.
Part 5. Appendixes
Appendix A. Default security setup for z/OSMF

This section describes the default security environment for z/OSMF. Included are the RACF profiles, resources names, and group assignments that are created when your installation uses the REXX execs that are supplied with z/OSMF.

Profiles, resource names, and group assignments

For your reference, Table 46 on page 228 shows the relationship of profiles, resource names, and group assignments for z/OSMF running in SAF Authorization Mode, which is the default authorization mode for z/OSMF.

As shown in Table 46 on page 228 resource profiles in z/OSMF are qualified by the WebSphere SAF profile prefix, which is shown as <SAF-prefix> in Table 46 on page 228. By default, the profile prefix is BBNBASE.

Note: This table is formatted in landscape view to improve usability when you print copies of these pages. To adjust the view in Adobe Reader, select View > Rotate View > Clockwise.
<table>
<thead>
<tr>
<th>Resource profile</th>
<th>Resource name</th>
<th>Protects</th>
<th>Permitted groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;SAF-prefix&gt;.ZOSMF.CAPACITY_PROVISIONING.**</td>
<td>ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.getView</td>
<td>Capacity Provisioning task</td>
<td>IZUADMIN, IZUUSER</td>
</tr>
<tr>
<td>&lt;SAF-prefix&gt;.ZOSMF.CONFIGURATION_ASSISTANT.**</td>
<td>ZOSMF.CONFIGURATION_ASSISTANT.CONFIGURATION_ASSISTANT</td>
<td>Configuration Assistant task</td>
<td>IZUADMIN, IZUUSER</td>
</tr>
<tr>
<td>&lt;SAF-prefix&gt;.ZOSMF.SOFTWARE_DEPLOYMENT.**</td>
<td>ZOSMF.SOFTWARE_DEPLOYMENT.** ZOSMF.SOFTWARE_DEPLOYMENT.DATA.**</td>
<td>Deployment task</td>
<td>IZUADMIN, IZUUSER</td>
</tr>
<tr>
<td>&lt;SAF-prefix&gt;.ZOSMF.INCIDENT_LOG.**</td>
<td>ZOSMF.INCIDENT_LOG.INCIDENT_LOG</td>
<td>Incident Log task</td>
<td>IZUADMIN, IZUUSER</td>
</tr>
<tr>
<td>&lt;SAF-prefix&gt;.ZOSMF.ISPF.**</td>
<td>ZOSMF.ISPF.ISPF</td>
<td>ISPF task</td>
<td>IZUADMIN, IZUUSER</td>
</tr>
<tr>
<td>&lt;SAF-prefix&gt;.ZOSMF.RESOURCE_MONITORING.**</td>
<td>ZOSMF.RESOURCE_MONITORING.PERFDESKS ZOSMF.RESOURCE_MONITORING.OVERVIEW</td>
<td>Resource Monitoring task System Status task</td>
<td>IZUADMIN, IZUUSER</td>
</tr>
<tr>
<td>&lt;SAF-prefix&gt;.ZOSMF.WORKLOAD_MANAGEMENT.**</td>
<td>ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT_VIEW ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.MODIFY ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.INSTALL</td>
<td>Workload Management View Workload Management Modify Workload Management Install</td>
<td>IZUADMIN</td>
</tr>
<tr>
<td>&lt;SAF-prefix&gt;.ZOSMF.LINK.**</td>
<td>ZOSMF.LINKS.SHOPZSERIES ZOSMF.LINKS.SUPPORT_FOR_Z_0S ZOSMF.LINKS.WSC_FLASHES_TECHDOCS ZOSMF.LINKS.Z_0S_BASICS_INFORMATION_CENTER ZOSMF.LINKS.Z_0S_HOME_PAGE ZOSMF.LINKS.Z_0S_INTERNET_LIBRARY</td>
<td>Links</td>
<td>IZUADMIN, IZUUSER</td>
</tr>
<tr>
<td>&lt;SAF-prefix&gt;.ZOSMF.ADMINTASKS.**</td>
<td>ZOSMF.ADMINTASKS.UI_LOG_MANAGEMENT ZOSMF.ADMINTASKS.APPLINKING ZOSMF.ADMINTASKS.LINKSTASK ZOSMF.ADMINTASKS.LOGGER</td>
<td>z/OSMF Administration tasks</td>
<td>IZUADMIN</td>
</tr>
</tbody>
</table>
Common event adapter (CEA) security profiles

The common event adapter (CEA) component of z/OS has security profiles for protecting different portions of its processing. The RACF command exec created by the z/OSMF configuration process (see "Step 2: Run the security commands" on page 69) provides CEA group access to CEA.CEAPDWB* in the SERVAUTH class. Table 47 shows the profiles that are included in this group.

<table>
<thead>
<tr>
<th>Security Profile</th>
<th>Corresponding CEA function</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEA.CEADOCMD</td>
<td>Cancel job. Used by Incident Log FTP processing.</td>
</tr>
<tr>
<td>CEA.CEADOCONSOLECMD *</td>
<td>Allow the IVP to issue operator commands to accomplish its function.</td>
</tr>
<tr>
<td>CEA.CEAGETPS</td>
<td>Obtain job information. Used by Incident Log FTP processing.</td>
</tr>
<tr>
<td>CEA.CEAPDWB.CEACHECKSTATUS</td>
<td>Check status and return incident information.</td>
</tr>
<tr>
<td>CEA.CEAPDWB.CEADELETEINCIDENT</td>
<td>Delete selected incidents, including the dumps, all diagnostic snapshot files and the corresponding sysplex dump directory entry.</td>
</tr>
<tr>
<td>CEA.CEAPDWB.CEAGETINCIDENT</td>
<td>Obtain data associated with a specific incident.</td>
</tr>
<tr>
<td>CEA.CEAPDWB.CEAGETINCIDENTCOLLECTION</td>
<td>Obtain collection of incident data for all incidents matching a filter.</td>
</tr>
<tr>
<td>CEA.CEAPDWB.CEAPREPAREINCIDENT</td>
<td>Prepare data for FTP (locate and compress/terse).</td>
</tr>
<tr>
<td>CEA.CEAPDWB.CEASETINCIDENTINFO</td>
<td>Set information associated with the incident, such as the Notes® field.</td>
</tr>
<tr>
<td>CEA.CEAPDWB.CEASETPROBLEMTRACKINGNUMBER</td>
<td>Set a problem ID (such as a PMR number) or problem management tracking ID.</td>
</tr>
<tr>
<td>CEA.CEAPDWB.CEAUNSUPPRESSDUMP</td>
<td>Allow a dump that has been marked for suppression through DAE to be taken.</td>
</tr>
<tr>
<td>CEA.CEATSO.CEATSOREQUEST</td>
<td>Allow a TSO user access to the CEATSOREQUEST API so that the user’s sessions can be managed through the ISPF task of z/OSMF.</td>
</tr>
</tbody>
</table>
Appendix B. z/OS system setup for the Incident Log task

Enabling your z/OS system for the Incident Log task requires some initial setup work on the z/OS host system. Information for performing this work is provided in the sections that follow, beginning with an overview of the system components that play a role in support of problem data management at your installation.

System components used by the Incident Log task

As shown in Figure 59, a number of base z/OS functions are involved when the Incident Log task is used to manage diagnostic data for your system.

Specifically, z/OSMF and the Incident Log task interact with z/OS system functions in the following ways:

- Common Information Model (CIM) server for handling requests made by z/OSMF
- SDUMP component for managing the capture of OPERLOG, SYSLOG, and logrec snapshots
- IPCS dump directory services for managing the inventory of dumps related to incidents
- System Logger to capture log snapshots when sysplex-scope recording is requested through the OPERLOG or logrec system logger streams
- Dump analysis and elimination (DAE) for enabling the “take next dump” feature of the Incident Log task
- Environmental Record Editing and Printing (EREP) program for formatting the logrec data
- Common Event Adapter (CEA) for providing the data that is subsequently displayed in the Incident Log task user interface.
CEA helps to coordinate these system functions on behalf of z/OSMF incidents, in single system and sysplex environments.

Similar to other z/OS components, the CEA address space has the following attributes:

- Is started automatically during z/OS system initialization
- Supports a set of operator commands for interaction, such as MODIFY CEA
- Issues WTO messages (prefixed with CEA)
- Supports an abend code for handling incorrect actions (100)
- Requires security profile setup (through the CEA resource profile)
- Supports a variety of reason codes to indicate errors in CEA processing. Reason codes that might appear during z/OSMF operations are listed in Appendix H, “Common event adapter (CEA) reason codes,” on page 269.

The role of CEA in z/OSMF processing can be summarized, as follows:

- When CEA becomes active, it establishes an association with your installation’s sysplex dump directory (typically SYS1.DDIR), which contains the inventory of SVC dumps taken in your sysplex, plus relevant information about each dump incident. This processing is done for SVC dumps taken on behalf of system abends, as well as those taken through the DUMP command and SLIP traps.
- Whenever an SVC dump is written to a data set, the DUMPSRV address space (on behalf of SVC dump processing) creates a new entry in the sysplex dump directory and informs CEA that the new incident has arrived. Then, CEA attempts to capture log snapshots, as follows:
  - If the system hardcopy log is recorded to the OPERLOG log stream, CEA directs the system logger component to create the log snapshot in a DASD log stream for the specified time duration. If the hardcopy is written to SYSLOG (that is, a single system scope), CEA uses spool allocation interfaces to access the SYSLOG data set and obtain the required snapshot, which is written to a DASD data set.
  - Similarly, if the logrec stream is written to a system logger log stream, CEA directs system logger to create a log snapshot of logrec data for the specified time period. If logrec is written to a data set, CEA invokes EREP to create the log snapshot.
  - Associates the snapshots with the corresponding incidents, based on snapshot data set name.
- When you use the Incident Log task to display incidents, CEA is invoked through the CIM server and uses IPCS functions to read the sysplex dump directory to obtain the inventory of SVC dumps taken on your system. CEA then extracts information from all relevant entries and returns it to z/OSMF for display. Similarly, when you use the Incident Log task to display details about an incident, z/OSMF receives those details from CEA, which obtains the information from the sysplex dump directory.
- When you request z/OSMF to send all or selected diagnostic materials to the specified URL, CEA is invoked to prepare the data, with different options, depending on whether you plan to use standard FTP or the z/OS Problem Documentation Upload Utility (PDUU). Here, all binary log data is formatted before being sent to the target system.
- In some instances, CEA performs its processing using System REXX execs, which are invoked through the AXREXX function.

As a result of this processing, your z/OS incidents are managed reliably on the system closest to the source of the information.
System customization needed for the Incident Log task

Table 2 on page 25 summarizes the z/OS system changes that are required or recommended for enabling the Incident Log task. Much of this work might already be done on your system, or might not be applicable. If so, you can skip the particular setup action. Other setup actions might require modifications to an existing setting, for example, if your installation has already defined a couple data set for the system logger component, you might need to increase the space allocation for system logger log stream records.

The setup actions are described in more detail in the sections that follow:

- “Defining a couple data set for system logger”
- “Enabling the operations log (OPERLOG)” on page 235
- “Defining and activating the LOGREC log stream” on page 237
- “Defining diagnostic snapshot log streams” on page 239
- “Enabling SYSLOG for diagnostic snapshots” on page 240
- “Configuring automatic dump data set allocation” on page 241
- “Configuring dump analysis and elimination” on page 242
- “Creating the sysplex dump directory” on page 243
- “Ensuring that CEA is active” on page 245
- “Ensuring that System REXX is set up and active” on page 247
- “Ensuring that dump data set names are correct” on page 248
- “Authorizing the SYS1.MIGLIB data set” on page 249

---

Defining a couple data set for system logger

The Incident Log task requires that a couple data set be defined for the system logger component of z/OS to represent the diagnostic log snapshots. If your installation has not already defined the system logger data set, this topic describes the steps for doing so.

How to check if this step is done

To display LOGR couple data sets on a system, enter the following command:

```bash
d xcf,couple,type=LOGR
```

Figure 60 on page 234 shows the expected results:
If this step is not already done

Define or update the system logger couple data set (LOGR CDS) with a large enough log stream records (LSR) value to allow sufficient space for managing the DASD-only log streams that will be created for capturing diagnostic log snapshots. The LSR value must be large enough to allow for two snapshot log streams for each dump recorded in z/OSMF, plus two model log streams, which are used as templates for defining the storage attributes for the snapshots. For information about modifying and reformatting a couple data set, see z/OS MVS Setting Up a Sysplex, SA22-7625.

System logger supports shared sysplex-scope (coupling facility resident) log streams and single-system DASD-only log streams, as follows:

- Coupling facility (CF) log streams are sysplex-wide in scope; any system in the sysplex can write to these log streams.
- DASD-only log streams can be written to by the local system only. When a DASD-only log stream is closed, it can be read from other systems in the sysplex if it resides on DASD that is shared by the other systems in the sysplex.

The system creates DASD-only log streams for the operations log (OPERLOG) and the sysplex logrec diagnostic snapshots. You do not need to predefine the DASD-only log streams. For the model used, see sample job CEASNPLG, which is supplied by IBM in SYS1.SAMPLIB(CEASNPLG).

Use shared DASD as the target for OPERLOG and logrec snapshots, so that the Incident Log task can access the log snapshots from any system in the sysplex.

In planning the space requirements for your system logger couple data set, plan for two DASD-only log streams per incident. To allow up to 100 incidents, for example, you must allow enough space for 200 log streams.

IBM recommends that you allow space for up to 1000 DASD-only log streams (or 500 incidents). To do so, use the IXCL1DSU format utility, for example:

```
//FMTLCDS JOB MSGLEVEL=(1,1)
// EXEC PGM=IXCL1DSU
// * $ SUBMIT, JOB=LOGGER.Z0S17.JCL(FORMAT17)
```
If the system logger couple data set lacks sufficient space to contain the diagnostic snapshots, the system issues message CEA0600I to indicate that the log streams could not be created.

To allow the Incident Log task to access diagnostic log snapshots on other systems in the sysplex, the log streams must reside on shared DASD. DASD-only log streams are expected to be written to SMS-managed DASD.

**Related information**

For more information, see [z/OS MVS Setting Up a Sysplex](http://www.ibm.com/library/ibmx/SA22-7625) SA22-7625, which explains the following concepts:

- DASD-only log streams
- Setting up an SMS environment for DASD data sets
- Adding the data sets to the GRSRNL inclusion list
- Managing system logger log stream data sets
- Defining authorization.

---

**Enabling the operations log (OPERLOG)**

The operations log (OPERLOG) is a sysplex-wide log of system messages (WTOs) residing in a system logger log stream, comparable to SYSLOG, which is a single system message log residing on JES spool.

If OPERLOG is enabled on your system, z/OSMF can use OPERLOG to collect message data on a sysplex wide basis. Here, OPERLOG must be active in a system logger log stream. For the steps to follow, see “Steps for setting up OPERLOG” on page 236.

If you choose to defer this step, z/OSMF collects message data on a single system basis, using the system log (SYSLOG) as the source.

**How to check if this step is done**

To display the active medium where messages are recorded, enter the following command:

```
d c,nc
```

Figure 61 on page 236 shows the expected results:
Steps for setting up OPERLOG

The following instructions are a summary of the details found in IBM Redbook System Programmer’s Guide to: z/OS System Logger, which is available from http://www.redbooks.ibm.com/. For more information about setting up OPERLOG, see the topic on preparing to use system logger applications in z/OS MVS Setting Up a Sysplex, SA22-7625.

Before you begin

You must define the logger subsystem.

Procedure

1. Define the hardcopy device as OPERLOG in the HARDCOPY statement of the CONSOLxx parmlib member. You can change this setting using the command V OPERLOG,HARDCPY. To deactivate OPERLOG, you can use the command V OPERLOG,HARDCPY,OFF.

2. Define the corresponding coupling facility structure in the CFRM policy. For example:

```
//OPERLOG JOB CLASS=A,MSGCLASS=A
//POLICY EXEC PGM=IXCMIAPU
//SYSPRINT DD SYSOUT=A
//SYSIN DD *
DATA TYPE(CFRM)
STRUCTURE NAME(OPERLOG)
SIZE(40448)
INITSIZE(40448)
PREFLIST(FACIL01,FACIL02)
```

3. Activate the CFRM policy through the command START,POLICY,TYPE=CFRM,POLNAME=polname, or through the COUPLExx parmlib member.

4. Define the log stream to the LOGR policy. The following example is for illustrative purposes only; follow the recommendations in z/OS MVS Setting Up a Sysplex and z/OS MVS Programming: Assembler Services Guide.

```
//OPERLOG JOB CLASS=A,MSGCLASS=A
//POLICY EXEC PGM=IXCMIAPU
//SYSPRINT DD SYSOUT=A
//SYSIN DD *
DATA TYPE(LOGR)
DEFINE STRUCTURE NAME(OPERLOG)
LOGSNUM(1)
MAXBUFSIZE(4092)
AVGBUFSIZE(512)
```
DEFINE LOGSTREAM NAME(SYSPLEX.OPERLOG)
STRUCTNAME(OPERLOG)
LS_DATACLAS(LOGR4K)
HLQ(IXGLOGR)
LS_SIZE(1024)
LOWOFFLOAD(0)
HIGHOFFLOAD(80)
STG_DUPLEX(NO)
RETPD(30)
AUTODELETE(No)

5. Create the security definitions for RACF (or an equivalent security product). In the following example, the SYSPLEX.OPERLOG of the LOGSTRM resource CLASS is given READ permission, which allows all users to browse the operations log and userid1 has UPDATE access level, which allows userid1 to delete records from the log stream. That is, the user ID associated with the job running the IEAMDBLG program. For example:

RDEFINE LOGSTRM SYSPLEX.OPERLOG UACC(READ)
PERMIT SYSPLEX.OPERLOG CLASS(LOGSTRM) ID(userid1)
ACCESS(UPDATE) SETROPTS CLASSACT(LOGSTRM)

This example is for illustrative purposes only. Follow the guidelines for your installation.

6. After you activate OPERLOG, you must manage the way in which records are handled.

SYS1.SAMPLIB contains a sample program, IEAMDBLG, to read log blocks from the OPERLOG log stream and convert them to SYSLOG format. The program is an example of how to use the services of the system logger component to retrieve and delete records from the OPERLOG log stream. It reads the records created in a given time span, converts them from message data block (MDB) format to hardcopy log format (HCL or JES2 SYSLOG), and writes the SYSLOG-format records to a file. It also has an option to delete from the log stream the records created before a given date.

When you use the delete option, you might want to first copy the records on alternate media and then conditionally delete the records in a separate JCL step to ensure that you have a copy of the data before deleting. If you do not run them on two separate conditional steps, deletion occurs simultaneously with copy without any guarantee that the copy process was successful.

For more information, see the topic on managing log data in z/OS MVS Setting Up a Sysplex SA22-7625.

Results

To verify the completion of this work, enter the command DISPLAY CONSOLES,HARDCOPY to display OPERLOG status.

Defining and activating the LOGREC log stream

Logrec is the z/OS error log. It contains binary data describing error records that are written on behalf of system abends and other system recording requests. Logrec data is formatted through the batch utility EREP. The single-system version usually resides in a data set named SYS1.LOGREC or &SYSNAME.LOGREC. The sysplex version resides in a system logger log stream (the LOGREC log stream).
If the LOGREC log stream is active on your system, z/OSMF uses this log stream to collect logrec data on a sysplex wide basis. For information about defining and activating the LOGREC log stream, see “Steps for setting up the LOGREC log stream.”

If you choose to defer this step, z/OSMF collects logrec data on a single system basis, using the logrec data set as the source.

**How to check if this step is done**

To display the active medium for collecting logrec data, enter the following command:

```plaintext
D LOGREC
```

Figure 62 shows the expected results:

```
IFB090I 15.22.12 LOGREC DISPLAY 062
CURRENT MEDIUM = DATASET
 MEDIUM NAME = SYS1.P02.LOGREC
```

*Figure 62. Expected results from the D LOGREC operator command*

If the medium is DATASET, the logrec data is recorded using a data set. If the medium is LOGSTREAM, the logrec data is recorded in a LOGR logstream.

**Steps for setting up the LOGREC log stream**

The following instructions are a summary of the details found in *IBM Redbook System Programmer’s Guide to: z/OS System Logger*, which is available from [http://www.redbooks.ibm.com/](http://www.redbooks.ibm.com/) For more information about defining the log stream, see the topic on preparing to use system logger applications in [z/OS MVS Setting Up a Sysplex](http://www.redbooks.ibm.com/) SA22-7625.

**Before you begin**

You must define the logger subsystem.

**Procedure**

1. IPL each system using its own logrec data set specified in the IEASYxx parmlib member. Then, switch to using the log stream through the SETLOGRC command. This process allows your installation to fall back to using the data set if needed. To use the log stream immediately from the IPL, specify LOGREC=LOGSTREAM in IEASYxx, as follows:

   IEASYxx with logrec data set:
   - LOGCLS=L,
   - LOGLMT=010000,
   - LOGREC=SYS1.&SYSNAME..LOGREC, or LOGREC=LOGSTREAM,
   - MAXUSER=128,
   - MLPA=80

2. Define the LOGREC log stream structure definition in the CFRM policy. For example:

   ```plaintext
   //LOGREC JOB CLASS=A,MSGCLASS=A
   //POLICY EXEC PGM=IXCMIAPU
   //SYSIN DD SYSOUT=A
   //SYSIN DD *
   DATA TYPE(CFRM)
   ```
3. Define the system logger policy. For example:

```
//DEFINE EXEC PGM=IXCMIAPU
//SYSPRINT DD SYSOUT=A
//SYSIN DD *
DATA TYPE (LOGR)
DEFINE STRUCTURE NAME(LOGREC)
LOGSNUM(1)
AVGBUFSIZE(4068)
MAXBUFSIZE(4068)
DEFINE LOGSTREAM NAME(SYSPLEX.LOGREC.ALLRECS)
STRUCTNAME(LOGREC)
LS_DATACLAS(LOGR4K)
HLQ(IXGLOGR)
LS_SIZE(1024)
LOWOFFLOAD(0)
HIGHOFFLOAD(80)
STG_DUPLEX(NO)
RETPD(0)
AUTODELETE(NO)
```

4. Change the logrec recording medium:

```
SETLOGRC {LOGSTREAM|DATASET|IGNORE}
```

5. Create the required security definitions. For example:

```
RDEFINE LOGSTRM SYSPLEX.LOGREC.ALLRECS UACC(READ)
SETROPTS CLASSACT(LOGSTRM)
```

### Results

To verify the completion of this work, enter the command `DISPLAY LOGREC` to display the current logrec error recording medium.

---

**Defining diagnostic snapshot log streams**

For optimal performance of the Incident Log task, it is recommended that your installation define operations log (OPERLOG) and logrec log streams for the CEA component of z/OS. Doing so allows the system logger component to determine the storage characteristics for storing diagnostic snapshots.

### How to check if this step is done

To display the OPERLOG logstream, enter the following command:

```
D LOGGER,L,LSN=SYSPLEX.OPERLOG
```

[Figure 63 on page 240](#) shows the expected results:
If this step is not already done

To create the log streams, you can use a batch job like sample job CEASNPLG, which is supplied by IBM in SYS1.SAMPLIB(CEASNPLG). The CEASNPLG job deletes and redefines CEA diagnostic snapshot model log streams, using the IBM utility program, IXCMIAPU.

For information about the IXCMIAPU utility, see z/OS MVS Setting Up a Sysplex, SA22-7625.

Enabling SYSLOG for diagnostic snapshots

If your installation collects messages about programs and system functions (the hardcopy message set) on a single system basis, the Incident Log task uses the system log (SYSLOG) as the source for diagnostic log snapshots. This function requires one of the following minimum levels of JES on your system: JES2 V1R11 or JES3 V1R11 (with the PTF for APAR OA29534).

Here, you must ensure that the proper security permissions exist, so that the JES subsystem can access SYSLOG on behalf of the common event adapter (CEA) component of z/OS. For example, in a system with RACF as the security management product, your security administrator can issue RACF commands like those shown in Figure 64.

```
RDEFINE JESSPOOL SY1.+MASTER+.SYSLOG.*.* UACC(NONE)
PERMIT SY1.+MASTER+.SYSLOG.*.* CLASS(JESSPOOL) ID(CEA_userid) ACC(ALTER)
SETROPTS RACLST(JESSPOOL) REFRESH
```

Figure 64. RACF commands to enable CEA to access SYSLOG

where CEA_userid is the user ID that you use to access CEA.

Your installation might not have defined JESSPOOL under RACF authority; if so, your setting for the SETROPTS command will be different.

For more information about RACF commands, see z/OS Security Server RACF Command Language Reference.
Configuring automatic dump data set allocation

For full functionality, the Incident Log task requires that automatic dump data set allocation (auto-dump) be active on the z/OS host system. If your installation has not already set up auto-dump, this topic describes the steps for doing so. If you choose to defer this step, the Incident Log task runs with limited functionality.

If your installation uses automatic dump data set allocation, the Incident Log task uses the resulting dump data set names in the “Send Data” action, which allows your installation to transmit this data to a remote destination through FTP.

To set up automatic dump data set allocation, do the following:

1. Define the dump data set naming convention to be used by the system. Specify it using the “DUMPDS NAME=” command, for example:
   $sysplex..DUMP.D&date..T&time..&SYSNAME..&S&seq

2. Determine where the dumps are to be stored. It is recommended that you use an SMS storage class or a shared DASD volume for dumps. Examples:

   DUMPDS ADD,SMS=class
   DUMPDS ADD,VOL=(volser,volser,volser,..)

   If you use a shared volume, ensure that the volume is managed through a shared catalog for the sysplex. Otherwise, for an incident with multi-system dumps, when deleting the incident, only the primary dump is deleted because the remote dumps are not accessible.

3. Start the function through the following command:

   DUMPDS ALLOC=ACTIVE

For more details, see the following information:

- Topic on the DUMPDS command in z/OS MVS System Commands, SA22-7627
- Topic on SVC dump in z/OS MVS Diagnosis: Tools and Service Aids, GA22-7589.

If your installation does not use automatic dump data set allocation, it is likely that you have defined pre-allocated dump data sets (SYS1.DUMPxx) for the system to use. Typically, an installation archives an SVC dump to another data set as soon as the dump is complete, to avoid having the system overlay the data set with a subsequent dump. The archive data set name is defined by the installation and is not known to the system. If so, the following limitations result:

- Incident Log records identify the pre-allocated dumps. Thus, the same property information is shown for each incident.
- Send Data action does not locate the dump data set because the name is unknown to the Incident Log task. The system, however, continues to process the log snapshots.

To continue using pre-allocated dump data sets, your installation can use an IBM-supplied JCL step to rename the dump data set in the sysplex dump directory, to allow z/OSMF to locate the correct data set. For information, see “Ensuring that dump data set names are correct” on page 248.

Some installations use automatic dump data set allocation, but then, subsequently, copy the dump data sets to another volume (to preserve space in the SMS DASD set). If the copied data set has the same name as the original dump data set, and the data set is cataloged, the Incident Log “Send data” action will locate the copied dump data sets. However, if the copied dump data set has a different name, use
the IBM-supplied JCL step to rename the dump data set in the sysplex dump directory so that the Incident Log task will locate it.

**Configuring dump analysis and elimination**

The Incident Log task requires that dump analysis and elimination (DAE) be active on the z/OS host system to avoid capturing duplicate problems in the Incident Log task display. If your installation has not already configured DAE, this topic summarizes the steps for doing so.

IBM recommends that you enable DAE to suppress SVC dumps with duplicate symptoms. This action ensures that the Incident Log task displays only the initial instance of a dump-related incident. If necessary, you can use the *allow next dump* option of the Incident Log task to allow the system to take and report the next dump that occurs for the same symptoms. You might use this option, for example, after you apply a fix for the problem. The Allow Next Dump option allows you to collect diagnostic data for the next new occurrence of the same problem.

IBM also recommends that you enable DAE to manage symptoms for a sysplex-wide collection of symptoms, rather than for a single system only.

For information about how to set up DAE, see [z/OS MVS Diagnosis: Tools and Service Aids](#).

To configure DAE processing, you use the following IBM-supplied members, which are provided in SYS1.PARMLIB:

- ADYSET00 to turn on DAE with single system scope
- ADYSET01 to turn off DAE with single system scope
- ADYSET02 is a copy of ADYSET00.

For more information about the IBM-supplied ADYSETxx parmlib members, see [z/OS MVS Initialization and Tuning Reference](#).

The steps for configuring DAE for Incident Log processing are summarized, as follows:

1. To ensure that duplicate SVC dumps are suppressed, verify that SUPPRESSALL is specified on the SVCDUMP parameter in the ADYSET00 member.
2. To have DAE use a sysplex-wide scope, edit the ADYSET00 and ADTSET01 members, as follows.
   - Edit the ADYSET00 member to include the settings SHARE, DSN and GLOBAL. For example:

   ```
   DAE=START,RECORDS(400),
   SVCDUMP(MATCH,SUPPRESSALL,UPDATE,NOTIFY(3,30)),
   SYSMDUMP(MATCH,UPDATE),
   SHARE(DSN,OPTIONS),DSN(SYS1.DAESH2) GLOBAL(DSN,OPTIONS)
   ```
   - Edit the ADYSET01 member to include the setting GLOBALSTOP. For example:

   ```
   DAE=STOP,GLOBALSTOP
   ```
Creating the sysplex dump directory

The sysplex dump directory is a shared VSAM data set that contains information about SVC dumps that have been taken on each of the systems in the sysplex. As each SVC dump is written to a data set, an entry is added by the dumping services address space (DUMPSRV) to the sysplex dump directory to store information like dump data set name, dump title, and symptom string.

The Incident Log task uses the sysplex dump directory as the repository for information about incidents that have occurred in the sysplex. If your installation has not already created a sysplex dump directory, this topic describes the steps for doing so.

Steps for creating the sysplex dump directory

To enable the Incident Log, your installation requires a sysplex dump directory data set (SYS1.DDIR or an installation-supplied name) with 15,000 records, which is about 60 cylinders. Approximately 50 directory entries are used for each incident and more are used for multi-system dumps.

To allow the Incident Log task (running on one system in the sysplex) to deliver a sysplex view of SVC dumps that are taken, select a DASD volume with shared access to all of the systems in the sysplex (or all systems that you want the Incident Log task to represent).

To create the sysplex dump directory, follow these steps:

1. Run the BLSCDDIR CLIST, which resides in system data set SYS1.SBLSCLI0(BLSCDDIR). For example:

   EXEC 'SYS1.SBLSCLI0(BLSCDDIR)'
   'DSNAME(SYS1.DDIR) VOLUME(volser) RECORDS(15000)'

   This CLIST creates SYS1.DDIR as a VSAM data set with SHAREOPTIONS(1,3).

2. Update BLSCUSER with the dump directory name.

3. Recycle DUMPSRV so that the dump directory name is registered to this address space. To do so, enter the command CANCEL DUMPSRV. The DUMPSRV address space restarts automatically.

4. Start BLSJPRMI through the command START BLSJPRMI. This action registers the dump directory name to IPCS.

The name of the sysplex dump directory needs to be established before you perform any requests for incident information, and needs to be cataloged on the current system and any other (backup) system running the CIM server, to allow access by the Incident Log task.

For more information about using the BLSCDDIR CLIST, see z/OS MVS IPCS User's Guide.
Considerations for using a sysplex dump directory

When using a sysplex dump directory, observe the following considerations:

- The sysplex dump directory (SYS1.DDIR, by default) is a shared VSAM data set serialized with an exclusive ENQ on the data set. This ENQ is used only by
  - DUMPSRV address space, when writing an entry to the directory for a new SVC dump
  - CEA address space, when reading or updating the dump directory for Incident Log requests.
- The sysplex dump directory is different from the IPCS user local dump directory. A local directory is created for each IPCS user to store detailed data related to the IPCS session. The sysplex dump directory is used only to save name and symptom data for all SVC dumps taken, and must not be used as an IPCS user local dump directory.
- **Do not access the sysplex dump directory from an IPCS user.** Instead, use a batch job to access the directory.
- If new entries are not being added to the Incident Log task, or if z/OSMF requests are not being satisfied, check for contention on the sysplex dump directory through the D GRS command. Verify that no IPCS user is accessing the sysplex dump directory.

Establishing a larger sysplex dump directory

Over time, your sysplex dump directory might become full with the dumps you have saved. To create more space for dumps, you can delete old dumps from the directory. If you must retain the saved dumps, however, you can instead migrate your existing dumps to a larger sysplex dump directory.

To establish a larger sysplex dump directory, follow these steps:

1. Create a new sysplex dump directory data set through the BLSCDDIR CLIST, for example:

   ```
   EXEC 'SYS1.SBLSCLI0(BLSCDDIR)' 'DSNAME(new.DDIR) VOLUME(volser) RECORDS(25000)
   ```

   If your existing dump directory was created with the default size of 15000 records, you might want to specify a larger size. Approximately 50 directory entries are used for each incident and more are used for multi-system dumps.

2. Use the IPCS COPYDDIR command to copy the old directory entries to the new directory data set, as follows:

   ```
   COPYDDIR INDSNAME(SYS1.DDIR) DSNAME(new.DDIR)
   ```

3. Update BLSCUSER with the new dump directory name (but make note of the old dump directory name).

4. Recycle the DUMPSRV address space (CANCEL DUMPSRV; it restarts automatically). This action registers the new dump directory name to DUMPSRV.

5. Run BLSJPRMI (START BLSJPRMI). This action updates the in-storage copy of the dump directory name.

Your new sysplex dump directory now contains the old dumps and can be used to store new dumps.
Ensuring that CEA is active

The Incident Log task and the ISPF task of z/OSMF require that the common event adapter (CEA) component be active on your z/OS system. CEA provides the ability to deliver z/OS events to clients, such as the CIM server, and create or manage TSO user address spaces under the ISPF task. Usually, the CEA address space is started automatically during z/OS initialization. If your installation has stopped CEA, it is recommended that you restart it. Otherwise, the Incident Log task and the ISPF task are not operational.

z/OSMF requires that CEA runs in full function mode on your system. In this mode, both internal z/OS components and clients such as CIM providers can use CEA indication functions.

For information about how to configure CEA, see z/OS Planning for Installation, GA22-7504.

The common event adapter (CEA) component of z/OS has security profiles for protecting different portions of its processing. For example, users of the Incident Log task require access to the CEA.CEAPDWB* profile in the SERVAUTH class. For the profiles related to CEA, see Table 47 on page 229.

Also, if your installation plans to use the ISPF task, you must ensure that the TRUSTED attribute is assigned to the CEA started task, as described in “Assigning the TRUSTED attribute to CEA” on page 28.

How to check if CEA is active

To determine whether the CEA address space is active, enter the following command:

```
D A,CEA
```

Figure 65 shows the expected results:

```
IEE115I 15.32.17 2010.132 ACTIVITY 109
JOBS M/S TS USERS SYSS AS INITS ACTIVE/MA MAX VTAM OAS
00018 00040 00002 00043 00246 00002/03500 00043
CEA CEA IEFPROC NSWPR=0 A=001A PER=YES SMC=000
PGN=N/A DMN=N/A AFF=NONE
CT=000.426S ET=45.32.29
WKL=S YSTEM SCL=SYSTEM P=1
RGP=N/A SRVR=NO QSC=NO
ADDR SPACE ASTE=05A34680
DSPNAME=CEACTDSP ASTE=1002D600
DSPNAME=CEAPDWB ASTE=1002D580
DSPNAME=CEACADS ASTE=7EF42700
DSPNAME=CEACOMP ASTE=1002D480
```

Figure 65. Expected results from the D A,CEA operator command

Starting the CEA address space

To start the CEA address space, enter the following command from the operator console: START CEA

It is recommended that you edit your active IEASYSxx parmlib member to identify the CEAPRMxx parmlib member to be used for the next IPL of the system. Specify
the CEAPRMxx member suffix on the CEA=xx statement of IEASYSxx. The
member specified in IEASYSxx will be in effect after the next system IPL.

To dynamically change the active CEA configuration, enter the MODIFY command,
as follows: F CEA,CEA=xx, where xx is the suffix of the CEAPRMxx member to be
used.

You can specify multiple CEAPRMxx members, for example:

F CEA,CEA=(01,02,03)

To check the resulting CEA configuration, enter the following command:

F CEA,D,PARMS

**Identifying the CEAPRMxx member to use at IPL time**

To ensure that common event adapter (CEA) is always active and using the correct
settings, it is recommended that you edit your active IEASYSxx parmlib member to
identify the CEAPRMxx parmlib member to use for the next IPL of the system.
Specify the CEAPRMxx member suffix on the CEA=xx statement of IEASYSxx.

**Modifying the common event adapter (CEA) settings**

At any time during z/OSMF operations, you can modify CEA settings by selecting
a new CEAPRMxx member. You can do so dynamically, that is, without having to
restart CEA.

You might want to update the CEA settings to do the following:

- Add an eighth volume to CEA. Earlier, during the configuration prompts, if you
  provided VOLSER values to be used in the target CEAPRMxx member, you
  specified up to seven volumes as input. If you want to add an eighth volume,
  for example, to allow more space for diagnostic snapshots, you can update the
  CEAPRMxx member manually.
- Adjust the duration of OPERLOG or logrec that the system should capture for
  all future incidents.

If needed, you can restart CEA and specify a new CEAPRMxx member
dynamically. To do so, enter the START command, as follows: START CEA. Then,
enter the MODIFY command, as follows:

F CEA,CEA=xx

where xx represents the CEAPRMxx member suffix.

You can specify multiple CEAPRMxx members, for example: F CEA,CEA=(01,02,03)

To check the results of these commands, enter the MODIFY command, as follows:

F CEA,D,PARMS

For information about how to configure CEA, see [z/OS Planning for Installation](GA22-7504).
Ensuring that System REXX is set up and active

For full functionality, the Incident Log task requires that the System REXX (SYSREXX) component be set-up and active on your z/OS system.

This topic contains the following information:
- “Ensuring that System REXX is set-up properly”
- “Ensuring that System REXX is active”
  - “How to check if this step is done”
- “Starting the SYSREXX address space” on page 248

Ensuring that System REXX is set-up properly

Observe the following considerations regarding System REXX set-up:
- Ensure that you have an AXRnn JCL member in PROCLIB, similar to the AXRnn member in SYS1.IBM.PROCLIB.
- If you have an AXRnn member in SYS1.IBM.PROCLIB, ensure that SYS1.IBM.PROCLIB is in the MSTJCLxx IEFPDSI DD concatenation.
- Ensure that the user ID specified for AXRUSER in AXRnn has the correct permissions.

For more information about setting up System REXX, see the following documents:
- z/OS MVS Authorized Assembler Services Guide, SA22-7608
- z/OS MVS Initialization and Tuning Reference, SA22-7592.

Ensuring that System REXX is active

SYSREXX is started automatically during IPL. If your installation has stopped SYSREXX, it is recommended that you restart it.

If you choose to defer this step, the Incident Log task runs with limited functionality. Also, the installation verification program (IVP) described in “Step 5: Complete the setup” on page 75 fails any tests that require an active SYSREXX component.

How to check if this step is done

If the AXR address space is active on the z/OS system, the System REXX component is active. To determine whether the AXR address space is active, enter the following command:

```bash
D A,AXR
```

Figure 66 on page 248 shows the expected results:
Starting the SYSREXX address space

To start the SYSREXX component, enter the following command from the operator console:

```
START AXRPSTRT
```

For information about configuring System REXX on your system, see the jobs described in z/OS Program Directory.

Ensuring that dump data set names are correct

If your installation has an automation program that copies an SVC dump data set to a different location using a different data set name, you must ensure that the dump data set name is changed accordingly in the sysplex dump directory. This action is necessary to allow the Incident Log task to locate the correct dump.

In your automation program, add a step to rename the dump data set in the sysplex dump directory; Figure 67 provides an example of the JCL you can use.

```
//IPCS EXEC PGM=IKJEFT01,DYNAMNBR=20,REGION=1500K
//IPCSDDIR DD DSN=SYS1.DDIR,DISP=(SHR)
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPRT DD SYSOUT=* 
//SYSTSPR
Authorizing the SYS1.MIGLIB data set

SYS1.MIGLIB must be APF-authorized to allow AMATERSE to be called by System REXX execs, which are authorized.

How to check if this step is done

To determine whether SYS1.MIGLIB is APF-authorized, enter the following command:

D PROG,APF,DSNAME=SYS1.MIGLIB

Figure 68 shows the expected results:

```plaintext
CSV450I 15.37.25 PROG,APF DISPLAY 123
FORMAT=DYNAMIC
ENTRY VOLUME DSNAME
  1 D83ELC SYS1.MIGLIB
```

Figure 68. Expected results from the D PROG operator command

How to APF-authorize SYS1.MIGLIB

To APF-authorize SYS1.MIGLIB, enter the following command:

SETPROG APF,ADD,DSNAME=SYS1.MIGLIB,VOLUME=xxxxx

where xxxxx is the volume serial (VOLSER).
Appendix C. izusetup.sh script

z/OSMF provides a front end interactive script, called izusetup.sh, that you use to configure the product on your z/OS system. This script, when invoked with a number of different options, sets up and deploys a working instance of the product in your z/OS system. After the configuration is created, you can use this script to add more plug-ins or links to the configured instance of z/OSMF.

You can run this script from an OMVS or telnet/rlogin session. You cannot run this script from ISHELL.

**Format**

```
izusetup.sh -file izuconfig1.cfg -config
[-overridefile <filename>.ovr] [-fastpath] [-add]
izusetup.sh -file izuconfig1.cfg -verify [all|core|log|racf]
izusetup.sh -file izuconfig1.cfg -prime [-add]
izusetup.sh -file izuconfig1.cfg -finish [-add]
izusetup.sh -file izuconfig1.cfg -service
izusetup.sh -file izuconfig1.cfg -addlink <pathname>/<link-properties-filename>
```

*Figure 69. izusetup.sh syntax*

**Required parameters**

Always include the -file parameter, which specifies the name of the configuration file that the izusetup.sh script is to use as input.

You must also specify one of the following parameters, which identify the particular operation that the izusetup.sh script is to perform. You cannot specify more than one of these operations on the same invocation.

- **-config**
  
  This parameter indicates that you want to create a REXX exec with sample RACF commands for setting up security. The script also creates and mounts the z/OSMF data file system if it does not already exist.

- **-finish**
  
  This parameter indicates that you want to complete the configuration of the z/OSMF.

- **-prime**
  
  This parameter indicates that you want to initialize the z/OSMF data file system.

- **-verify**
  
  This parameter indicates that you want to verify the configuration of z/OSMF. To indicate the scope of this verification, specify -verify with one of the following options:

  - **racf**
    
    Verify the RACF security setup for all configured tasks and functions.
core Verify the system setup for the core functions only.

log Verify the system setup for the Incident Log task only, as listed in Table 2 on page 25.

all Verify the system setup for all configured tasks and functions. all is the default.

-service
This parameter indicates that you want to apply the service from a PTF to your z/OSMF configuration. For information, see “Updating plug-ins after service is applied” on page 127.

-addlink
This parameter indicates that you want to add a link to the z/OSMF navigation area. Use this option only at the direction of your vendor. For information, see “Adding links through the izusetup.sh script” on page 131.

Optional parameters

You can specify one of the following optional parameters with a required parameter.

-add
This parameter indicates that you want to add plug-ins to an already configured instance of z/OSMF. Specify the -add option with the existing options -config, -prime, and -finish to limit the scope of these operations to new plug-ins only.

You can specify which plug-ins are to be added in your override file, which you specify on the optional -overridefile option. In the override file, mark the plug-ins to be added with the character A. If you omit the override file, the script prompts you to specify which plug-ins are to be added.

When specified with the optional -fastpath parameter, the script runs without any interactive prompting. Instead, the script uses the values from the configuration file and the override file, if specified. Omitted values will cause the script to end with errors.

For more information, see “Updating plug-ins after service is applied” on page 127.

-fastpath
This optional parameter indicates that you want to use the variable values that are specified in the configuration file, the override file, or a combination of both files. When you specify this parameter, during the configuration process, you are not prompted for new values for the variables.

You must ensure that any variables specified in the override file are set to valid values for your installation. Some variables are initially set to the following value, which is not a valid setting: NO.DEFAULT.VALUE.

For more information, see “Choosing a script mode: Interactive or fastpath” on page 34.

-overridefile overridefilename
This optional parameter indicates that you want to use the variable values that are specified in the override file. For overridefilename, specify the name of the override file that the izusetup.sh script is to use as input.
The override file takes precedence over the same values specified in the configuration file. For any configuration values not found in either of these files, the script prompts you for valid values.

For more information, see “Using an override file” on page 34.

Examples

In the following example, the izusetup.sh script begins the configuration process for z/OSMF. Your input values will be saved in the configuration file izuconfig1.cfg.

```
izusetup.sh -file izuconfig1.cfg -config
```

The script locates the configuration file (izuconfig1.cfg) in the directory specified on the IZU_CONFIG_DIR configuration variable. By default, this is /etc/zosmf.

In the following example, the izusetup.sh script runs the configuration process for any new plug-ins to be added. Because the optional parameter -fastpath is omitted, the script will run in interactive mode, prompting you for which plug-ins are to be configured and for related setup information.

```
izusetup.sh -file izuconfig1.cfg -config -add
```
Appendix D. Default configuration file and default override file

A default configuration file, called izudflt.cfg, and a default override file, called izudflt.ovr, are provided with z/OSMF. You can use these files to provide your input to the izusetup.sh script.

The contents of these files are shown in the following sections:
- “Default configuration file”
- “Default override file” on page 258.

Default configuration file

The default configuration file, izudflt.cfg, contains the variables and associated default values that the izusetup.sh script uses to configure your z/OSMF instance. This file is located in the <IZU_CODE_ROOT>/defaults directory.

Table 48. Default configuration file

<table>
<thead>
<tr>
<th>Variable name</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IZU_CONFIG_FILE_VERSION</td>
<td>1.13.0</td>
<td>Version number, which identifies the format of this configuration file.</td>
</tr>
<tr>
<td>IZU_DATA_DIR</td>
<td>/var/zosmf/data</td>
<td>Mount point (the fully-qualified path name) for the z/OSMF data file system.</td>
</tr>
<tr>
<td>IZU_DATA_FS_NAME</td>
<td>IZU.SIZUDATA</td>
<td>z/OSMF data file system.</td>
</tr>
<tr>
<td>IZU_DATA_FS_TYPE</td>
<td>ZFS</td>
<td>Type of file system (ZFS or HFS) to be used for creating the z/OSMF data file system.</td>
</tr>
<tr>
<td>IZU_DATA_FS_VOLUME</td>
<td>*</td>
<td>Volume serial number (VOLSER) of the DASD to be used for creating the z/OSMF data file system, or * to let SMS select a volume.</td>
</tr>
<tr>
<td>IZU_DATA_FS_SIZE</td>
<td>200</td>
<td>Initial space allocation, in cylinders, for the z/OSMF data file system data set. The script uses 90% of this value for the primary allocation and 10% for the secondary allocation.</td>
</tr>
<tr>
<td>IZU_AUTHORIZATION_MODE</td>
<td>SAF</td>
<td>Authorization mode to be used for this z/OSMF configuration: SAF or REPOSITORY. This value must be entered in uppercase characters. The valid modes are: SAF mode. Security is based entirely on profiles and groups defined in your security product. SAF mode is the default. REPOSITORY mode. Security is based on the user and role selections defined in z/OSMF.</td>
</tr>
<tr>
<td>IZU_AUTOUID_OVERRIDE</td>
<td>NO.DEFAULT.VALUE</td>
<td>If you have AUTOUID enabled, this variable indicates whether (Y or N) RACF is to assign unused UIDs for your group IDs.</td>
</tr>
<tr>
<td>IZU_AUTOGID_OVERRIDE</td>
<td>NO.DEFAULT.VALUE</td>
<td>If you have AUTOGID enabled, this variable indicates whether (Y or N) RACF is to assign unused GIDs for your group IDs.</td>
</tr>
</tbody>
</table>
Table 48. Default configuration file (continued)

<table>
<thead>
<tr>
<th>Variable name</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IZU_ADMIN_GROUP_NAME</td>
<td>IZUADMIN</td>
<td>Primary group for z/OSMF administrator role.</td>
</tr>
<tr>
<td>IZU_ADMIN_GROUP_GID</td>
<td>9003</td>
<td>Group ID (GID) for the z/OSMF administrator group.</td>
</tr>
<tr>
<td>IZU_USERS_GROUP_NAME</td>
<td>IZUUSER</td>
<td>Primary group for z/OSMF users.</td>
</tr>
<tr>
<td>IZU_USERS_GROUP_GID</td>
<td>9004</td>
<td>Group ID (GID) for the z/OSMF user group.</td>
</tr>
<tr>
<td>IZU_ADMIN_NAME</td>
<td>ZOSMFAD</td>
<td>User ID for the z/OSMF administrator.</td>
</tr>
<tr>
<td>IZU_ADMIN_UID</td>
<td>9001</td>
<td>UID for the z/OSMF administrator.</td>
</tr>
<tr>
<td>IZU_ADMIN_HOME</td>
<td>/u/zosmfad</td>
<td>Home directory for the z/OSMF administrator. Do not specify a home directory to be created under the mount point of the z/OSMF data file system, which by default is /var/zosmf/data. The mount point owner and group permissions do not allow the z/OSMF administrator ID access.</td>
</tr>
<tr>
<td>IZU_ADMIN_PROGRAM</td>
<td>/bin/sh</td>
<td>Program path for the z/OSMF administrator identity for z/OS UNIX system services.</td>
</tr>
<tr>
<td>IZU_ADMIN_PROC</td>
<td>NO.DEFAULT.VALUE</td>
<td>TSO/E logon procedure to be used by the z/OSMF administrator.</td>
</tr>
<tr>
<td>IZU_ADMIN_ACCOUNT</td>
<td>NO.DEFAULT.VALUE</td>
<td>User account number for z/OSMF administrator identity.</td>
</tr>
<tr>
<td>IZU_WAS_CONFIG_FILE_KNOWN</td>
<td>Y</td>
<td>The WebSphere Application Server response file, which was created when you configured IBM WebSphere Application Server OEM Edition for z/OS on this system, exists and is available to be used as input to the IBM z/OS Management Facility process. This file is described in IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide, GA32-0631.</td>
</tr>
<tr>
<td>IZU_WAS_CONFIG_FILE_LOCATION</td>
<td>/etc/zWebSphereOEM/V7R0/conf/CONFIG1/CONFIG1.responseFile</td>
<td>Fully-qualified path name of the WebSphere Application Server response file. Your installation created this file when customizing IBM WebSphere Application Server OEM Edition for z/OS for this system.</td>
</tr>
<tr>
<td>IZU_APPSERVER_GROUP</td>
<td>WSCFG1</td>
<td>WebSphere application server group.</td>
</tr>
<tr>
<td>IZU_APPSERVER_ROOT</td>
<td>/zWebSphereOEM/V7R0/config1</td>
<td>WebSphere root directory path of the application server.</td>
</tr>
<tr>
<td>IZU_WAS_PROFILE_PREFIX</td>
<td>BBNBASE</td>
<td>WebSphere SAF profile prefix.</td>
</tr>
<tr>
<td>IZU_CLUSTER_TRANSITION_NAME</td>
<td>BBNCO01</td>
<td>WebSphere cluster transition name.</td>
</tr>
<tr>
<td>IZU_CELL_SHORT_NAME</td>
<td>BBNBASE</td>
<td>WebSphere application server cell short name.</td>
</tr>
<tr>
<td>IZU_SERVANT_USERID</td>
<td>WSSRU1</td>
<td>WebSphere application server servant region user ID.</td>
</tr>
<tr>
<td>IZU_CONTROL_USERID</td>
<td>WSCRU1</td>
<td>WebSphere application server control region user ID.</td>
</tr>
<tr>
<td>Variable name</td>
<td>Default value</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IZU_ORB_PORT</td>
<td>32203</td>
<td>ORB port number, as specified in the WebSphere Application Server response file. If your installation selected to use the advanced configuration procedure of IBM WebSphere Application Server OEM Edition for z/OS, the default port number is 32203. For the typical configuration procedure, this is an installation-specific port number selected from your TCP/IP profile.</td>
</tr>
<tr>
<td>IZU_HTTP_SSL_PORT</td>
<td>32208</td>
<td>HTTPS transport port number, as specified in the WebSphere Application Server response file. If your installation selected to use the advanced configuration procedure of IBM WebSphere Application Server OEM Edition for z/OS, the default port number is 32208. For the typical configuration procedure, this is an installation-specific port number selected from your TCP/IP profile.</td>
</tr>
<tr>
<td>IZU_APPSERVER_HOSTNAME</td>
<td>NO.DEFAULT.VALUE</td>
<td>WebSphere application server host name.</td>
</tr>
<tr>
<td>IZU_WBEM_ROOT</td>
<td>/usr/lpp/wbem</td>
<td>Root directory path of the CIM server installation.</td>
</tr>
<tr>
<td>IZU_IL_CONFIGURE</td>
<td>NO.DEFAULT.VALUE</td>
<td>Indicates whether (Y or N) the Incident Log plug-in is to be included in z/OMSF.</td>
</tr>
<tr>
<td>IZU_CA_CONFIGURE</td>
<td>NO.DEFAULT.VALUE</td>
<td>Indicates whether (Y or N) the Configuration Assistant plug-in is to be included in z/OMSF.</td>
</tr>
<tr>
<td>IZU_WLM_CONFIGURE</td>
<td>NO.DEFAULT.VALUE</td>
<td>Indicates whether (Y or N) the Workload Management plug-in is to be included in z/OMSF.</td>
</tr>
<tr>
<td>IZU_RMF_CONFIGURE</td>
<td>NO.DEFAULT.VALUE</td>
<td>Indicates whether (Y or N) the Resource Monitoring plug-in is to be included in z/OMSF.</td>
</tr>
<tr>
<td>IZU_CP_CONFIGURE</td>
<td>NO.DEFAULT.VALUE</td>
<td>Indicates whether (Y or N) the Capacity Provisioning plug-in is to be included in z/OMSF.</td>
</tr>
<tr>
<td>IZU_DM_CONFIGURE</td>
<td>NO.DEFAULT.VALUE</td>
<td>Indicates whether (Y or N) the Deployment plug-in is to be included in z/OMSF.</td>
</tr>
<tr>
<td>IZU_WISPF_CONFIGURE</td>
<td>NO.DEFAULT.VALUE</td>
<td>Indicates whether (Y or N) the ISPF plug-in is to be included in z/OMSF.</td>
</tr>
<tr>
<td>IZU_IL_CEA_CONFIGURE</td>
<td>Y</td>
<td>Indicates whether z/OMSF is to enable the common event adapter (CEA) component and related parmlib options for using the Incident Log task.</td>
</tr>
<tr>
<td>IZU_CEA_HLQ</td>
<td>CEA</td>
<td>The high level qualifier to be used for CEA data sets, as defined in the CEAPRMxx parmlib member (one to four characters). This value is used in creating RACF commands for the Incident Log task.</td>
</tr>
<tr>
<td>IZU_COUNTRY_CODE</td>
<td>NO.DEFAULT.VALUE</td>
<td>IBM-defined country code for your site (3-character alphanumeric).</td>
</tr>
</tbody>
</table>
### Table 48. Default configuration file (continued)

<table>
<thead>
<tr>
<th>Variable name</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IZU_BRANCH_CODE</td>
<td>NO.DEFAULT.VALUE</td>
<td>IBM-defined branch code (or branch office) for your site (3-character alphanumeric).</td>
</tr>
</tbody>
</table>
| IZU_STORAGE_VALUE      | NO.DEFAULT.VALUE | Indicates where CEA is to store the snapshot information for Incident Log processing. Specify either an SMS storage class or up to seven volumes, as follows:  
- STORCLAS(STRCLS)  
- VOLSER(volume1, volume2, volume3,...,volume7) |
| IZU_CEAPRM_SOURCE_PARMLIB | SYS1.PARMLIB | Source data set that contains the IBM-supplied member, CEAPRM00.                 
- Usually, is your SMPE-installed SYS1.PARMLIB data set. Ensure that the data set exists and is cataloged. |
| IZU_CEAPRM_TARGET_PARMLIB | SYS1.PARMLIB | Target data set that will contain the newly created CEAPRM<nn> member for Incident Log processing. |
| IZU_IEADMC_SOURCE_PARMLIB | SYS1.SAMPLIB | Source data set that contains the IBM-supplied member, IEADMCZM.                 
- Usually, is your SMPE-installed SYS1.SAMPLIB data set. Ensure that the data set exists and is cataloged. |
| IZU_IEADMC_TARGET_PARMLIB | SYS1.PARMLIB | Target data set that will contain the newly created IEADMC<nn> member for Incident Log processing. |
| IZU_CEA_PARM_NAME      | 01             | Two-character suffix of a new CEAPRM<xx> parmlib member to be used for enabling captures or "snapshots" of the system logs. Two characters are required. |
| IZU_IEA_PARM_NAME      | ZM             | Two-character suffix of a new IEADMC<xx> parmlib member to be used for setting dump options. Two characters are required. |
| IZU_WLM_GROUP_NAME     | WLMGRP         | Workload Manager task group name.                                                |

### Default override file

The override response file is the last configuration file to be processed. Therefore, you can use this file to:
- Override values in the configuration file without directly modifying the configuration file.
- Make variable substitutions.

A default override response file is located in the `<IZU_CODE_ROOT>/defaults` directory. Figure 70 on page 259 shows the content of the default override file.
As shown in Figure 70, the STORCLAS and VOLSER values must be enclosed in double quotes.
Appendix E. Values from the WebSphere Application Server response file

During the z/OSMF configuration process, you supply the izusetup.sh script with the directory path and name of the WebSphere Application Server response file. Your installation created this file earlier when installing IBM WebSphere Application Server OEM Edition for z/OS. If you cannot supply this value, for example, because the response file is not accessible or no longer exists, the script prompts you for the following WebSphere values [Table 49].

Table 49. WebSphere response file values

<table>
<thead>
<tr>
<th>WebSphere value</th>
<th>Description</th>
<th>Variable name</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>zConfigurationGroup</td>
<td>WebSphere application server group.</td>
<td>IZU_APPSERVER_GROUP</td>
<td>WSCFG1</td>
</tr>
<tr>
<td>zConfigMountPoint</td>
<td>WebSphere root directory path of the application server.</td>
<td>IZU_APPSERVER_ROOT</td>
<td>/zWebSphereOEM/V7R0/config1</td>
</tr>
<tr>
<td>zSAFProfilePrefix</td>
<td>WebSphere SAF profile prefix.</td>
<td>IZU_WAS_PROFILE_PREFIX</td>
<td>BBNBASE</td>
</tr>
<tr>
<td>zClusterTransition</td>
<td>WebSphere cluster transition name.</td>
<td>IZU_CLUSTER_TRANSITION_NAME</td>
<td>BBNC001</td>
</tr>
<tr>
<td>zCellShortName</td>
<td>WebSphere application server cell short name.</td>
<td>IZU_CELL_SHORT_NAME</td>
<td>BBNBASE</td>
</tr>
<tr>
<td>zServantUserid</td>
<td>WebSphere application server servant region user ID.</td>
<td>IZU_SERVANT_USERID</td>
<td>WSSRU1</td>
</tr>
<tr>
<td>zControlUserid</td>
<td>WebSphere application server control region user ID.</td>
<td>IZU_CONTROL_USERID</td>
<td>WSCRU1</td>
</tr>
<tr>
<td>zOrbListenerPort</td>
<td>Port for IOP requests that acts as the bootstrap port for this server, and also as the port through which the ORB accepts IOP requests.</td>
<td>IZU_ORB_PORT</td>
<td>32203</td>
</tr>
<tr>
<td></td>
<td>This is the default port number if your installation selected to use the advanced configuration procedure of IBM WebSphere Application Server OEM Edition for z/OS. For the typical configuration procedure, this is an installation-specific port number selected from your TCP/IP profile.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>zOrbListenerSslPort</td>
<td>Port for secure IOP requests.</td>
<td>IZU_HTTP_SSL_PORT</td>
<td>32208</td>
</tr>
<tr>
<td></td>
<td>This is the default port number if your installation selected to use the advanced configuration procedure of IBM WebSphere Application Server OEM Edition for z/OS. For the typical configuration procedure, this is an installation-specific port number selected from your TCP/IP profile.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 49. WebSphere response file values (continued)

<table>
<thead>
<tr>
<th>WebSphere value</th>
<th>Description</th>
<th>Variable name</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostName</td>
<td>WebSphere application server host name.</td>
<td>IZU_APPSERVER_HOSTNAME</td>
<td>NO.DEFAULT.VALUE</td>
</tr>
</tbody>
</table>

You must provide a value for this.

### Appendix F. Modifying advanced settings for the z/OSMF configuration

z/OSMF includes a number of advanced settings that affect the behavior of the product. In most cases, you should not need to change these values. In special situations, however, you might be asked by IBM Support to modify the z/OSMF advanced settings. To do so, you will use the `izuupdate.sh` script, as described in this section.

#### About this script

This script allows you to display or modify the z/OSMF advanced settings. When used to modify the settings, the script takes as input values that you specify in a separate file and applies the values to your z/OSMF configuration.

Table 50 describes the z/OSMF advanced settings. You can change one or more of the settings in each invocation of the `izuupdate.sh` script.

<table>
<thead>
<tr>
<th><code>izuadmin.env</code> variable</th>
<th>Description</th>
<th>Allowable range of values</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>cimjnitimeout</td>
<td>Amount of time (in seconds) that z/OSMF is to wait for a response from the CIM server. If timeouts from CIM providers occur frequently, increasing this value can help to reduce the number of timeouts.</td>
<td>1 – 3600</td>
<td>300</td>
</tr>
<tr>
<td>ltpatimeout</td>
<td>Amount of time (in minutes) for LTPA credentials to be forwarded between servers. z/OSMF user sessions expire when this period of time has elapsed. For information, see &quot;Re-authenticating in z/OSMF&quot; on page 79.</td>
<td>25 – 35971</td>
<td>490</td>
</tr>
<tr>
<td>ltp cachetimeout</td>
<td>Amount of time (in seconds) for authentication settings to be held in cache.</td>
<td>1500 – 2158260</td>
<td>29400</td>
</tr>
<tr>
<td>sessiontimeout</td>
<td>Amount of time (in minutes) for the session management session timeout. This value must be at least 5 greater than the ltpatimeout value.</td>
<td>This value must be less than or equal to the ltpatimeout value multiplied by 60.</td>
<td>495</td>
</tr>
<tr>
<td>izutracespec</td>
<td>Initial trace state for the WebSphere server. These settings are read when the server is started. If there is a problem with starting the server, this value is used to enable tracing for server startup.</td>
<td>This value is provided by IBM Support.</td>
<td>Reserved by IBM.</td>
</tr>
<tr>
<td>izugwrkmanwlmclass</td>
<td>WLM transaction class to be used for managing the execution of long-running work. This setting is applicable if your z/OSMF configuration includes the Software Deployment plug-in.</td>
<td>One to eight alphanumeric characters (A-Z, a-z, 0-9) or special characters (#, $, or @).</td>
<td>IZUGWORK</td>
</tr>
</tbody>
</table>
Before running the script

If your installation currently uses a modified version of the izuadmin.env file, perhaps from a previous z/OSMF configuration, it is recommended that you make a backup copy of the file. Check for a modified version of the izuadmin.env file in the z/OSMF configuration directory and make note of any customized settings that should be preserved in the new copy. By default, the z/OSMF configuration directory is /etc/zosmf and is specified through the environment variable, IZU_CONFIG_DIR, as described in "Setting the z/OSMF environment variables for your shell session" on page 62.

Ensure that the z/OSMF environment variables are set properly for your z/OS UNIX shell session. See "Setting the z/OSMF environment variables for your shell session" on page 62.

You can run this script regardless of whether the WebSphere server is running. Your changes, however, do not take effect until after the server is started or recycled. For information about starting and stopping the server, see IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide GA32-0631.

Displaying your current settings

You can use the izuupdate.sh script to display the current settings for your configuration. To do so, include the -display option on your script invocation. The results are written to standard output and to the script log file. If you include the -display option on your invocation, the script displays your current settings, but does not modify them.

Figure 71 shows an example of the display output.

```
IZUG2151: Starting z/OSMF "display" procedure.
Thu Jan 12 14:15:06 EDT 2012
IZUG146I: Invoking script "/u/usr/lpp/zosmf/bin/izuadmin.sh -display".
IZUG300I: Script "izuadmin.sh" has started at "Thu Jan 12 14:15:06 EDT 2012".
IZUG387I: Setting "ltpatimeout" has a value of "490".
IZUG387I: Setting "ltpacachetimeout" has a value of "29400".
IZUG387I: Setting "sessiontimeout" has a value of "495".
IZUG387I: Setting "cimjnitimeout" is not set.
IZUG387I: Setting "izugworkmanwlcmclass" has a value of "IZUGWORK".
IZUG308I: Processing of script "izuadmin.sh" has completed at "Thu Jan 12 14:15:37 EDT 2012".
IZUG210I: The script "/u/usr/lpp/zosmf/bin/izuupdate.sh" has completed.
```

Figure 71. Sample results from the izuupdate.sh -display script invocation

Modifying your current settings

A sample izuadmin.env file is supplied with z/OSMF in the following directory:

<IZU_CODE_ROOT>/defaults/

where <IZU_CODE_ROOT> is the product file system. By default, this is /usr/lpp/zosmf/V1R13.

To override any of the current settings, use this procedure:
1. Copy the file `izuadmin.env` from the directory `<IZU_CODE_ROOT>/defaults` to the directory `<IZU_CONFIG_DIR>`.

2. Edit the `<IZU_CONFIG_DIR>/izuadmin.env` file using an editor of your choice, updating the settings as needed. Figure 72 shows which settings are processed by the `izuupdate.sh` script.

```
ltpatimeout=490
ltpacachetimeout=29400
sessiontimeout=495
izugwrkmanwlmclass=IZUGWORK
#cimjnitimeout=300
#izutracespec="com.ibm.zoszmf.*=INFO:com.ibm.zoszmf.environment.ui=finer"
```

Figure 72. Settings that are processed through the `izuupdate.sh` script

Observe the following considerations for the `izuadmin.env` file:
- Do not modify the file version identifier: `izufileversion=n.nn.n`
- Do not modify or delete settings other than those shown in Figure 72
- If you omit a setting, comment it out, or set it to null, the IBM default value is used
- Some input fields are commented. To modify these settings, you must remove the comment character `#`

3. Run the `izuupdate.sh` script, as described in "Running the script."

**Running the script**

**Authority**
Run this script from the z/OSMF administrator user ID that you created previously (ZOSMFAD, by default). You must log on to this user ID; you cannot switch to it from another user ID, for example, through the `su` shell command.

**Environment**
Run the script in either an OMVS or telnet/rlogin session. You cannot run it from ISHELL.

**Location**
The script resides in the following directory:

```
<IZU_CODE_ROOT>/bin
```

where `<IZU_CODE_ROOT>` is the product file system. By default, this is `/usr/lpp/zosmf/V1R13`.

**Invocation**
From your shell session, run the script, as follows:

```
izuupdate.sh -file [pathname]/izuconfig1.cfg [-display]
```

Figure 73. Syntax for the `izuupdate.sh` script

Where:
- `-file` is a required parameter; use it to specify the configuration file for your configuration. You created the configuration file previously in "Step 1: Create the initial configuration" on page 65. On the `-file` parameter,
<pathname> is optional. If you omit a path name, the script obtains the configuration file from the z/OSMF configuration directory: <IZU_CONFIG_DIR>.

- `-display` is an optional parameter; use it to query your current settings. If you include the `-display` option on your invocation, the script displays your current settings, but does not modify them.

**Results**

On completion, the script writes messages to standard output and to the script log file:

<IZU_LOGFILE_DIR>/izuupdate_mm.dd.yy.hh.mm.ss.tt.log

where <IZU_LOGFILE_DIR> is the log file directory for your installation. By default, this is /var/zosmf/configuration/logs/.

Check the messages to determine whether a problem occurred during script processing. If so, you must resolve the problem before the request can be completed.
Appendix G. Examples of working with z/OSMF runtime logs

For your reference, this topic describes the attributes of the z/OSMF log files that are created at runtime.

Examining log data that originates from the server

Figure 74 shows portions of an example of z/OSMF server side log data.

Example log record:

```
2009-04-29T18:38:51.285Z|00000012|com.ibm.zoszmf.util.eis.cim.ccp.CimClientPool|getClient(Endpoint, String, Set<Locale>) INFO:IZUG911I: Connection to "http://null:5988" cannot be established, or was lost and cannot be re-established using protocol "CIM".
com.ibm.zoszmf.util.eis.EisConnectionException: IZUG911I: Connection to "http://null:5988" cannot be established, or was lost and cannot be re-established using protocol "CIM".
com.ibm.zoszmf.util.eis.EisException.getEisException(EisException.java:146)
com.ibm.zoszmf.util.eis.EisException.diagnoseAndThrow(EisException.java:221)
com.ibm.zoszmf.util.eis.cim.ccp.CimClientPool.getWBEMClient(CimClientPool.java:279)
```

Figure 74. Portion of a z/OSMF server side log data

As shown in Figure 74, each log record begins with a line divided by 'pipe' (|) characters into the following components:
- Timestamp in ISO8601 format, set to UTC timezone. Example: 2009-03-10T18:04:08.051Z
- Thread ID as an 8 digit hex number. Example: 00000010
- Class name. Example: com.ibm.zoszmf.util.eis.cim.ccp.CimClientPool
- Method name. Example: getClient(Endpoint, String).

The next line of a log record contains the logging level, followed by a colon, followed by the message text. Messages logged at level INFO, WARNING, or SEVERE begin with an eight character message ID at the start of the message text. Message IDs that begin with "IZU" are part of the z/OSMF product. For descriptions of these messages, see IBM z/OS Management Facility Messages SA38-0654.

If the log record includes an exception, the exception is logged next. The exception class is logged, followed by a colon, followed by the message text of the exception. The lines following this make up the traceback information embedded in the exception, which is useful first-failure data capture. If the exception has attached causes, each cause is also logged with "+->" indicating the start of an attached cause.
The last line in every log record is contained in square brackets. If the log record is written during a specific user's context, information about that context is logged, as follows:

- "Transaction ID". An internal counter value that applies to all actions between a specific set and clear of a context. This identifier begins with "tx", followed by a sixteen digit hex ID, and ends with a colon ':'.
- Remote user name (null for a guest user). This value is followed by an 'at' symbol (@).
- Remote host name. This value is followed by a space.
- Servlet "verb" is next, contained in parenthesis. Examples include GET and POST.
- URL of the request and query string, ending with the closing square bracket ']').

If the log record is created during an initialization sequence, the transaction ID is printed and the user name is listed as "*bootstrap*". No other data are provided.

If the log record is created with no known context, only "[tx:]" appears on the last line.

**Viewing client side log data**

Included with the server statistics in the z/OSMF logs are client side data, which are used to monitor the JavaScript activity of each user login session. Client side log data differs in format from server side log data, as shown in Figure 75.

Log records that originate from the client side are formatted using the same data as those that originate within the server. However, the "message text" itself is specially formatted to represent the state of the client when the message occurred. This is done to compensate for the fact that client side messages might not be immediately sent to the server.

The following fields are recorded on the client when the message occurs, and are formatted within the message text of a log record as such:

- Client timestamp in square brackets [ ]
- Browser name and level
- ENTRY or RETURN, to indicate the beginning or the end of a routine
- Package name, such as AuthorizationServices
- Module name, such as util.ui.messages.Message.js
- Method name, such as _getMessageType()
- Detailed message.
Appendix H. Common event adapter (CEA) reason codes

A problem in the configuration of z/OSMF might be indicated by reason codes from the common event adapter (CEA) component of z/OS.

This section describes the configuration-related CEA reason codes and includes a cross-reference of reason codes to CIM messages and z/OSMF messages. Where an associated z/OSMF message is indicated, check the z/OSMF message for more information about resolving the error.

This section is organized, as follows:

- “CEA reason codes related to the Incident Log task” on page 270
- “CEA reason codes related to the ISPF task” on page 274.
## CEA reason codes related to the Incident Log task

Table 51 describes the CEA reason codes you might encounter when setting up or using the Incident Log task. By default, CEA reason codes without an associated z/OSMF message are accompanied by z/OSMF message IZUP631E.

### Table 51. CEA reason codes related to Incident Log task processing

<table>
<thead>
<tr>
<th>Reason code (hex)</th>
<th>Description</th>
<th>System programmer action</th>
<th>CIM message</th>
<th>Associated z/OSMF message</th>
<th>IBM Support information</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>The CEA address space is not running.</td>
<td>Follow the steps in &quot;Ensuring that CEA is active&quot; on page 245.</td>
<td>CEZ05002E</td>
<td>IZUP634E</td>
<td>CEAUNAVAIL</td>
</tr>
<tr>
<td>121</td>
<td>CIM indication processing is not available because the CEA address space is running in MIN mode. To support Incident Log processing, CEA must be operated in FULL mode.</td>
<td>Use the MODIFY CEA,MODE command to adjust the CEA mode of operation to FULL mode. To do so, enter the following command from the operator console: <code>F CEA,MODE=FULL</code> Running CEA in FULL mode requires that z/OS UNIX System Services be available.</td>
<td>CEZ05013E</td>
<td>CEAFORCEMINMODE</td>
<td></td>
</tr>
<tr>
<td>32D</td>
<td>The user is not authorized for this request.</td>
<td>Define the appropriate authority for the user. See &quot;Creating the commands to authorize a user ID&quot; on page 120.</td>
<td>CEZ05003E</td>
<td>IZUP635E</td>
<td>CEANOINSTRAUTH</td>
</tr>
<tr>
<td>33E</td>
<td>An abend occurred in the CEA task that interacts with the IPCS environment.</td>
<td>Report the problem to IBM Support.</td>
<td>CEZ05001E</td>
<td>IZUP639E</td>
<td>CEAIPRQServerAbended</td>
</tr>
<tr>
<td>342</td>
<td>The sysplex dump directory is empty.</td>
<td>Ensure that the sysplex dump directory is not empty.</td>
<td></td>
<td></td>
<td>CEASDDIREMPTY</td>
</tr>
<tr>
<td>343</td>
<td>A dump incident was not found. Most likely, the incident was deleted by another user.</td>
<td>No action is required.</td>
<td>CEZ05004E</td>
<td>IZUP636E</td>
<td>CEAADDFAILED</td>
</tr>
</tbody>
</table>
| 352               | The dump analysis and elimination (DAE) data set name (typically SYS1.DAE) could not be determined. Most likely, DAE is not configured or is not running. Or, the user attempted to unsuppress a dump without having write access to the DAE data set. | Ensure that:  
  - DAE is active.  
  - DAE is configured, as described in z/OS MVS Diagnosis: Tools and Service Aids.  
  - User has write access to the active DAE data set.  
  For more information, see "Configuring dump analysis and elimination" on page 242. |  | IZUP637E | CEADAEDSNNOTAvailable |
<table>
<thead>
<tr>
<th>Reason code (hex)</th>
<th>Description</th>
<th>System programmer action</th>
<th>CIM message</th>
<th>Associated z/OSMF message</th>
<th>IBM Support information</th>
</tr>
</thead>
<tbody>
<tr>
<td>357</td>
<td>The called function could not generate a prepared data set name (DSN).</td>
<td>Verify that the compiled REXX exec CEACDMPP exists and can be run by System REXX.</td>
<td></td>
<td></td>
<td>CEAGENPREPAREDDSNFAIL</td>
</tr>
</tbody>
</table>
| 358              | An error was encountered when invoking a REXX exec. Typically, this error occurs when the SYS1.MIGLIB data set is not APF-authorized (is not defined in the PROGxx parmlib member). If so, this reason code is accompanied by message CEZ05000E with the following codes (in decimal):  
  • DIAG1=12  
  • DIAG2=25  
  • DIAG3=774. | Follow the steps in “Authorizing the SYS1.MIGLIB data set on page 249.” | CEZ05000E   | IZUP639E                 | CEAREXENVERROR           |
| 359              | An internal CEA error occurred when attempting to invoke a SYSREXX exec. | If this reason code is accompanied by the following codes (in decimal), check the SYSREXX concatenation for a missing exec:  
  • DIAG=8  
  • DIAG2=851.  
  Also, check message CEZ05000E in SYSLOG.  
  CEAERRO_Msg contains the name of the SYSREXX exec. | CEZ05000E   |                          | CEAAXREXXERROR           |
<p>| 365              | The System REXX address space or the functions it provides are not available. | Follow the steps in “Ensuring that System REXX is set up and active” on page 247. | CEZ05005E   | IZUP640E                 | CEASYRXXNOTACTIVE        |
| 366              | System REXX cannot process an exec. | This problem usually indicates that the run time support for compiled REXX has not been set up. See “Ensuring that System REXX is set up and active” on page 247. | CEZ05006E   | IZUP643E                 | CEASYRXXBADENVIRONMENT   |
| 367              | System REXX cannot process the exec at this time. | Try the request again later. | CEZ05007W   | IZUP644E                 | CEAXEXECUTETIMEOUT       |
| 368              | System REXX cannot schedule the exec to run at this time. | Try the request again later. | CEZ05008W   | IZUP645E                 | CEASYRXXOVERLOADED       |</p>
<table>
<thead>
<tr>
<th>Reason code (hex)</th>
<th>Description</th>
<th>System programmer action</th>
<th>CIM message</th>
<th>Associated z/OSMF message</th>
<th>IBM Support information</th>
</tr>
</thead>
<tbody>
<tr>
<td>36E</td>
<td>The SYS1.MIGLIB data set is not APF-authorized, which has prevented REXX execs from being invoked.</td>
<td>Follow the steps in &quot;Authorizing the SYS1.MIGLIB data set&quot; on page 249.</td>
<td>CEZ05009E</td>
<td>CEAMIGLIBNOTAPFAUTH</td>
<td></td>
</tr>
<tr>
<td>36F</td>
<td>The user is not authorized to view operations log (OPERLOG) snapshot information.</td>
<td>Perform the corrective action described in &quot;User is not SAF authorized&quot; on page 166.</td>
<td>CEZ05010E</td>
<td>CEANOSAFOPERLOGSNAP</td>
<td></td>
</tr>
<tr>
<td>370</td>
<td>The system logger component is not available.</td>
<td>For an explanation of the logger reason code in CEAERRO_DIAG4, see mapping macro IXGCON. If the system is not running with a logger couple data set, this is a permanent condition for the IPL. Otherwise restart system logger and enter the request again. For more information, see &quot;Defining a couple data set for system logger&quot; on page 233. For information about the IXGCON macro, see z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG.</td>
<td>CEZ05011E</td>
<td>CEALOGGERNOTAVAIL</td>
<td></td>
</tr>
<tr>
<td>371</td>
<td>The function that prepares incident materials to be sent through FTP could not allocate a new data set for the tersed diagnostic snapshot.</td>
<td>Check the CIM trace file for system messages associated with the return code indicating the reason for the failure. For assistance, contact IBM Support.</td>
<td></td>
<td></td>
<td>CEABADALLOCNEW</td>
</tr>
<tr>
<td>372</td>
<td>The function that prepares an incident to be sent through FTP could not allocate the data set to be tersed.</td>
<td>Check the CIM trace file for system messages associated with the return code indicating the reason for the failure. For assistance, contact IBM Support.</td>
<td></td>
<td></td>
<td>CEATERSEBADALLOC1</td>
</tr>
<tr>
<td>376</td>
<td>The operations log (OPERLOG) snapshot was not created. When attempting to access the OPERLOG snapshot, the system logger service IXGCONN received a bad return or reason code indicating that the OPERLOG snapshot does not exist.</td>
<td>Check SYSLOG for message CEA0600I, which contains the return and reason codes.</td>
<td></td>
<td></td>
<td>CEANOSNAPSHOT</td>
</tr>
<tr>
<td>Reason code (hex)</td>
<td>Description</td>
<td>System programmer action</td>
<td>CIM message</td>
<td>Associated z/OSMF message</td>
<td>IBM Support information</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>--------------------------</td>
<td>-------------</td>
<td>--------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>378</td>
<td>No log data was accumulated in diagnostic snapshot.</td>
<td>If this problem occurs frequently, adjust the DUMPCAPTURETIME setting in the CEAPRMxx parmlib member.</td>
<td>CIM message</td>
<td>CEAPDWB_DIAGDATAEMPTY</td>
<td>CEAPDWB_DIAGDATAEMPTY</td>
</tr>
<tr>
<td>379</td>
<td>An incorrect format or value was supplied for the IBM PMR number.</td>
<td>Correct the IBM PMR number and try again. The format of the IBM PMR number should be nnnn.nnnn where nnnn is the PMR number and nnnn is the branch code, and ccc is the country code.</td>
<td>CIM message</td>
<td>CEAWRONGIBMPMRFORMAT</td>
<td>CEAWRONGIBMPMRFORMAT</td>
</tr>
<tr>
<td>37D</td>
<td>An attempt to obtain the enqueue on the sysplex dump directory failed; another program already holds the enqueue.</td>
<td>• Ensure that only one user is attempting to access the dump information at one time. To check for enqueue contention, enter the following command at the operator console: DGRS wait for the enqueue to be released and try again.</td>
<td>CIM message</td>
<td>CEAPCSENQERROR</td>
<td>CEAPCSENQERROR</td>
</tr>
<tr>
<td>37E</td>
<td>The requested function failed to open the sysplex dump directory.</td>
<td>Verify that the sysplex dump directory (default name SYS1.DDIR) is set up and usable. For more information, see &quot;Creating the sysplex dump directory&quot; on page 243.</td>
<td>CIM message</td>
<td>CEAPCSENQERROR</td>
<td>CEAPCSENQERROR</td>
</tr>
<tr>
<td>382</td>
<td>The component table is corrupted.</td>
<td>Report the problem to IBM Support.</td>
<td>CIM message</td>
<td>CEAXMLTAGSTOOODEEP</td>
<td>CEAXMLTAGSTOOODEEP</td>
</tr>
<tr>
<td>385</td>
<td>The diagnostic data to be sent is currently in use.</td>
<td>Try the request again later.</td>
<td>CIM message</td>
<td>CEAPREPAREOBJINUSE</td>
<td>CEAPREPAREOBJINUSE</td>
</tr>
<tr>
<td>386</td>
<td>The diagnostic data to be sent is currently in use.</td>
<td>Try the request again later.</td>
<td>CIM message</td>
<td>CEAPREPAREENQERR</td>
<td>CEAPREPAREENQERR</td>
</tr>
<tr>
<td>38C</td>
<td>The sysplex dump directory has no space available to record new SVC dumps.</td>
<td>See &quot;Establishing a larger sysplex dump directory&quot; on page 244.</td>
<td>CIM message</td>
<td>CEACKSTINVALDALLOCVALUE</td>
<td>CEACKSTINVALDALLOCVALUE</td>
</tr>
<tr>
<td>391</td>
<td>The JES subsystem is not available.</td>
<td>Determine why the JES subsystem is not accessible. Perhaps, it has not been started.</td>
<td>CIM message</td>
<td>CEAJESNOTAVAILABLE</td>
<td>CEAJESNOTAVAILABLE</td>
</tr>
<tr>
<td>397</td>
<td>The Set Incident field data was truncated at 256 characters.</td>
<td>Specify a smaller amount of data for the user comment field to prevent truncation. Retry the request.</td>
<td>CIM message</td>
<td>CEASETINCIFVALIDATATRUNC</td>
<td>CEASETINCIFVALIDATATRUNC</td>
</tr>
</tbody>
</table>
**CEA reason codes related to the ISPF task**

Table 52 describes the CEA reason codes you might encounter when setting up or using the ISPF task.

<table>
<thead>
<tr>
<th>Reason code (hex)</th>
<th>Description</th>
<th>System programmer action</th>
<th>Associated z/OSMF message</th>
<th>IBM Support information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>An error occurred during CEATSOREQUEST processing. The z/OS UNIX message queue processing failed.</td>
<td>Ensure that the CEA started task is TRUSTED; see System prerequisites for the ISPF plugin on page 27. For more information, check the z/OSMF logs and the system logs.</td>
<td>IZUIS615E, IZUIS616E, IZUIS620E</td>
<td>CEATSONUSERIDFOUND</td>
</tr>
<tr>
<td>1001</td>
<td>An error occurred during CEATSOREQUEST processing. An input user ID value was expected, but was not received.</td>
<td>For more information, check the z/OSMF logs and the system logs.</td>
<td>IZUIS615E, IZUIS616E, IZUIS620E</td>
<td>CEATSONUSERIDFOUND</td>
</tr>
<tr>
<td>1002</td>
<td>An error occurred during CEATSOREQUEST processing. A user ID was expected, but was not found in the session table.</td>
<td>For more information, check the z/OSMF logs and the system logs.</td>
<td>IZUIS615E, IZUIS616E, IZUIS620E</td>
<td>CEATSONMATCHMISSING</td>
</tr>
<tr>
<td>1003</td>
<td>An error occurred during CEATSOREQUEST processing. An input STOKEN value was expected, but was not received.</td>
<td>For more information, check the z/OSMF logs and the system logs.</td>
<td>IZUIS615E, IZUIS616E, IZUIS620E</td>
<td>CEATSTOKENMISSING</td>
</tr>
<tr>
<td>1004</td>
<td>An error occurred during CEATSOREQUEST processing. The input table index is too big or too small for the session table.</td>
<td>For more information, check the z/OSMF logs and the system logs.</td>
<td>IZUIS615E, IZUIS616E, IZUIS620E</td>
<td>CEATOINDEXOUTOFRANGE</td>
</tr>
<tr>
<td>1005</td>
<td>An error occurred during CEATSOREQUEST processing. CEA could not create a TSO/E user address space.</td>
<td>Ensure that sufficient system resources are available to create the address space, and verify that the user is authorized to create address spaces.</td>
<td>IZUIS617E, IZUIS620E</td>
<td>CEATSOSTARTFAILED</td>
</tr>
<tr>
<td>1006</td>
<td>An error occurred during CEATSOREQUEST processing. CEA could not invoke TSO/E attention processing.</td>
<td>For more information, check the z/OSMF logs and the system logs.</td>
<td>IZUIS615E, IZUIS616E, IZUIS620E</td>
<td>CEATSOATTNFALIED</td>
</tr>
<tr>
<td>1007</td>
<td>An error occurred during CEATSOREQUEST processing. CEA could not end a TSO/E user address space.</td>
<td>For more information, check the z/OSMF logs and the system logs.</td>
<td>IZUIS615E, IZUIS616E, IZUIS620E</td>
<td>CEATSOENDFAILED</td>
</tr>
<tr>
<td>1008</td>
<td>An error occurred during CEATSOREQUEST processing. An attempt to query the session table failed.</td>
<td>For more information, check the z/OSMF logs and the system logs.</td>
<td>IZUIS615E, IZUIS616E, IZUIS620E</td>
<td>CEATSOQUERYFAILED</td>
</tr>
<tr>
<td>1009</td>
<td>An error occurred during CEATSOREQUEST processing. An attempt to query the session table for the users associated with a specific application failed.</td>
<td>For more information, check the z/OSMF logs and the system logs.</td>
<td>IZUIS615E, IZUIS616E, IZUIS620E</td>
<td>CEATSOQUERYAPPFAILED</td>
</tr>
<tr>
<td>100A</td>
<td>An error occurred during CEATSOREQUEST processing. Ping processing failed.</td>
<td>For more information, check the z/OSMF logs and the system logs.</td>
<td>IZUIS615E, IZUIS616E, IZUIS620E</td>
<td>CEATSTOPINGFAILED</td>
</tr>
</tbody>
</table>
Table 52. CEA reason codes related to ISPF task processing (continued)

<table>
<thead>
<tr>
<th>Reason code (hex)</th>
<th>Description</th>
<th>System programmer action</th>
<th>Associated z/OSMF message</th>
<th>IBM Support information</th>
</tr>
</thead>
<tbody>
<tr>
<td>100B</td>
<td>An error occurred during CEATSOREQUEST processing. Normal log-off failed for a TSO/E user address space. Cancel will now be attempted.</td>
<td>Most likely, the system cancelled the user address space and no further action is needed. If that did not occur, check the z/OSMF logs and the system logs for more information.</td>
<td>IZUIS615E, IZUIS616E, IZUIS620E, IZUIS630W</td>
<td>CEATSOENDSENDLOGOFF_FAILED</td>
</tr>
<tr>
<td>100C</td>
<td>A request to start a TSO/E session was received from a program running in an incorrect addressing mode. The interface requires that the calling program be running in AMODE(64).</td>
<td>Ensure that the ISPF run time support for compiled REXX is set up properly.</td>
<td></td>
<td>CEATSOBADAMODE</td>
</tr>
<tr>
<td>100D</td>
<td>A request to start a TSO/E session was received from a program that was disabled for interrupts. The interface requires that the calling program be enabled for interrupts.</td>
<td>Contact IBM Support for assistance.</td>
<td></td>
<td>CEATSONODISABLED</td>
</tr>
<tr>
<td>100E</td>
<td>A request to start a TSO/E session was received from a program that was not running in task mode, for example, a service request block (SRB) routine or an interrupt request block (IRB) routine. The interface requires that the calling program be running in task mode.</td>
<td>Contact IBM Support for assistance.</td>
<td></td>
<td>CEATSONOTASKMODE</td>
</tr>
<tr>
<td>100F</td>
<td>A request to start a TSO/E session was received from a program having a functional recovery routine (FRR), which is not allowed.</td>
<td>Contact IBM Support for assistance.</td>
<td></td>
<td>CEATSOFRRSET</td>
</tr>
<tr>
<td>1010</td>
<td>A request to start a TSO/E session was received from a program holding a system lock, which is not allowed.</td>
<td>Contact IBM Support for assistance.</td>
<td></td>
<td>CEATSOLOCKED</td>
</tr>
<tr>
<td>1011</td>
<td>A request to start a TSO/E session was received from a program running in cross memory mode, which is not allowed.</td>
<td>Contact IBM Support for assistance.</td>
<td></td>
<td>CEATSOXMMODE</td>
</tr>
<tr>
<td>1012</td>
<td>A request to display the CEA TSO ISPF session table encountered an error.</td>
<td>Ensure that the MODIFY command was entered correctly, for example: F CEAS,DIAG,SESSTABLE If the command was entered correctly, make note of any diagnostic codes that accompany this error and contact IBM Support for assistance.</td>
<td></td>
<td>CEATSOSESTBLDSPFILEFAILED</td>
</tr>
<tr>
<td>1013</td>
<td>A request to start or communicate with a TSO/E session contained incorrect data in the request structure interface.</td>
<td>Make note of any diagnostic codes that accompany this error and contact IBM Support for assistance.</td>
<td></td>
<td>CEATSOREQSTRUCTFILEBAD</td>
</tr>
<tr>
<td>Reason code (hex)</td>
<td>Description</td>
<td>System programmer action</td>
<td>Associated z/OSMF message</td>
<td>IBM Support information</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>---------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>1014</td>
<td>A request to communicate with a TSO/E session contained an incorrect eye-catcher in the output structure.</td>
<td>Contact IBM Support for assistance.</td>
<td></td>
<td>CEATSOBADQUERYEYECATCHER</td>
</tr>
<tr>
<td>1015</td>
<td>A request to communicate with a TSO/E session contained an incorrect version number in the output structure.</td>
<td>Contact IBM Support for assistance.</td>
<td></td>
<td>CEATSOBADQUERYVERSION</td>
</tr>
</tbody>
</table>
Appendix I. Contents of the RACF commands exec

During the z/OSMF configuration process, the izusetup.sh script creates the izuconfig1.cfg.rexx exec, which contains RACF commands for your installation. The contents of the exec are tailored for your installation and depend on which plug-ins you have chosen to configure, and which authorization mode you have selected: SAF Authorization Mode or Repository Authorization Mode.

For your reference, this topic shows which RACF commands are created when your installation chooses to deploy all of the plug-ins. The commands are those that would be included for SAF Authorization Mode (the default). Thus, for each plug-in to be enabled, the REXX exec contains commands for:

- Activating the ZMFAPLA resource class, which is new in z/OS V1R13, and enabling it for RACLST processing.
- Creating profiles in ZMFAPLA for each of the z/OSMF tasks to be enabled on your system
- Creating groups and permitting those groups to z/OSMF resources. By default, z/OSMF creates the groups IZUADMIN and IZUUSER, which correspond to the administrator and user roles, respectively.

The contents of the exec are provided in sections, as follows:

- “Commands for configuring the core functions” on page 278
- “Commands for permitting z/OSMF tasks to your CIM server” on page 280
- “Commands for configuring the Capacity Provisioning plug-in” on page 281
- “Commands for configuring the Configuration Assistant plug-in” on page 282
- “Commands for configuring the Incident Log plug-in” on page 283
- “Commands for configuring the ISPF plug-in” on page 285
- “Commands for configuring the Resource Monitoring plug-in” on page 286
- “Commands for configuring the Software Deployment plug-in” on page 287
- “Commands for configuring the Workload Management plug-in” on page 288
Commands for configuring the core functions

The RACF commands for securing the z/OSMF core functions are shown in Figure 76 and Figure 77 on page 279.

```
/*-----------------------------------------------*/
/* */
/* Begin Core Setup */
/* */
/*-----------------------------------------------*/

/* Create the z/OSMF Administrators group */
Call RacfCmd "ADDGROUP IZUADMIN OMVS(GID(9003))"
/* Create the z/OSMF Users group */
Call RacfCmd "ADDGROUP IZUUSER OMVS(GID(9004))"
/* Create the z/OSMF Administrator UserID */
/* The home directory is created in the -prime step */
Call RacfCmd "ADDUSER ZOSMFAD DFLTGRP(IZUADMIN) OMVS(UID(8001) HOME(/home/zosmfad) PROGRAM(/bin/sh)) NOPASSWORD NOIDCARD"
Call RacfCmd "ALU ZOSMFAD TSO(PROC(PROCAT) ACCTNUM(ABC123) SIZE(2098128)) OMVS(ASSIZEMAX(2147483647) MEMLIMIT(2G))"
/* Assign a password to the Administrator UserID before using it */
/* This is an example only - it is not recommended to insert passwords in this file */
/* Call RacfCmd "ALU ZOSMFAD PASSWORD(InsertAValidPassword) NOEXPIRED" */
/* Connect the z/OSMF Administrator UserID to the WebSphere Application Server Administrators Group */
Call RacfCmd "CONNECT ZOSMFAD GROUP(WSCFG1)"
/* Permit the z/OSMF groups to the WebSphere Application Server resources */
/* Assumption: APPL class has been defined, activated, and raclisted during the WebSphere Application Server setup. */
Call RacfCmd "PERMIT BBNBASE CLASS(APPL) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
/* The EJBROLE definitions are case-sensitive in RACF. Insure you preserve case for these commands */
/* Assumption: EJBROLE is defined, activated, and raclisted during the WebSphere Application Server setup. */
Call RacfCmd "RDEFINE EJBROLE BBNBASE.izuUsers UACC(NONE)"
Call RacfCmd "PERMIT BBNBASE.izuUsers CLASS(EJBROLE) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT BBNBASE.izuUsers CLASS(EJBROLE) ID(IZUUSER) ACCESS(READ)"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
/* SyncToOSThread permits */
/* Assumption: BBO.SYNC.XXXXXX.YYYYYY facility class has been defined, activated, and raclisted during the WebSphere Application Server setup. */
/* Call RacfCmd "DEFINE FACILITY BBO.SYNC.BBNBASE.BBNCOO1 UACC(NONE)" */
Call RacfCmd "PERMIT BBO.SYNC.BBNBASE.BBNCOO1 CLASS(FACILITY) ID(WSCRMU1) ACC(CONTROL)"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
/* List-of-groups authority checking supplements the normal RACF access authority checking */
/* by allowing all groups of which a user ID is a member to enter into the access list checking process. */
/* Assumption: GRPLIST is activated during the WebSphere Application Server setup. */
/* Un-comment the following line to activate this. */
/* Call RacfCmd "SETROPTS GRPLIST" */
```

Figure 76. Sample RACF commands for configuring the core functions of z/OSMF (Part 1 of 2)
/* Setup for Multi-Layer Security (MLS) */
/* This step is only necessary if the installation is already using MLS. Otherwise, it can be skipped. */
/* Call RacfCmd *ALTUSER ZOSMFAD SECLABEL(SYSMULTI)*/
/* Call RacfCmd *PERMIT SYSMULTI CLASS(SECLABEL) ID(ZOSMFAD) ACCESS(READ)*/

/* Activate the ZMFAPLA class */
Call RacfCmd "SETROPTS CLASSACT(ZMFAPLA) GENERIC(ZMFAPLA) RACLIST(ZMFAPLA)"

/* Define the z/OSMF profile */
Call RacfCmd "RDEFINE ZMFAPLA BBNBASE.ZOSMF.** UACC(NONE)"

/* Permit the Administrators group to the z/OSMF profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.** CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Permit the Users group to the z/OSMF profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.** CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/* Define the Administrator task profile */
Call RacfCmd "RDEFINE ZMFAPLA BBNBASE.ZOSMF.ADMINTASKS.** UACC(NONE)"

/* Permit the Administrators group to the Administrator task profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.ADMINTASKS.** CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Define the Links profile */
Call RacfCmd "RDEFINE ZMFAPLA BBNBASE.ZOSMF.LINK.** UACC(NONE)"

/* Permit the Administrators group to the Links profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.LINK.** CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Permit the Users group to the Links profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.LINK.** CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/* Make changes effective */
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"

/* End Core Setup */

Figure 77. Sample RACF commands for configuring the core functions of z/OSMF (Part 2 of 2)
Commands for permitting z/OSMF tasks to your CIM server

If your installation selects one or more plug-ins that require the use of the CIM server on your z/OS system, the exec includes instructions for authorizing users to the CIM server resources, as shown in Figure 78. These instructions, and the sample command, are commented out in the generated exec.

/* During the z/OSMF configuration process, your installation selected */
/* one or more CIM dependent plug-in(s). As a result, your security */
/* administrator must ensure that the z/OSMF user has the proper level */
/* of access to CIM server resources. Your security administrator must */
/* do the following: */

/* 1) The user needs UPDATE access to the CIMSERV profile in the WBEM class. */
/* This can either be an explicit PERMIT or if a group is already */
/* permitted with UPDATE access then the user can be connected to this */
/* group. The WBEM class may need to be refreshed. */
/* The following commented command would be appropriate to use if a */
/* group has been permitted to the WBEM class. The group name is a */
/* default value and may need to be modified according to your setup. */
/* Call RacfCmd "CONNECT ZOSMFAD GROUP(CFZADMGP)" */

/* 2) The user ID under which the CIM server is running needs SURROGAT */
/* access for the zOSMF user. */
/* There may be a generic BPX.SRV.* profile in the SURROGAT class that */
/* is already authorized. If so, no additional actions are required. */
/* Otherwise, a discrete profile may need to be defined and authorized. */
/* The SURROGAT class may need to be refreshed if it is RACLISTed. */

Figure 78. Sample RACF command for authorizing users to the CIM server resources
Commands for configuring the Capacity Provisioning plug-in

If your installation has chosen to configure the Capacity Provisioning plug-in, the izuconfig1.cfg.rexx exec includes a section with RACF commands for creating the required security definitions. Figure 79 shows the commands that are created when SAF Authorization Mode has been selected for the configuration.

```c
/*-----------------------------------------------------------------------*/
/* */
/* Begin Capacity Provisioning Setup */
/* */
/*-----------------------------------------------------------------------*/

/* Connect the z/OSMF Administrator UserID to the Capacity Provisioning Query Group */
Call RacfCmd "CONNECT (ZOSMFAD) GROUP(CPOQUERY) AUTH(USE)"

/* Connect the z/OSMF Administrator UserID to the Capacity Provisioning Control Group */
Call RacfCmd "CONNECT (ZOSMFAD) GROUP(CPOCTRL) AUTH(USE)"

/* Define the Capacity Provisioning profile */
Call RacfCmd "RDEFINE ZMFAPLA BBNBASE.ZOSMF.CAPACITY_PROVISIONING.** UACC(NONE)"

/* Permit the Administrators group to the Capacity Provisioning profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.CAPACITY_PROVISIONING.** CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Permit the Users group to the Capacity Provisioning profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.CAPACITY_PROVISIONING.** CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/* Make changes effective */
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"

/*-----------------------------------------------------------------------*/
/* */
/* End Capacity Provisioning Setup */
/* */
/*-----------------------------------------------------------------------*/
```

Figure 79. Sample RACF commands for configuring the Capacity Provisioning plug-in

---

Appendix I. Contents of the RACF commands exec 281
Commands for configuring the Configuration Assistant plug-in

If your installation has chosen to configure the Configuration Assistant plug-in, the izuconfig1.cfg.rexx exec includes a section with RACF commands for creating the required security definitions. Figure 80 shows the commands that are created when SAF Authorization Mode has been selected for the configuration.

```plaintext
/*-----------------------------------------------*/
/* */
/* Begin Configuration Assistant Setup */
/* */
/*-----------------------------------------------*/

/* Define the Configuration Assistant profile */
Call RacfCmd "RDEFINE ZMFAPLA BBNBASE.ZOSMF.CONFIGURATION_ASSISTANT.** UACC(NONE)"

/* Permit the Administrators group to the Configuration Assistant profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.CONFIGURATION_ASSISTANT.** CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Permit the Users group to the Configuration Assistant profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.CONFIGURATION_ASSISTANT.** CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/* Make changes effective */
Call RacfCmd "SETROPTS RACLST(ZMFAPLA) REFRESH"

/*-----------------------------------------------*/
/* */
/* End Configuration Assistant Setup */
/* */
/*-----------------------------------------------*/
```

Figure 80. Sample RACF commands for configuring the Configuration Assistant plug-in
Commands for configuring the Incident Log plug-in

If your installation has chosen to configure the Incident Log plug-in, the izuconfig1.cfg.rexx exec creates the security definitions for CEA and the other system components used in Incident Log processing. An example of this REXX output is shown in Figure 81 and Figure 82 on page 284.

```/*-----------------------------------------------------------------------*/
/* */
/* Begin Incident Log Setup */
/* */
/*-----------------------------------------------------------------------*/

/* Setup for CIM Providers to use CEA for Incident Log */
/*------------------------------------------------------------------- */
/* Assumption SERVAUTH class is active */
Call RacfCmd "SETROPTS GENERIC(SERVAUTH)"

/* Define the CEA resource profiles required to perform/retrieve */
/* properties for JES. */
Call RacfCmd "RDEFINE SERVAUTH CEA.CEAGETPS UACC(NONE)"
Call RacfCmd "RDEFINE SERVAUTH CEA.CEADOCMD UACC(NONE)"

/* Grant the z/OSMF groups, authority to the following and to grant access */
/* to perform JES operations and obtain job properties. */
Call RacfCmd "PERMIT CEA.CEAGETPS CLASS(SERVAUTH) ID(IZUADMIN) ACCESS(UPDATE)"
Call RacfCmd "PERMIT CEA.CEAGETPS CLASS(SERVAUTH) ID(IZUUSER) ACCESS(UPDATE)"
Call RacfCmd "PERMIT CEA.CEADOCMD CLASS(SERVAUTH) ID(IZUADMIN) ACCESS(UPDATE)"
Call RacfCmd "PERMIT CEA.CEADOCMD CLASS(SERVAUTH) ID(IZUUSER) ACCESS(UPDATE)"

/* Permit z/OSMF groups to Incident Log */
Call RacfCmd "RDEFINE SERVAUTH CEA.CEAPDWB* UACC(NONE)"
Call RacfCmd "RDEFINE SERVAUTH CEA.CEADOCONSOLECMD UACC(NONE)"

/* Activate authority checking for the SERVAUTH class: */
Call RacfCmd "SETROPTS RACLIST(SERVAUTH) CLASSACT(SERVAUTH)"

/* If the SERVAUTH class already active, issue: */
Call RacfCmd "SETROPTS RACLIST(SERVAUTH) REFRESH"

/* If your installation sets up PROTECT-ALL (RACF exit to protect all datasets) */
/* you will need to setup a CEA.* RACF profile and permit user identity. */
/* The HLQ CEA is the CEA HLQ provided during the configuration prompts. */
/* Please ensure the commands are appropriate for your environment. */
/* You may want to consider assigning an owner or group to the data set profile. */
/* The commands is: */
Call RacfCmd "ADDSD 'CEA.*' OWNER(userid or group-name) UACC(NONE)"
Call RacfCmd "ADDSD 'CEA.*' UACC(NONE)"
Call RacfCmd "PERMIT 'CEA.*' ID(IZUADMIN) ACCESS(ALTER)"
Call RacfCmd "PERMIT 'CEA.*' ID(IZUUSER) ACCESS(ALTER)"
Call RacfCmd "SETROPTS GENERIC(DATASET) REFRESH"

Figure 81. Sample RACF commands for configuring the Incident Log plug-in (Part 1 of 2)
/* Additional considerations */
/* If your installation has master catalog setup you may need to permit the */
/* user to the master catalog dataset class. */
/* Call RacfCmd "PERMIT 'your_master_catalog' CLASS(DATASET) ID('your_cim_admin_name') ACCESS(UPDATE)" */
/* Call RacfCmd "SETROPTS GENERIC(DATASET) REFRESH" */

/* If your installation is using SYSLOG for the Operations Log, you may need to */
/* define and permit the CEA user id to JESSPOOL class below. */
/* REDEFINE JESSPOOL 'your_system_name'.MASTER+.SYSLOG.*.* UACC(NONE) */
/* PERMIT 'your_system_name'.MASTER+.SYSLOG.*.* CLASS(JESSPOOL) ID('your_cea_user_id') ACC(ALTER) */
/* SETR RACLIST(JESSPOOL) REFRESH */

/* If your installation protects MVS commands with RACF class OPERCMDS */
/* for the incident log verify step. */
/* This template does not have RDEFINE for these resources. */
/* If your installation doesn't define these, you will need to either define them first */
/* or change the PERMIT to a higher level qualifier. */
/* Call RacfCmd "PERMIT MVS.DISPLAY.** CLASS(OPERCMDS) ID('your_cim_admin_name') ACCESS(READ)" */
/* Call RacfCmd "PERMIT MVS.DUMP CLASS(OPERCMDS) ID('your_cim_admin_name') ACCESS(CONTROL)" */
/* Call RacfCmd "PERMIT MVS.MODIFY.JOB.** CLASS(OPERCMDS) ID('your_cim_admin_name') ACCESS(UPDATE)" */
/* Call RacfCmd "SETROPTS RACLIST(OPERCMDS) REFRESH" */

/* Define the Incident Log profile */
Call RacfCmd "RDEFINE ZMFAPLA BBNBASE.ZOSMF.INCIDENT_LOG.** UACC(NONE)"

/* Permit the Administrators group to the Incident Log profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.INCIDENT_LOG.** CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Permit the User group to the Incident Log profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.INCIDENT_LOG.** CLASS(ZMFAPLA) ID(IZUSER) ACCESS(READ)"

/* Make changes effective */
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"

/*-------------------------------------------------------------------------*/
/* */
/* End Incident Log Setup */
/* */
/*-------------------------------------------------------------------------*/

Figure 82. Sample RACF commands for configuring the Incident Log plug-in (Part 2 of 2)
Commands for configuring the ISPF plug-in

If your installation has chosen to configure the ISPF plug-in, the izuconfig1.cfg.rexx exec includes a section with RACF commands for creating the required security definitions. Figure 83 shows the commands that are created when SAF Authorization Mode has been selected for the configuration.

```/*-----------------------------------------------*/
/* */
/* Begin ISPF Setup */
/* */
/*-----------------------------------------------*/

/* Assumption: SERVAUTH class is active */
/* Call RacfCmd "SETROPTS GENERIC(SERVAUTH)" */

/* Define the CEA resource profile required for ISPF */
Call RacfCmd "RDEFINE SERVAUTH CEA.CEATSO.* UACC(NONE)"

/* Permit the Administrators group to this profile */
Call RacfCmd "PERMIT CEA.CEATSO.* CLASS(SERVAUTH) ID(IZUADMIN) ACCESS(READ)"

/* Permit the Users group to this profile */
Call RacfCmd "PERMIT CEA.CEATSO.* CLASS(SERVAUTH) ID(IZUUSER) ACCESS(READ)"

/* Permit the WAS servant to this profile */
Call RacfCmd "PERMIT CEA.CEATSO.* CLASS(SERVAUTH) ID(WSSRU1) ACCESS(READ)"

/* Make changes effective */
Call RacfCmd "SETROPTS RACLIST(SERVAUTH) REFRESH"

/* Define the ISPF profile */
Call RacfCmd "RDEFINE ZMFAPLA BBNBASE.ZOSMF.ISPF.** UACC(NONE)"

/* Permit the Administrators group to the ISPF profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.ISPF.** CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Permit the Users group to the ISPF profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.ISPF.** CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/* Make changes effective */
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"

/*-----------------------------------------------*/
/* */
/* End ISPF Setup */
/* */
/*-----------------------------------------------*/
```

Figure 83. Sample RACF commands for configuring the ISPF plug-in
Commands for configuring the Resource Monitoring plug-in

If your installation has chosen to configure the Resource Monitoring plug-in, the `izuconfig1.cfg.rexx` exec includes a section with RACF commands for creating the required security definitions. Figure 84 shows the commands that are created when SAF Authorization Mode has been selected for the configuration.

```plaintext
/*-----------------------------------------------------------------------*/
/* */
/* Begin Resource Monitoring Facility Setup */
/* */
/*-----------------------------------------------------------------------*/

/* Define the Resource Monitoring profile */
Call RacfCmd "RDEFINE ZMFAPLA BBNBASE.ZOSMF.RESOURCE_MONITORING.** UACC(NONE)"

/* Permit the Administrators group to the Resource Monitoring profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.RESOURCE_MONITORING.** CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Permit the Users group to the Resource Monitoring profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.RESOURCE_MONITORING.** CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/* Make changes effective */
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"

/*-----------------------------------------------------------------------*/
/* */
/* End Resource Monitoring Facility Setup */
/* */
/*-----------------------------------------------------------------------*/
```

Figure 84. Sample RACF commands for configuring the Resource Monitoring plug-in
Commands for configuring the Software Deployment plug-in

If your installation has chosen to configure the Software Deployment plug-in, the izuconfig1.cfg.rexx exec includes a section with RACF commands for creating the required security definitions. Figure 85 shows the commands that are created when SAF Authorization Mode has been selected for the configuration.

If APARs PM40764 and PM50651 are installed, additional support is provided in the exec for controlling user access to the Deployment task and its objects, as described in “Creating access controls for the Deployment task” on page 86. This support is included in Figure 85.

```bash
/*-----------------------------------------------------------------------*/
/*                                                                   */
/* Begin Software Deployment Setup                                   */
/*                                                                   */
/*-----------------------------------------------------------------------*/

/* Define the Software Deployment profile */
Call RacfCmd "RDEFINE ZMFAPLA BBNBASE.ZOSMF.SOFTWARE_DEPLOYMENT.* UACC(NONE)"

/* Define the Software Deployment profile */
Call RacfCmd "RDEFINE ZMFAPLA BBNBASE.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.* UACC(NONE)"

/* Permit the Administrators group to the Software Deployment profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.SOFTWARE_DEPLOYMENT.* CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Permit the Users group to the Software Deployment profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.SOFTWARE_DEPLOYMENT.* CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/* Permit the Administrators group to the Software Deployment profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.* CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(CONTROL)"

/* Permit the Users group to the Software Deployment profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.* CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(CONTROL)"

/* Make changes effective */
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"

/*-----------------------------------------------------------------------*/
/*                                                                   */
/* End Software Deployment Setup                                    */
/*                                                                   */
/*-----------------------------------------------------------------------*/
```

Figure 85. Sample RACF commands for configuring the Software Deployment plug-in
Commands for configuring the Workload Management plug-in

Figure 86 shows an example of the REXX file created for configuring security for the Workload Management plug-in.

```
/*-----------------------------------------------------------------------*/
/* */
/* Begin Workload Management Setup */
/* */
 /*-----------------------------------------------------------------------*/
/* Define Workload Management facility */
/* The following commented command is to be issued only if the profile does not exist */
/* It normally would have been created during z/OS setup */
/* Call RacfCmd "RDEFINE FACILITY MVSADMIN.WLM.POLICY UACC(NONE)" */

/* Permit the Workload Management group */
Call RacfCmd "PERMIT MVSADMIN.WLM.POLICY CLASS(FACILITY) ID(WLMGRP) ACCESS(UPDATE)"

/* Make changes effective */
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"

/* Connect the z/OSMF Administrator UserID to the Workload Management group */
Call RacfCmd "CONNECT ZOSMFAD GROUP(WLMGRP)"

/* Define the Workload Management profiles */
Call RacfCmd "RDEFINE ZMFAPLA BBNBASE.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.VIEW UACC(NONE)"
Call RacfCmd "RDEFINE ZMFAPLA BBNBASE.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.MODIFY UACC(NONE)"
Call RacfCmd "RDEFINE ZMFAPLA BBNBASE.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.INSTALL UACC(NONE)"

/* Permit the Administrators group to all the Workload Management profiles */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.VIEW CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT BBNBASE.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.MODIFY CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT BBNBASE.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.INSTALL CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Permit the Users group to only the Workload Management VIEW profile */
Call RacfCmd "PERMIT BBNBASE.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.VIEW CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/* Make changes effective */
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"

/*-----------------------------------------------------------------------*/
/* */
/* End Workload Management Setup */
/* */
/*-----------------------------------------------------------------------*/
```
Appendix J. Format of the installation verification program report

When you use the izusetup.sh script to verify the system setup for the Incident Log task, the installation verification program (IVP) report is created. For your reference, this section shows the format of the IVP report.

For a description of the IVP report, see “Reviewing the results of the izuincidentlogverify.report file” on page 162.

The format of the IVP report is shown in Figure 87 and Figure 88 on page 290.

```rexx
/* rexx */
/* Licensed Materials - Property of IBM */
/* 5655-S2B */
/* Copyright IBM Corp. 2009, 2010 */
/* */
/* Status = HSMA120 */
/* */
/* ------------------------------------------------------------------ */

--------------------------------
Incident Log Verification Report
--------------------------------

To verify the configuration of the Incident Log task, z/OSMF creates a test SVC dump on the system and performs a series of tests on the test dump. For each test, this report shows either "SUCCESS" or an error message. For information about the errors and corrective actions you can take, see the Troubleshooting chapter of IBM z/OS Management Facility User's Guide, SA38-0652. Each error message corresponds to a possible cause and one or more corrective actions for the problems described by this report.

The following section describes key dependencies for the Incident Log task. A value of "SUCCESS" indicates that the dependency is configured and active on the system.

Sysplex Dump Directory : SDDIR_RESULT
CEA : CEA_RESULT
System REXX : SYSREXX_RESULT
System Logger Active : LOGGER_VALUE

Diagnostic Data Results

Four diagnostic data objects are associated with an incident:
The SVC dump and three "log snapshots". A value of "SUCCESS" indicates that the diagnostic objects were found for the incident. Identified errors are described in the Troubleshooting chapter of z/OSMF User's Guide.

SVCdump : DUMP_RESULT
Operations Log : OPERLOG_RESULT
Error Log : ERRORLOG_RESULT
Error Log Summary : ERRORLOGSUMMARY_RESULT

Incident Log Operations Results

Each diagnostic object is "prepared", that is, formatted and tersed. Usually, each diagnostic object is prepared before the incident is sent to IBM through FTP. A value of "SUCCESS" indicates that the diagnostic information was prepared successfully. Identified errors are described in the Troubleshooting chapter of z/OSMF User's Guide.

-- Figure 87. Format of the installation verification program report (Part 1 of 2) --
The common event adapter (CEA) component of z/OS captures diagnostic data objects. The following section describes the relevant properties in the active CEAPRMxx parmlib member. Identified errors are described in the Troubleshooting chapter of z/OSMF User's Guide.

- **SnapShot**: SNAPSHOT_VALUE
- **Branch**: BRANCH_VALUE
- **Country**: COUNTRY_VALUE
- **Storage Value**: STORAGE_VALUE
- **HLQ**: HLQ_VALUE
- **SLIP OperLog time**: SLIP_OPERLOG_VALUE
- **SLIP LOGREC time**: SLIP_LOGREC_VALUE
- **SLIP LOGRECSUMMARY time**: SLIP_LOGRECSUMMARY_VALUE
- **DUMP OperLog time**: DUMP_OPERLOG_VALUE
- **DUMP LOGREC time**: DUMP_LOGREC_VALUE
- **DUMP LOGRECSUMMARY time**: DUMP_LOGRECSUMMARY_VALUE
- **ABEND OperLog time**: ABEND_OPERLOG_VALUE
- **ABEND LOGREC time**: ABEND_LOGREC_VALUE
- **ABEND LOGRECSUMMARY time**: ABEND_LOGRECSUMMARY_VALUE

---

**Incident Log Logstreams Properties**

OPERLOG and sysplex logrec diagnostic snapshots are written to system logger log streams. The following section describes the log stream properties expected to be active on the system. Identified errors are described in the Troubleshooting chapter of z/OSMF User's Guide.

- **Operations Log**: OPERLOG_DESTINATION_VALUE
- **Logrec**: LOGREC_MEDIUM_VALUE
- **LOGR Subsystem Active**: LOGR_SUBSYSTEM_VALUE
- **Primary Logger CDS**: PRIMARY_LOGGER_CDS_VALUE
- **Alternate Logger CDS**: ALTERNATE_LOGGER_CDS_VALUE
- **Number of LSR for Primary CDS**: LSR_VALUE
- **CEA OperLog Logstream Model**: CEA_OPERLOG_VALUE
- **CEA Logrec Logstream Model**: CEA_LOGREC_VALUE

---

**Sysplex Dump Directory Properties**

The sysplex dump directory contains the inventory of SVC dumps that are described by z/OSMF incidents. The following section describes the sysplex dump directory that is active on the z/OS system. Identified errors are described in the Troubleshooting chapter of z/OSMF User's Guide.

- **Name**: SDDIR_NAME
- **Size**: SDDIR_SIZE
- **On Shared Volume**: SDDIR_SHARED
- **Free Space Available**: SDDIR_FULL
- **IPCS Initialized**: SDDIR_IPCS

---

Figure 88. Format of the installation verification program report (Part 2 of 2)
Appendix K. Example of the migration report

When you use the izumigration.sh script to migrate your configuration file to the latest format, the script creates a report file named izumigration.report. The report file records the actions that were taken to migrate your configuration and override files—the settings that have been modified, removed, or added between releases. For your reference, this section shows a sample of the migration report file.

The following example shows the major sections of the migration report file. In this example, the report file records the results of updating the configuration file and the override file from the z/OSMF V1R12 format to the z/OSMF V1R13 format. The sample migration report is presented in a multi-part figure, as follows:

- Figure 89 on page 292
- Figure 90 on page 293
- Figure 91 on page 294
- Figure 92 on page 295
Invocation command: /usr/lpp/zosmf/V1R13/bin/izumigrate.sh -file /config/v1r12.cfg -overridefile /config/v1r12.ovr

User ID: IBMUSER
Date: 06.09.11
Time: 11.02.28

The following environment variables were in effect during the creation of this report file:

IZU_CODE_ROOT=/usr/lpp/zosmf/V1R13
IZU_CONFIG_DIR=/etc/zosmf
IZU_LOGFILE_DIR=/var/zosmf/configuration/logs

Configuration File Processing

Previous configuration file was saved as: "/config/v1r12.cfg.V1R12"

Updated configuration file was created as: "/config/v1r12.cfg"

The complete list of properties contained in the default configuration file for the current release of z/OSMF are:

IZU_CONFIG_FILE_VERSION=1.13.0
IZU_DATA_DIR=/var/zosmf/data
IZU_DATA_FS_NAME=IZU.SIZUDATA
IZU_DATA_FS_TYPE=ZFS
IZU_DATA_FS_VOLUME='v'
IZU_DATA_FS_SIZE=200
IZU_AUTHORIZATION_MODE=SAF
IZU_AUTOUID_OVERRIDENO.DEFAULT.VALUE
IZU_AUTOGID_OVERRIDENO.DEFAULT.VALUE
IZU_ADMIN_GROUP_NAME=IZUADMIN
IZU_ADMIN_GROUP_GID=9003
IZU_USERS_GROUP_NAME=IZUUSER
IZU_USERS_GROUP_GID=9004
IZU_ADMIN_NAME=ZOSMFAD
IZU_ADMIN_UID=9001
IZU_ADMIN_HOME=/u/zosmfad
IZU_ADMIN_PROGRAM=/bin/sh
IZU_ADMIN_PROCNO.DEFAULT.VALUE
IZU_ADMIN_ACCOUNTNO.DEFAULT.VALUE
IZU_WAS_CONFIG_FILE_KNOWN=Y
IZU_WAS_CONFIG_FILE_LOCATION=/etc/zWebSphereOEM/V7R0/conf/CONFIG1/CONFIG1.responseFile
IZU_APPSERVER_GROUP=WSCFG1
IZU_APPSERVER_ROOT=/zWebSphereOEM/V7R0/config1
IZU_WAS_PROFILE_PREFIX=BBNBASE
IZU_CLUSTER_TRANSITION_NAME=BBNC001
IZU_CELL_SHORT_NAME=BBNBASE
IZU_SERVANT_USERID=WSSRU1
IZU_CONTROL_USERID=WSCRU1
IZU_ORB_PORT=32203
IZU_HTTP_SSL_PORT=32208
IZU_APPSERVER_HOSTNAME=NO.DEFAULT.VALUE
IZU_WBEM_ROOT=/usr/lpp/wbem
IZU_IL_CONFIGURENO.DEFAULT.VALUE
IZU_CA_CONFIGURENO.DEFAULT.VALUE
IZU_WLM_CONFIGURENO.DEFAULT.VALUE
IZU_RMF_CONFIGURENO.DEFAULT.VALUE
IZU_DM_CONFIGURENO.DEFAULT.VALUE
IZU_WISPF_CONFIGURENO.DEFAULT.VALUE
IZU_IL_CEA_CONFIGURENO.DEFAULT.VALUE
IZU_CEA_HLQ='CEA'
IZU_COUNTRY_CODE=NO.DEFAULT.VALUE
IZU_BRANCH_CODE=NO.DEFAULT.VALUE
IZU_STORAGE_VALUE=NO.DEFAULT.VALUE
IZU_CEAPRM_SOURCE_PARMLIB=SYS1.PARMLIB
IZU_CEAPRM_TARGET_PARMLIB=SYS1.PARMLIB

Figure 89. Sample migration report file (Part 1 of 4)
IZU_IEADMC_SOURCE_PARMLIB=SYS1.SAMPLIB
IZU_IEADMC_TARGET_PARMLIB=SYS1.PARMLIB
IZU_CEA_PARM_NAME=01
IZU_IEA_PARM_NAME=ZM
IZU_WLM_GROUP_NAME=WLMGRP
IZU_CP_QUERY_GROUP_NAME=CPOQUERY
IZU_CP_CONTROL_GROUP_NAME=CPOCTRL
IZU_CIM_ADMIN_GROUP_NAME=CFZADMGP
IZU_CIM_USER_GROUP_NAME=CFZUSRGP
IZU_ADMIN_GROUP=ZOSMFGRP
IZU_ADMIN_REGION=2096128
IZU_CONFIG_DIR=/etc/zosmf
IZU_CEA_GROUP_NAME=CEAGP
IZU_CEA_GROUP_ID=6321
IZU_PARMLIB=HDENNIS.ZOS17.PARMLIB
IZU_PARMLIB_SOURCE=HDENNIS.ZOS17.PARMLIB
IZU_CIM_CONFIGURE=Y
IZU_CIM_SERVER_GROUP_NAME=CFZSRVGP
IZU_CIM_SERVER_GROUP_GID=9501
IZU_CIM_ADMIN_GROUP_GID=9502
IZU_CIM_USER_GROUP_GID=9503
IZU_CIM_SERVER_GID=9504
IZU_CIM_SERVER_ID=CFZSRV
IZU_CIM_SERVER_HOME=/u/cfzsrv
IZU_CIM_SERVER_PROGRAM=/bin/sh
IZU_WLM_GROUP_GID=9600

/**---------------------------------------------------------------------*/
/**---------------------------------------------------------------------*/
Removed Properties

The following properties are removed from the updated configuration file. These properties are no longer supported in the current release of z/OSMF. In the list below, each property is shown with its value as specified in the previous configuration file. This value is either an installation supplied value, if one was specified, or the IBM default value.

IZU_ADMIN_GROUP=ZOSMFGRP
IZU_ADMIN_REGION=2096128
IZU_CONFIG_DIR=/etc/zosmf
IZU_CEA_GROUP_NAME=CEAGP
IZU_CEA_GROUP_ID=6321
IZU_PARMLIB=HDENNIS.ZOS17.PARMLIB
IZU_PARMLIB_SOURCE=HDENNIS.ZOS17.PARMLIB
IZU_CIM_CONFIGURE=Y
IZU_CIM_SERVER_GROUP_NAME=CFZSRVGP
IZU_CIM_SERVER_GROUP_GID=9501
IZU_CIM_ADMIN_GROUP_GID=9502
IZU_CIM_USER_GROUP_GID=9503
IZU_CIM_SERVER_GID=9504
IZU_CIM_SERVER_ID=CFZSRV
IZU_CIM_SERVER_HOME=/u/cfzsrv
IZU_CIM_SERVER_PROGRAM=/bin/sh
IZU_WLM_GROUP_GID=9600

Added Properties

The following properties are added to the updated configuration file. These properties are new for z/OSMF since the time of your last configuration. In the list below, each property is shown with its IBM default value, unless a value from your previous configuration applies to an added property. In this case, your value is used in its place.

IZU_AUTHORIZATION_MODE=REPOSITORY
IZU_AUTOUID_OVERRIDE=NO.DEFAULT.VALUE
IZU_AUTOGID_OVERRIDE=NO.DEFAULT.VALUE
IZU_ADMIN_GROUP_NAME=ZOSMFGRP
IZU_USERS_GROUP_NAME=IZUUSER
IZU_USERS_GROUP_GID=9004
IZU_CIM_CONFIGURE=NO.DEFAULT.VALUE
IZU_DM_CONFIGURE=NO.DEFAULT.VALUE
IZU_WISPF_CONFIGURE=NO.DEFAULT.VALUE
IZU_CEA_HLQ='CEA'
IZU_CEAPRM_SOURCE_PARMLIB=HDENNIS.ZOS17.PARMLIB
IZU_CEAPRM_TARGET_PARMLIB=HDENNIS,ZOS17.PARMLIB
IZU_IEADMC_SOURCE_PARMLIB=SYS1.SAMPLIB
IZU_IEADMC_TARGET_PARMLIB=HDENNIS,ZOS17.PARMLIB
IZU_CP_QUERY_GROUP_NAME=CPOQUERY
IZU_CP_CONTROL_GROUP_NAME=CPOCTRL

Updated Properties

The following properties have been updated in the configuration file for the current release.

IZU_CONFIG_FILE_VERSION=1.13.0
IZU_DATA_FS_SIZE=200

/**---------------------------------------------------------------------*/
/**---------------------------------------------------------------------*/

The migration of the configuration file has completed.

Figure 90. Sample migration report file (Part 2 of 4)
Override File Processing

Previous override file was saved as: "/config/v1r12.ovr.V1R12"

Updated override file was created as: "/config/v1r12.ovr"

The complete list of properties contained in the default override file for the current release of z/OSMF are:

IZU_OVERRIDE_FILE_VERSION=1.13.0
IZU_DATA_DIR=/var/zosmf/data
IZU_DATA_FS_NAME=IZU.SIZUDATA
IZU_DATA_FS_TYPE=ZFS
IZU_DATA_FS_VOLUMES="*"
IZU_DATA_FS_SIZE=200
IZU_AUTHORIZATION_MODE=SAF
IZU_AUTOUID_OVERRIDE=NO.DEFAULT.VALUE
IZU_AUTOGID_OVERRIDE=NO.DEFAULT.VALUE
IZU_ADMIN_GROUP_NAME=IZUADMIN
IZU_ADMIN_GROUP_GID=9003
IZU_USERS_GROUP_NAME=IZUUSER
IZU_USERS_GROUP_GID=9004
IZU_ADMIN_NAME=ZOSMFAD
IZU_ADMIN_UID=9001
IZU_ADMIN_HOME=/u/zosmfad
IZU_ADMIN_PROGRAM=/bin/sh
IZU_ADMIN_PROC=NO.DEFAULT.VALUE
IZU_ADMIN_ACCOUNT=NO.DEFAULT.VALUE
IZU_WAS_CONFIG_FILE_KNOWN=Y
IZU_WAS_CONFIG_FILE_LOCATION=/etc/zWebSphereOEM/V7R0/conf/CONFIG1/CONFIG1.responseFile
IZU_IL_CONFIGURE=NO.DEFAULT.VALUE
IZU_CP_CONFIGURE=NO.DEFAULT.VALUE
IZU_WLM_CONFIGURE=NO.DEFAULT.VALUE
IZU_RMF_CONFIGURE=NO.DEFAULT.VALUE
IZU_DM_CONFIGURE=NO.DEFAULT.VALUE
IZU_WISPF_CONFIGURE=NO.DEFAULT.VALUE
IZU_IL_CEA_CONFIGURE=Y
IZU_CEA_HLQ='CEA'
IZU_COUNTRY_CODE=NO.DEFAULT.VALUE
IZU_BASED_CODE=NO.DEFAULT.VALUE
IZU_STORAGE_VALUE=NO.DEFAULT.VALUE
IZU_CEAPRM_SOURCE_PARMLIB=SYS1.PARMLIB
IZU_CEAPRM_TARGET_PARMLIB=SYS1.PARMLIB
IZU_IEADMC_SOURCE_PARMLIB=SYS1.SAMPLIB
IZU_IEADMC_TARGET_PARMLIB=SYS1.PARMLIB
IZU_CEA_PARM_NAME=01
IZU_IA_PARM_NAME=ZM
IZU_WLMGROUP_NAME=WLMGRP
IZU_CP_QUERY_GROUP_NAME=CPOQUERY
IZU_CP_CONTROL_GROUP_NAME=CPOCTRL
IZU_CIMADMIN_GROUP_NAME=CFZADMGP
IZU_CIMUSER_GROUP_NAME=CFZUSRGP

If a property was removed from the current release of z/OSMF and it was found in your override file, the migration process will remove that property from your override file.

If a property has been added to the current release of z/OSMF and it corresponds to a property in your override file, that property will be added to your override file with your existing value.

Figure 91. Sample migration report file (Part 3 of 4)
Removed Properties

The following properties have been removed from the override file for the current release and are no longer supported. The properties are displayed with their default values unless a corresponding value was found in your override file. In this case, your value is used in its place.

IZU_CONFIG_DIR=/etc/zosmf
IZU_ADMIN_GROUP=ZOSMFGRP
IZU_ADMIN_REGION=2096128
IZU_CEA_GROUP_NAME=CEAGP
IZU_CEA_GROUP_ID=6321
IZU_PARMLIB=SYS1.PARMLIB
IZU_PARMLIB_SOURCE=SYS1.PARMLIB
IZU_CIM_CONFNAME=C
IZU_CIM_SERVER_GROUP_NAME=CFZSRVGP
IZU_CIM_SERVER_GROUP_GID=9501
IZU_CIM_ADMIN_GROUP_GID=9502
IZU_CIM_USER_GROUP_GID=9503
IZU_CIM_SERVER_ID=CFZSRV
IZU_CIM_SERVER_HOME=/u/cfzsrv
IZU_WLM_GROUP_GID=9600
IZU_CIM_SERVER_PROGRAM=/bin/sh
IZU_WLM_GROUP_GID=9600

Added Properties

The following properties have been added to the override file for the current release. The properties are displayed with their default values unless a corresponding value was found in your override file. In this case, your value is used in its place.

IZU_AUTHORIZATION_MODE=SAF
IZU_AUTUID_OVERRIDE=NO.DEFAULT.VALUE
IZU_AUTOGID_OVERRIDE=NO.DEFAULT.VALUE
IZU_ADMIN_GROUP_NAME=ZOSMFGRP
IZU_USERS_GROUP_NAME=IZUUSER
IZU_CP_CONFIGURE=NO.DEFAULT.VALUE
IZU_DM_CONFIGURE=NO.DEFAULT.VALUE
IZU_CP_QUERY_GID=9004
IZU_CP_QUERY_NAME=CPOQUERY
IZU_CP_CONTROL_NAME=CPOCTRL
IZU_WLM_CONFIGURE=NO.DEFAULT.VALUE
IZU_CEAPRM_SOURCE_PARMLIB=SYS1.PARMLIB
IZU_CEAPRM_TARGET_PARMLIB=SYS1.PARMLIB
IZU_IEADMC_SOURCE_PARMLIB=SYS1.SAMPLIB
IZU_CEAPRM_TARGET_PARMLIB=SYS1.PARMLIB
IZU_CP_QUERY_GROUP_NAME=CPOQUERY
IZU_CP_CONTROL_GROUP_NAME=CPOCTRL

Updated Properties

The following properties have been updated in the override file for the current release:

IZU_OVERRIDE_FILE_VERSION=1.13.0
IZU_DATA_FS_SIZE=200

The migration of the override file has completed.
Appendix L. Accessibility

Publications for this product are offered in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when using PDF files, you may view the information through the z/OS Internet Library Web site or the z/OS Information Center. If you continue to experience problems, send an e-mail to mhvrdfs@us.ibm.com or write to:

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Mail Station P181
2455 South Road
Poughkeepsie, NY 12601-5400
U.S.A.

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/OSMF 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/OSMF. Consult the assistive technology documentation for specific information when using such products to access z/OSMF interfaces.

Keyboard shortcuts

This topic describes the keyboard shortcuts that you can use to navigate within z/OSMF.

The keyboard shortcuts are described in the following sections:

- “Panes”
- “Tabs” on page 298
- “Trees” on page 298
- “Tables” on page 298
- “Other interface controls” on page 299

Panes

<table>
<thead>
<tr>
<th>Action</th>
<th>Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to splitters for resizable panes</td>
<td>Tab</td>
</tr>
<tr>
<td>Change the size of a vertical pane</td>
<td>Left Arrow, Right Arrow</td>
</tr>
<tr>
<td>Change the size of a horizontal pane</td>
<td>Up Arrow, Down Arrow</td>
</tr>
</tbody>
</table>
Tabs

Table 54. Keyboard shortcuts for tabs

<table>
<thead>
<tr>
<th>Action</th>
<th>Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the next tab</td>
<td>Right Arrow</td>
</tr>
<tr>
<td>Navigate to the previous tab</td>
<td>Left Arrow</td>
</tr>
<tr>
<td>Navigate into a page</td>
<td>Tab</td>
</tr>
<tr>
<td>Navigate to the next page</td>
<td>Ctrl+Page Down</td>
</tr>
<tr>
<td>Navigate to the previous page</td>
<td>Ctrl+Page Up</td>
</tr>
<tr>
<td>Close a tab</td>
<td>Delete</td>
</tr>
</tbody>
</table>

Trees

Table 55. Keyboard shortcuts for trees

<table>
<thead>
<tr>
<th>Action</th>
<th>Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the first tree item</td>
<td>Tab</td>
</tr>
<tr>
<td>Navigate to the next sibling</td>
<td>Down Arrow</td>
</tr>
<tr>
<td>Navigate to the previous sibling</td>
<td>Up Arrow</td>
</tr>
<tr>
<td>Open a subtree</td>
<td>Right Arrow</td>
</tr>
<tr>
<td>Close a subtree</td>
<td>Left Arrow</td>
</tr>
<tr>
<td>Activate a tree item</td>
<td>Enter</td>
</tr>
</tbody>
</table>

Tables

Table 56. Keyboard shortcuts for tables

<table>
<thead>
<tr>
<th>Action</th>
<th>Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate between sections of the table</td>
<td>Tab</td>
</tr>
<tr>
<td>Navigate between column headers</td>
<td>Left Arrow, Right Arrow</td>
</tr>
<tr>
<td>Navigate to links in the column header</td>
<td>Right Arrow</td>
</tr>
<tr>
<td>Activate a link in the column header</td>
<td>Enter</td>
</tr>
<tr>
<td>Sort a column using the column header</td>
<td>Enter</td>
</tr>
<tr>
<td>Navigate between table cells</td>
<td>Left Arrow, Right Arrow, Up Arrow, Down Arrow, Page Up, Page Down</td>
</tr>
<tr>
<td>Navigate between items in the table toolbar</td>
<td>Tab, Shift+Tab</td>
</tr>
<tr>
<td>Activate an item in the table toolbar</td>
<td>Enter</td>
</tr>
<tr>
<td>Select a row</td>
<td>Spacebar</td>
</tr>
<tr>
<td>Open a context menu</td>
<td>Shift+F10</td>
</tr>
<tr>
<td>Move between menu items</td>
<td>Up Arrow, Down Arrow</td>
</tr>
<tr>
<td>Activate a menu item</td>
<td>Spacebar, Enter</td>
</tr>
<tr>
<td>Close a context menu</td>
<td>Esc</td>
</tr>
<tr>
<td>Activate a search</td>
<td>Enter</td>
</tr>
<tr>
<td>Modify the data in an editable cell</td>
<td>F2, Enter</td>
</tr>
<tr>
<td>Accept the value entered into an editable cell</td>
<td>Enter</td>
</tr>
<tr>
<td>Discard the value entered into an editable cell</td>
<td>Esc</td>
</tr>
</tbody>
</table>
### Table 56. Keyboard shortcuts for tables (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expand a node in a tree table</td>
<td>Ctrl+Right Arrow</td>
</tr>
<tr>
<td>Collapse a node in a tree table</td>
<td>Ctrl+Left Arrow</td>
</tr>
<tr>
<td>Display the message for a table cell</td>
<td>Ctrl+M</td>
</tr>
<tr>
<td>Display the message for an editable table cell</td>
<td>Ctrl+click</td>
</tr>
<tr>
<td>Display the help for a message in a table cell</td>
<td>Ctrl+Q</td>
</tr>
</tbody>
</table>

### Other interface controls

**Table 57. Keyboard shortcuts for other interface controls**

<table>
<thead>
<tr>
<th>Action</th>
<th>Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select or deselect a check box</td>
<td>Spacebar</td>
</tr>
<tr>
<td>Select a radio button</td>
<td>Spacebar</td>
</tr>
<tr>
<td>Display the help for a message in a text entry field</td>
<td>Ctrl+Q</td>
</tr>
<tr>
<td>Close a window</td>
<td>Esc</td>
</tr>
<tr>
<td>Activate a button</td>
<td>Enter, Spacebar</td>
</tr>
<tr>
<td>Modify the number spinner value by a single increment</td>
<td>Up Arrow, Down Arrow</td>
</tr>
<tr>
<td>Modify the number spinner value by 10 increments</td>
<td>Page Up, Page Down</td>
</tr>
<tr>
<td>Open pull down menus</td>
<td>Down Arrow</td>
</tr>
<tr>
<td>Navigate through pull down menus</td>
<td>Up Arrow, Down Arrow</td>
</tr>
<tr>
<td>Select a menu option</td>
<td>Enter</td>
</tr>
<tr>
<td>Close the menu</td>
<td>Esc</td>
</tr>
</tbody>
</table>

### Customizing your browser display attributes

If you choose to change the text size, be aware that text-only zooming can cause web content to display incorrectly. When you zoom text, you do not change the size of the browser window. As a result, the amount of information that can be displayed changes, with less information displayed as the text size increases.

Text-only zooming can also adversely affect the format of the information displayed in your browser.

### z/OSMF information

z/OSMF information is accessible using screen readers with the BookServer/Library Server version of this book in the Internet library at:

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  
U.S.A

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan, Ltd.  
1623-14, Shimotsuruma, Yamato-shi  
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

Site Counsel  
IBM Corporation  
2455 South Road  
Poughkeepsie, NY 12601-5400  
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

**Policy for unsupported hardware**

Various z/OS elements, such as DFSMS, HCD, JES2, JES3, and MVS, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

**Programming interface information**

This information documents intended programming interfaces that allow the customer to write programs to obtain the services of z/OS or IBM z/OS Management Facility.
Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [http://www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Intel is a trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names might be trademarks or service marks of others.
Glossary of terms and abbreviations

This glossary defines technical terms and abbreviations used in z/OSMF help information. If you do not find the term you are looking for, refer to the IBM Glossary of Computing Terms.

The following cross-references are used in this glossary:

- **Contrast with:** This refers to a term that has an opposed or substantively different meaning.
- **See:** This refers the reader to (a) a related term, (b) a term that is the expanded form of an abbreviation or acronym, or (c) a synonym or more preferred term.
- **Synonym for:** This indicates that the term has the same meaning as a preferred term, which is defined in its proper place in the glossary.
- **Synonymous with:** This is a reference from a defined term to all other terms that have the same meaning.
- **Obsolete term for:** This indicates that the term should not be used and refers the reader to the preferred term.

This glossary includes terms and definitions from American National Standard Dictionary for Information Systems, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Definitions are identified by an asterisk (*) that appears between the term and the beginning of the definition; a single definition taken from ANSI is identified by an asterisk after the item number for that definition.

A

abend  See abnormal end.

abnormal end
   The termination of a task, job, or subsystem because of an error condition that recovery facilities cannot resolve during execution.

active service policy
   In the Workload Management task, the service policy that WLM uses to manage the workload on the system.

AIX
   A UNIX operating system developed by IBM that is designed and optimized to run on POWER® microprocessor-based hardware such as servers, workstations, and blades.

allow next dump
   In the Incident Log task, the option to have dump analysis and elimination (DAE) take and report the next dump that occurs for the same symptoms.

alphabetic character
   A letter or other symbol, excluding digits, used in a language.

alphanumeric character
   Character set composed of uppercase and lowercase letters and numbers, not symbols.

APF
   Authorized program facility.

APF-authorized
   Pertaining to a program that is authorized by the authorized program facility (APF) to access restricted functions, such as supervisor calls (SVC) or SVC paths.

application environment
   In the Workload Management task, a group of application functions requested by a client that execute in server address spaces.

authentication
   Verification of the identity of a user or the user’s eligibility to access an object.

automatic control
   In the Workload Management task, a method of managing application environments. Under automatic control, the name of the startup JCL procedure has been defined for an application environment, giving WLM the ability to automatically start server address spaces. Contrast with manual control.

B

batch job
   A predefined group of processing actions
submitted to the system to be performed with little or no interaction between the user and the system.

catalog
A directory of files and libraries, with reference to their locations.

category
A group of related z/OSMF tasks. Each task in a category allows you to address some aspect of the category.

In the Deployment task, a grouping of deployments and software instances that are related in some way. For example, software instances used by a particular business unit might be included in a single category.

catalog
A directory of files and libraries, with reference to their locations.

class
An object that contains specifications, such as priority, maximum processing time, and maximum storage, to control the runtime environment of a job.

Parameter on the JCL JOB statement that specifies the class or group to which to assign a job. Assigning jobs to a class helps to:

- Achieve a balance between different types of jobs. A good balance of job class assignments helps to make the most efficient use possible of the system.
- Avoid contention between jobs that use the same resources.

class file
A compiled Java source file.

classification
In the Workload Management task, the first level qualifier in the classification rules. A classification specifies the subsystem type that receives the work request and contains all of the classification rules for that subsystem.

classification rules
In the Workload Management task, the rules WLM and subsystems use to assign a service class and, optionally, a report class to a work request.

client
A system or process that is dependent on another system or process (usually called the server) to provide it with access to data, services, programs, or resources. Contrast with server.

code page
A particular assignment of code points to graphic characters. Within a given code page, a code point can have only one specific meaning. A code page also identifies how undefined code points are handled.

A specification of code points from a defined encoding structure for each graphic character in a set or in a collection of graphic character sets. Within a code page, a code point can have only one specific meaning.

common event adapter (CEA)
A z/OS component that enables the delivery of z/OS management data to clients, such as the CIM server.

Common Information Model (CIM)
An implementation-neutral, object-oriented schema for describing network management information. The Distributed Management Task Force (DMTF) develops and maintains CIM specifications.

An open standard for systems management that defines the exchange of information between managed elements such as systems, networks, applications, and services.

Common Information Model Object Manager (CIMOM)
The common conceptual framework for data management that receives, validates, and authenticates the Common Information Model (CIM) requests from
the client application. It then directs the requests to the appropriate component or service provider. Synonymous with Common Information Model server.

**Common Information Model server (CIM server)**

Software, such as OpenPegasus, that allows use of the CIM standard on a system.

An object management engine that exists between the managed system and the management product. z/OSMF interacts with the CIM server (or similar technology) through a layer that converts the data from the CIM model to a format useable by the z/OSMF tasks. Synonymous with Common Information Model Object Manager.

**component**

A set of modules that performs a major function within a system.

**component ID**

Alphanumeric identifier that uniquely identifies the z/OS component.

**content area**

In a Web page that is based on a page template, the editable region of the page.

Area of the z/OSMF browser interface (the central pane) in which data for the active task is displayed.

**core functions**

The base functions of z/OSMF. These functions are enabled when z/OSMF is installed and configured.

**couple data set (CDS)**

A data set that contains information related to a sysplex, its systems, cross-system coupling facility (XCF) groups, and their members. See also *sysplex couple data set* and *WLM couple data set*.

**coupling facility**

A special logical partition that provides high-speed caching, list processing, and locking functions in a sysplex.

**CPU**

See *central processing unit*.

**CPU service units**

A measure of the task control block (TCB) execution time multiplied by an SRM constant which is CPU model dependent.

**Custom-built Product Delivery Option (CBPDO)**

A software delivery package consisting of uninstalled products and unintegrated service. Installation requires the use of SMP/E. CBPDO is one of the two entitled methods for installing z/OS; the other method is ServerPac.

**D**

**data set**

A named collection of related data records that is stored and retrieved by an assigned name. Equivalent to a file in other operating systems.

**data type**

The type of object associated with an incident, such as a dump or log.

**DDS**

See *RMF Distributed Data Server*.

**deploy**

To install software into an operational environment.

**deployment**

In the Deployment task, a checklist that guides you through the software deployment process, and the object in which z/OSMF stores your input and any output generated for each step in the checklist.

**description**

See *incident description*.

**destination**

Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent. See *FTP destination*.

**diagnostic**

Pertaining to the detection and isolation of an error.

**diagnostic data**

The collected information for an incident, such as dumps, OPERLOG, the logrec data set, and the logrec summary.

**diagnostic details**

Properties of an incident. The details include additional information about an incident and a list of the diagnostic data collected for the incident.
DNS  See Domain Name System.

domain name server  
In the Internet suite of protocols, a server program that supplies name-to-address translation by mapping domain names to IP addresses.

Domain Name System (DNS)  
The distributed database system that maps domain names to IP addresses.

dump analysis and elimination (DAE)  
A z/OS service that enables an installation to suppress SVC dumps and ABEND SYSUDUMP dumps that are not needed because they duplicate previously written dumps.

duration  
In the Workload Management task, the amount of service (in service units) that the work can consume before it is switched to the goals of the next period.

dynamic alias management  
In the Workload Management task, an option that you can specify within the service definition details to indicate whether WLM is to dynamically reassign alias addresses to parallel access volumes based on performance goals. When enabled, WLM dynamically reassigns alias addresses from one base to another to help work meet its goals and to minimize I/O subsystem (IOS) queueing.

E  

Electronic Technical Response (ETR)  
See problem management record.

Environmental Record Editing and Printing (EREP)  
The program that formats and prepares reports from the data contained in the error recording data set.

EREP  See Environmental Record Editing and Printing.

error  
A discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition. The smallest detectable anomaly or exception that can occur in an information system. Errors may be caused by hardware, software, internal code, media, or external causes, for example, people or environmental abnormalities.

error log  
A data set or file that is used to record error information about a product or system. See logrec.

error message  
An indication that an error has been detected.

error summary  
A summary log of system errors. This log corresponds to a logrec summary report.

F  

file permission bits  
In z/OS UNIX, information about a file that is used, along with other information, to determine if a process has read, write, or execute/search permission to a file or directory. The bits are divided into three parts, which are owner, group, and other.

firewall  
A network configuration, usually both hardware and software, that prevents unauthorized traffic into and out of a secure network.

An intermediate server that functions to isolate a secure network from an insecure network.

fixed-length record  
A record having the same length as all other records with which it is logically or physically associated. Contrast with variable-length record.

FTP  
See File Transfer Protocol.

File Transfer Protocol (FTP)  
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

FTP data file  
See FTP.DATA file.

FTP destination  
Object that specifies the settings required for an FTP client to connect to the FTP server on a system and download or upload files.
FTP job
A job running on z/OS that sends incident-related information to an FTP destination.

FTP job status
The state of the FTP job. For more details about the status of an FTP job, see the FTP job status details help topic.

FTP profile
Object that specifies the settings required for z/OSMF to gain access to an FTP destination through an organization’s FTP firewall or proxy.

FTP.DATA file
In z/OSMF, an installation-defined data set or UNIX file that is used to override the default system FTP configuration.

G
GDG  See generation data group.
GDS  See generation data set.

generation data group (GDG)
A chronological collection of historically related data sets that do not use the virtual storage access method (VSAM); each data set is called a generation data set.

generation data set (GDS)
One of the data sets in a generation data group (GDG); a GDS is historically related to the other data sets in the group.

graphical user interface (GUI)
A type of computer interface that presents a visual metaphor of a real-world scene, often of a desktop, by combining high-resolution graphics, pointing devices, menu bars and other menus, overlapping windows, icons and the object-action relationship.

group
A collection of RACF-defined users who can share access authorities for protected resources.

guest
In z/OSMF, a user who enters the system without an assigned role. Depending on how a guest user enters z/OSMF, a guest user is considered either authenticated or non-authenticated, as follows:

- z/OSMF Authenticated Guest. The user enters z/OSMF with a valid user ID and password, but is not assigned to a z/OSMF role.
- z/OSMF Guest. The user is neither logged into z/OSMF, nor assigned to a z/OSMF role.

A z/OSMF administrator can manage the access of guest users to z/OSMF tasks through the z/OSMF Roles panel.

GUI  See graphical user interface.

H
hardcopy log
In systems with multiple console support or a graphic console, a permanent record of system activity.

header
Area of the z/OSMF browser interface (the upper pane) in which the banner is displayed.

HFS  See hierarchical file system.

hierarchical file system (HFS)
A system for organizing files in a hierarchy, as in a UNIX system.

HTTP proxy
Object that specifies the settings required for the primary system to gain access to a secondary system through an organization’s HTTP proxy server.

I
I/O  See input and output.

I/O priority management
In the Workload Management task, an option that you can specify within the service definition details to indicate whether WLM is to dynamically set I/O priorities based on performance goals. When enabled, WLM dynamically adjusts I/O priorities based on how well each service class is meeting its goals, and WLM includes I/O usings and delays in its execution velocity calculation.

I/O service units
A measure of individual data set I/O
activity and JES spool reads and writes for all data sets associated with an address space.

IBM Support Center
The IBM organization responsible for software service.

IBM WebSphere Application Server OEM Edition for z/OS
A native Web services runtime environment for select system-level applications that run on z/OS.

IBM z/OS Management Facility (z/OSMF)
A framework for managing various aspects of z/OS systems. z/OSMF includes an intuitive graphical user interface (GUI) for performing various management tasks. Structurally, z/OSMF is comprised of a Web browser user interface and functions provided by z/OS components and the CIM server running in an address space on the host z/OS system. z/OSMF is provided at no charge, as a separately licensed and entitled z/OS program product.

IBMLink/ServiceLink
The IBM support site for opening, browsing, or updating customer problem management reports (PMRs). The site includes an interactive online database of PMRs. The contents include open and resolved authorized program analysis reports (APARs) and program temporary fix (PTF) information. The IBMLink/ServiceLink Web site is http://www.ibm.com/ibmlink/servicelink.

importance
In the Workload Management task, the degree of importance of a service class goal relative to other service class goals. There are five levels: lowest (5), low (4), medium (3), high (2), and highest (1).

incident
An event that is not part of the standard operation of a service and causes or may cause a disruption to or a reduction in the quality of services and customer productivity.

incident description
In the Incident Log task, the dump title for an incident, as it was specified by the operator or the abending system function.

Incident Log task
In z/OSMF, the management task that allows you to display a log of system records with details about each potential system problem. The Incident Log task provides a list of incidents through a summary view (Incident Log panel) and a selectable detail view (Diagnostic Details panel). The Incident Log task can help you obtain, aggregate, and send data to IBM Support or an independent software vendor (ISV) and manage the data associated with a particular problem.

initial program load (IPL)
The process of loading the operating system and other basic software into main storage.

The process by which an operating system is initialized at the beginning of the day or session. At IPL, the system operator enters the installation-specific information the operating system must have in order to manage the installation’s workloads. This information includes system parameters, system data set definitions, and other information needed for the operating system to begin operating.

input and output (I/O)
Pertaining to a device, process, channel, or communication path involved in data input, data output, or both.

installation
A particular computing system, including the work it does and the people who manage it, operate it, apply it to problems, service it, and use the results it produces.

installed service definition
In the Workload Management task, the service definition that resides in the WLM couple data set for the sysplex.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. Internet Protocol (IP) acts as an intermediary between the higher protocol layers and the physical network.

IP
See Internet Protocol.

IP address
The unique 32-bit address (or, for IP version 6, the 128-bit address) that
specifies the location of each device or workstation in the Internet. For example, 9.67.97.103 is an IP address. The address field contains two parts: the first part is the network address; the second part is the host number.

**IPL**  
See *initial program load*.

**IPv4**  
Internet Protocol version 4.

**IPv6**  
Internet Protocol version 6.

---

**J**  

**JCL**  
See *job control language*.

**job**  
A separately executable unit of work.

**job card**  
See *record*.

**job control language (JCL)**  
A command language that identifies a job to an operating system and describes the job’s requirements.

**JOB statement**  
The JOB statement is the first control statement in a JCL job. It marks the beginning of a job and also specifies the name of the job. The JOB statement also might provide details and parameters that apply to all job steps within the job, such as accounting information and conditions for job termination. It also may contain any comments that help describe the statement.

---

**L**  

**link**  
In the z/OSMF navigation area, a reference to an external Web resource that can be used when performing system management tasks. Your installation can customize z/OSMF with links to external sites for system management tools and information. z/OSMF comes supplied with several useful links by default.

**Linux**  
An open source operating system that runs on a wide range of hardware platforms and has many features that are similar to the UNIX system.

**Linux data gatherer**  
See *RMF Linux data gatherer*.

**lock**  
The process by which integrity of data is ensured by preventing more than one user from accessing or changing the same data or object at the same time.

**log in**  
To connect to a computer system or network by entering identification and authentication information at the workstation.

**log out**  
To discard authentication credentials and corresponding permissions. Once logged out, z/OSMF no longer recognizes the user and reverts to the authority of the z/OSMF Guest role.

**log snapshot**  
A subset of log data preserved and associated with an incident.

**logrec**  
The z/OS error log, which contains error information in binary, written to a system-scope data set or a sysplex-wide log stream. See *error log*.

---

**M**  

**managed system**  
A system that is being controlled by a given system management application.

**manual control**  
In the Workload Management task, a method of managing application environments. Under manual control, the name of the startup JCL procedure has not been defined for an application environment. The installation, therefore, must manually start server address spaces, as needed. Contrast with *automatic control*.

**member**  
A partition of a partitioned data set (PDS) or partitioned data set extended (PDSE).

**metric**  
A measurement type. Each resource that can be monitored for performance, availability, reliability, and other attributes has one or more metrics about which data can be collected.

**metric group**  
In the Resource Monitoring task, a container that displays the samples that have been collected for the metrics included in the container and provides controls that you can use to browse through the collected samples.
Monitor III
See RMF Monitor III.

monitoring dashboard
In the Resource Monitoring task, a set of metric groups or custom views that you can use to monitor the performance of z/OS sysplexes, AIX system complexes (System p), Linux system complexes (System x and System z), or Linux images (System z and Intel).

MSGCLASS
Parameter on the JCL JOB statement that specifies the output class for output listings (SYSOUT). Output classes are defined by the installation to designate unit record devices, such as printers.

N
navigation area
Area of the z/OSMF browser interface (the left pane) from which the user can select among various systems management tasks. For example: "To view potential problems, select the Incident Log task from the z/OSMF navigation area."

O
operations log (OPERLOG)
In a sysplex, the log of operational messages (WTOs and WTORs), which is stored in a z/OS system logger log stream.

OPERLOG
See operations log.

P
partitioned data set (PDS)
A data set in direct access storage that is divided into partitions, called members, each of which can contain a program, part of a program, or data. Synonymous with program library. Contrast with sequential data set.

partitioned data set extended (PDSE)
A system-managed data set that contains an indexed directory and members that are similar to the directory and members of partitioned data sets. A PDSE can be used instead of a partitioned data set.

pass phrase
A string consisting of mixed-case letters, numbers, and special characters, including blanks, that is used to control access to data and systems.

password
A string of characters known to a user who must specify it to gain full or limited access to a system and to the data stored within it. RACF uses a password to verify the identity of the user.

PDS
See partitioned data set.

PDSE
See partitioned data set extended.

PDUU
See z/OS Problem Documentation Upload Utility.

performance period
In the Workload Management task, a service goal and importance level that is assigned to a service class for a specific duration.

plug-in
In z/OSMF, a collection of one or more system management tasks. A plug-in can be added to z/OSMF during the product configuration process, or later by the z/OSMF administrator.

PMR
See problem management record.

policy
See service policy.

port
An access point for data entry or exit.

port number
The part of a socket address that identifies a port within a host.

primary system
z/OS image that host the z/OSMF instance an enterprise uses to perform all of its z/OS management tasks.

problem determination
The process of determining the source of a problem.

The process of isolating the source of a suspected problem to a hardware or software component or product.

problem management record (PMR)
The number in the IBM support
mechanism that represents a service incident with a customer.

A record of the activities performed during the course of resolving a customer reported problem. Customers with access to IBMLink can view their PMRs.

**problem number**
A tracking number used to refer to a problem reported to a service provider.

**processor**
In a computer, the part that interprets and executes instructions. Two typical components of a processor are a control unit and an arithmetic logic unit.

**product set**
The operating systems, subsystems, or products that should be installed, maintained, migrated, and deployed as a group.

**profile**
A file containing customized settings for a system or user.

**proxy**
An application gateway from one network to another for a specific network application such as FTP.

**R**

**RACF** See Resource Access Control Facility.

**reason code**
A return code that describes the reason for the failure or partial success of an attempted operation.

**record**
A group of related data, words, or fields treated as a unit, such as one name, address, and telephone number.

A self-contained collection of information about a single object. A record is made up of a number of distinct items, called fields. See fixed-length record, variable-length record.

**Remote Technical Assistance and Information Network (RETAIN®)**
Database used by IBM Support Centers to record all known problems with IBM licensed programs.

**report class**
In the Workload Management task, a group of work for which reporting information is collected separately. For example, you can have a report class for information combining two different service classes, or a report class for information on a single transaction.

**Repository Authorization Mode**
In z/OSMF, the security authorization mode wherein user access to tasks is managed through user and role definitions in the z/OSMF data repository. Authorization to tasks is administered by the z/OSMF Administrator, through the Roles, Users, and Links tasks.

**resource**
A facility of a computing system or operating system required by a job, task, or running program. Resources include main storage, input/output devices, the processing unit, data sets, files, libraries, folders, application servers, and control or processing programs.

In the Workload Management task, an actual physical entity such as a data base or a peripheral device, or an intangible quality such as a certain time of day or a certain day of the week.

**Resource Access Control Facility (RACF)**
A component of z/OS Security Server that provides access control by identifying and verifying the users to the system, authorizing access to protected resources, logging detected unauthorized attempts to enter the system, logging unauthorized attempts to enter the system, and logging detected accesses to protected resources.

**resource group**
In the Workload Management task, an amount of processing capacity across one or more z/OS images that is assigned to one or more service classes.

**Resource Measurement Facility (RMF)**
A feature of z/OS that measures selected areas of system activity and presents the data collected in the format of printed reports, System Management Facility (SMF) records, or display reports.

**RETAIN**
See Remote Technical Assistance and Information Network.

**RMF** See Resource Measurement Facility.
RMF Cross Platform Resource Monitoring (RMF XP)  Integrated solution of RMF to monitor the performance of heterogeneous environments, such as AIX running on System p, Linux running on System x, and Linux running on System z.

RMF DDS
See RMF Distributed Data Server.

RMF Distributed Data Server (DDS)
The data server in a sysplex that gathers data from the RMF Monitor III distributed on each system in the sysplex.

RMF Linux data gatherer
A tool that gathers performance data for Linux images (System z and Intel). The gatherer is an optional tool that you can download and install in your installation. The tool is provided as-is at no additional charge. It is not supported by IBM, and it is not shipped with z/OSMF. For more details about the tool or to download a copy, see the RMF PM with Support for Linux Enterprise Server Web page.

RMF Monitor III
A short-term data collector for z/OS images. It provides short-term data collection and online reports for continuous monitoring of system status and for solving performance problems, workflow delay monitoring, and goal attainment supervision.

RMF XP
See RMF Cross Platform Resource Monitoring.

role
In z/OSMF, a functional grouping of task authorizations. A role represents the authorizations associated with that role.

S

SAF Authorization Mode
In z/OSMF, the security authorization mode wherein user access to tasks is controlled through the z/OS system authorization facility (SAF). The authorization definitions used by SAF are managed by the installation's security management product. Authorization to tasks is granted based on user ID or the user's inclusion in a user group. In an system with RACF, for example, user authorization is based on RACF profiles and groups, and is maintained by the security administrator in the RACF database.

scheduling environment
In the Workload Management task, a list of resource names along with their required states. If a z/OS image satisfies all of the requirements in the scheduling environment associated with a given unit of work, that unit of work can be assigned to that z/OS image. If any of the requirements are not satisfied, then that unit of work cannot be assigned to that z/OS image.

SCHENV parameter
Parameter on the JCL JOB statement that specifies the name of the WLM scheduling environment for a job.

send diagnostic data
In the Incident Log task, the option to collect the information necessary for sending diagnostic data to IBM or another destination and initiate the FTP action.

sequential data set
A data set whose records are organized on the basis of their successive physical positions, such as on magnetic tape.

A data set in which the contents are arranged in successive physical order and are stored as an entity. The data set can contain data, text, a program, or part of a program. Contrast with partitioned data set (PDS).

server
In a network, hardware or software that provides facilities to clients. Examples of a server are a file server, a printer server, or a mail server.

A computer that contains programs, data, or provides the facilities that other computers on the network can access.

The party that receives remote procedure calls. Contrast with client.

ServerPac
A software-delivery package consisting of products and service for which IBM has performed the System Modification Program/Extended (SMP/E) installation steps and some of the post-SMP/E installation steps.
service
In the Workload Management task, the amount of resources consumed by a work request. The service definition coefficients specified in the service definition and the CPU, SRB, I/O and storage service units are used to calculate service.

service class
In the Workload Management task, a group of work that has the same service goals or performance objectives, resource requirements, or availability requirements.

service coefficient
In the Workload Management task, a value that specifies which type of resource consumption should be emphasized in the calculation of service rate. The types of resource consumption are central processing unit (CPU), input and output channel (IOC), main storage occupancy (MSO), and service request block (SRB).

service definition
In the Workload Management task, an explicit definition of all the workloads and processing capacity in a sysplex. A service definition consists of the following items: service definition details, service policies, workloads, service classes, resource groups, report classes, classification groups, classifications, application environments, resources, and scheduling environments.

Service Definition Details
In the Workload Management task, section of the WLM service definition that contains the name, description, and functionality level of the service definition. It also contains the service definition coefficients and the service options.

service policy
In the Workload Management task, a named set of performance goals that WLM uses as a guideline when matching resources to work.

service request block (SRB)
A control block that represents a routine that performs a particular function or service in a specified address space.

session
The period of time during which a user of a terminal can communicate with an interactive system; usually, the elapsed time from when a terminal is logged into the system until it is logged out of the system.

A logical or virtual connection between two stations, software programs, or devices on a network that allows the two elements to communicate and exchange data.

The time during which an authenticated user is logged in.

solution
A combination of products that addresses a particular customer problem or project.

source
In the Incident Log task, it is the name of the data set or log stream in which the dump or log is stored.

SPECIAL attribute
A user attribute that gives the user full control over all of the RACF profiles in the RACF database and allows the user to issue all RACF commands, except for commands and operands related to auditing.

software instance
For z/OS platform software, the SMP/E target and distribution zones associated with a product set and the target and distribution libraries described by those zones.

source
The initiator of an action or operation.

The input for an action or operation.

source software instance
Input for the software deployment process. It is the software instance to be deployed.

source system
In the Deployment task, the active (currently running) z/OS image that has access to the volumes and data sets where the source software instance resides.

SRB
See service request block.

SRB service units
A measure of the SRB execution time for both local and global SRBs multiplied by an SRM constant which is CPU model dependent.

SRM
See system resources manager.
status  The current condition or state of a program, object, or device, for example, the status of a printer.

The state of a job or job stream instance.

storage service units
A measure of the central storage page frames multiplied by 1/50 of the CPU service units. The 1/50 is a scaling factor designed to bring the storage service component in line with the CPU component.

structure
A construct used to map and manage storage on a coupling facility.

superuser
In z/OS UNIX, a system user who operates with the special privileges needed to perform a specified administrative task.

superuser authority
In z/OS UNIX, the unrestricted authority to access and modify any part of the operating system, usually associated with the user who manages the system.

supervisor call (SVC)
An instruction that interrupts a program being executed and passes control to the supervisor so that it can perform a specific service indicated by the instruction.

SVC  See supervisor call.

SVC dump
A dump that is issued when a z/OS or a DB2® functional recovery routine detects an error.

A representation of the virtual storage for the system when an error occurs.
Typically, a system component requests an SVC dump from a recovery routine when an unexpected error occurs. However, an authorized program or the operator can also request an SVC dump when diagnostic dump data is needed to solve a problem.

SYSLOG
A Berkeley Software Distribution (BSD) logging system used to collect and manage other subsystem's logging data.

A single-system log of operational messages, stored in JES spool files.

sysplex (system complex)
Multiple systems communicating and cooperating with each other through multisystem hardware elements and software services to process the installation's workloads.

sysplex couple data set
A couple data set (CDS) that contains sysplex-wide data about systems, groups, and members that use cross-system coupling facility (XCF) services. All systems in a sysplex must be connected to the sysplex CDS. See also couple data set and WLM couple data set.

sysplex dump directory
A shared VSAM data set used to store properties (data values) associated with the SVC dumps created on a z/OS system or sysplex. By default, this data set is named SYS1.DDIR.

system
The combination of a configuration (hardware) and the operating system (software). Often referred to simply as the z/OS system.

In the Deployment task, a z/OS image that hosts a z/OSMF instance.

In the Deployment task, the z/OS image that has access to the volumes and data sets associated with a software instance.

system-initiated abend
An abend caused by the operating system's inability to process a routine; may be caused by errors in the logic of the source routine. Contrast with user-initiated abend.

system log (SYSLOG)
In z/OS, the system log data set that includes all entries made by the WTL (write-to-log) macro as well as the hardcopy log. SYSLOG is maintained by JES in JES SPOOL space.

system logger
A central logging facility provided by z/OS. The system logger component provides an integrated logging facility that can be used by system and subsystem components.

system logger
A central logging facility provided by MVS. The system logger provides an
integrated MVS logging facility that can be used by system and subsystem components.
The z/OS component that creates sysplex-wide log streams, such as OPERLOG and the sysplex-wide logrec data set.

**system resource manager (SRM)**
A group of programs that controls the use of system resources, such as programs, devices, and storage areas that are assigned for use in jobs.
A component of the z/OS control program.

**system REXX**
The z/OS component that provides a programming interface for running REXX execs outside of TSO/E or the batch environment.

**SYSREXX**
A system function used to invoke REXX execs from a programmable interface imbedded in authorized system code.

**TCP/IP data file**
In z/OSMF, an installation-defined data set or UNIX file that is used to override the default system TCP/IP configuration.

**terse**
The process of compacting (packing) data before transmitting a copy to another site, typically employing FTP as the transmission mechanism. A complementary unpack service is provided to create a similar data set at the receiving site. On z/OS, the AMATERSE service aid program is used to compact data.

**tracking ID**
A local problem tracking number, available to correlate an incident with a problem management system.

**U**

**user**
A person who requires the services of a computing system.

**user-initiated abend**
A request made by user code to the operating system to abnormally terminate a routine. Contrast with *system-initiated abend*.

**V**

**variable-length record**
A record having a length independent of the length of other records with which it is logically or physically associated. Contrast with *fixed-length record*.

**velocity**
In the Workload Management task, a type of service class goal that you can use to specify the rate at which you expect work to be processed for a given service class when that work is ready to run. It is a measure of the acceptable processor and storage delays while work is running.

**virtual storage access method (VSAM)**
An access method for direct or sequential processing of fixed-length and variable-length records on disk devices. The records in a VSAM data set or file can be organized in logical sequence by a key field (key sequence), in the physical
sequence in which they are written on the data set or file (entry sequence), or by relative-record number.

**VSAM**
See *virtual storage access method*.

**W**

**WLM** See *Workload Manager*.

**WLM Administrative Application**
The Interactive System Productivity Facility (ISPF) application used to specify WLM service definitions.

**WLM couple data set**
A type of data set that is created through the XCF couple data set format utility for the WLM function. The data set contains the service definition information.

**work qualifier**
In the Workload Management task, an attribute of incoming work. Work qualifiers include: subsystem type, subsystem instance, userid, accounting information, transaction name, transaction class, source LU, netid, and LU name.

**work request**
A piece of work, such as a request for service, a batch job, a transaction, or a command.

**Workload Management task**
In z/OSMF, the management task that allows you to manage WLM service definitions and to operate WLM. You can use this task to define, modify, view, import, export, print, or install a service definition or activate a service policy.

**workload**
In the Workload Management task, a group of service classes to be tracked, managed, and reported as a unit.

**Workload Manager (WLM)**
A z/OS component that prioritizes workloads and matches them with available resources.

**write to operator (WTO)**
A system service used to send messages to an operator console informing the operator of errors or system conditions that might need correcting. A response is not required.

**WTO** See *write-to-operator*.

**WTOR**
See *write-to-operator-with-reply*.

**Z**

**z/OS** An IBM mainframe operating system that uses 64-bit real storage.

**z/OS host system**
The system on which z/OSMF is running.

**z/OS Problem Documentation Upload Utility (PDUU)**
A parallel File Transfer Protocol (FTP) utility that is designed to send documentation in a more efficient manner to IBM FTP sites. For more information about the utility, see *z/OS MVS Diagnosis: Tools and Service Aides*.

**z/OSMF**
See *IBM z/OS Management Facility*.

**zFS** See *zSeries® file system*.

**zSeries file system (zFS)**
A type of file system that resides in a VSAM linear data set (LDS).
Index

Special characters

_BPXK_AUTOCVT environment variable 152
-add option 124, 251
-addlink option 131, 251
-config option 65, 251
-fastpath option 34, 65, 67, 69, 252
-finish option 75, 251
-overridefile option 34, 65, 252
-prime option 73, 251
-service option 251
-verify option 72, 123, 251
/tmp directory 153
.modifying the default 45
.profile file defining for the administrator user ID 71
$TMPDIR environment variable 153

A

About page 127
description 152
About this document xi, xii
accessibility 297
administration task
overview 8, 135, 137
administration for z/OSMF 117
advanced settings
modifying 263
reviewing 45, 75
AGGRGROW setting
used for z/OSMF data file system 73, 81
alias
removing for UNIX shell commands 64
Application Linking Manager interface
description 211
obtaining a list of handlers for an event type 221
registering an event handler 218
registering an event type 215
unregistering an event handler 222
unregistering an event type 223
Application Linking Manager task
overview 136
application programming interface
for z/OSMF 179
ASSIZE recommendation 64
ASSIZEMAX value
setting for the administrator user ID 76
authorization mode 99
choosing 51
description 50
migration consideration 107, 108
selecting 36
authorizing users to z/OSMF 120, 121, 164
auto-mount process
using for z/OSMF 81
automatic dump data set allocation
(auto-dump)
using 241
verifying 25
automount facility
consideration for using 74, 82
AUTOMOVE setting
consideration 81
AXR address space
verifying active state 247
backup instance of z/OSMF
planning for 47
BBNBASE profile prefix 52, 55
BBNBASE.izuNOUsers resource 120
BBO.SYNC.userid
migration action 107, 109
BLSCDDIR CLIST
example 244
using 243
BLSRPRMI program
using 244
BPX.SRV.userid
migration action 107, 109
BPX.SRV.ZOSMFAD SURROGAT rule
migration action in z/OSMF 107, 109
BPXPRMxx parmlib member
modifying 81
settings 64
browser
See web browser
checking plug-in levels 127
CIM
See Common Information Model (CIM)
CIM_IVP_TIMEOUT variable
setting 160
cimivp timeout
corrective action 160
client side log data 153
description 268
command aliasing
removing for UNIX shell commands 64
common event adapter (CEA)
address space 25
assigning the TRUSTED attribute 28, 245
disconnecting from the sysplex dump directory 177
used during Incident Log task processing 231
verifying active state 164, 245
authorizing the z/OSMF administrator 245
authorizing z/OSMF administrator 278
CEAPRMxx parmlib member 233, 246
description 4
ensuring that it is active 25, 245, 246
full function mode 245
if not available 164
log stream recommendation 239
modifying settings 246
RACF security profiles 229
reason codes 269
Incident Log task 270
ISPF task 274
starting at IPL 233
Common Information Model (CIM)
provider
increasing the timeout interval 83, 263
server
increasing the timeout interval for CIM providers 83
logging 143
overview 4
security authorizations 71
starting 73, 83
trace 143
Common Information Model (CIM)
server
automatic startup 83
requirement 25
timeout setting 83
configuration
for z/OSMF 59
verifying 77

© Copyright IBM Corp. 2009, 2012
ISPF task (continued)
   troubleshooting 175
IXCMIAPU utility program 239
IZU_AUTHORIZ...MODE variable specifying 36
IZU_AUTOGID_OVERRIDE 36
IZU_AUTOUID_OVERRIDE 36
IZU_CODE_ROOT setting modifying the default 62
IZU_CONFIG_DIR variable default 61
IZU_LOGFILE_DIR setting modifying the default 62
izuadmin.env file 45, 75, 263
modifying settings 263
izualtusers.sh script 120, 164
izuconfig1.cfg.rexx using 69, 277, 280, 282, 283, 285, 286, 287, 288
izuconfig1.USERID.rexx using 121
izudflt.cfg file defaults 32, 255, 289
izudflt.ovr file defaults 32, 255, 289
using 34
IZUG0.log.lck file 152
IZUGn.log file 152
izuiltempdirvalue setting modifying 45
izuilunitvalue setting modifying 45
izuincidentlogverify.report file creating 161
reviewing 75, 123
izumigrate.sh script 104
izuNOUsers resource 120
izusetup.sh script -add option 124, 251
-addlink option 131, 251
-config option 34, 65, 251
-fastpath option 34, 67, 252
-finish option 75, 251
-overridefile option 34, 252
-prime option 73, 251
-service option 47, 127, 251
-verify option 72, 123, 251
overridefile file 34
syntax 251
izuupdate.sh script 263

job cancelling 196
changing the job class 198
job control language (JCL)
   sample for renaming dumps in the sysplex dump directory 248
job document 202
job spool file retrieving the contents 191
job spool files list obtaining 189
job status obtaining 185
JobFile document 203
jobs list obtaining 187
JSON document
   ErrorReport document 204
Job document 202
JobFile document 203
JSON document specifications 202
error reporting categories 205

K
keyboard shortcuts 297

L
link character limit in z/OSMF 109
defining in z/OSMF 55, 58, 135, 139
log format 267
log data 153
client side 268
server side 267
log file
   working with 152
log file directory
   modifying the default 62
log lock file 152
logging error data for z/OSMF 153
logging in to z/OSMF 78, 79, 263
LOGREC log stream
   setting up 238
ltpacachetimeout setting
   modifying 263
ltpatimeout setting
   default 79
   modifying 263

M
mainframe
   education xi
managing log lock files 152
MAXPROCUSER
   consideration 160
MEMLIMIT recommendation 64
message help 21
message IZUG295E 159
migration
   procedure 103
   upgrading the configuration file 104
   upgrading the override file 104
migration action 103, 107, 109
migration report file example 291
Monitoring Dashboards task
   required z/OS setup 29

N
network consideration 81

O
OMVS session
   INPUT status indicator 65
operations log (OPERLOG)
   setting up 235, 236
override file
   defaults 32, 255, 289
description 34
parameter on izusetup.sh 252

P
page-level help 21
parmlib data set
   access required 75
planning for z/OSMF 1, 23
planning worksheet 35
plug-in
   adding to an already-configured z/OSMF 69, 103
   choosing for configuration 23
description 23
   planning your selections 40
POST method
   register an event handler 218
   register an event type 215
PROCUSERMAX value
   setting 160
product file system
   mounted at IPL 81
product file system mount point
   modifying the default 62
profile file
   defining for the administrator user
   ID 71
programming interface for z/OSMF 179
PUT method
   Cancel a job 196
   change the class of a job 198
   submit a job 194

R
RACF commands
   Capacity Provisioning task 281
   RACF commands 281
   CIM server 280
   RACF commands 280
   Configuration Assistant task 282
   RACF commands 282
core functions 278
Deployment task 287
RACF commands 287
Incident Log task 283
RACF commands 283
ISPF task 285
RACF commands 285
Resource Monitoring plug-in 286
RACF commands 286
Workload Management plug-in 288
RACF commands 288
re-authenticating 79, 263
reason code
for common event adapter (CEA) 269
REGION recommendation 64
Repository Authorization Mode conversion to 101
description 50
specifying 36
using 56
Representational State Transfer (REST) interfaces
information resources 179
introduction 179
Resource Monitoring plug-in post-configuration tasks 85
required z/OS setup 29
Resource Monitoring task overview 16
reviewing the About page 127
REXX exec See exec role
assigning in z/OSMF 57
defining in z/OSMF 139
root code directory mount point modifying the default 62
runtime log format 267
using 152
SAF See system authorization facility
SAF Authorization Mode conversion to 99
description 50
specifying 36
using 52, 55
screen resolution minimum supported 46
script izuauthuser.sh script 120
izumigrate.sh script 104
izusetup.sh script -add option 124
-addlink option 131
-config option 65
-finish option 75
-prime option 73
-service option 127
-verify all option 123
-verify core option 123
-verify log option 123
-verify racf option 72
izupdate.sh script 263
startServer.sh script 77
where to find 61
script mode choosing 34
security administration task links 55, 58
overview 52, 55
security administrator managing links 55, 58
tasks performed by 52, 55
security concepts 49
security setup
authorizing users to z/OSMF 120
default for z/OSMF 227
verifying the RACF actions 72
Send Diagnostic Data wizard troubleshooting 178
server side log data description 267
ServerPac order configuration file 47, 127
considerations xi, 5, 6, 23, 61
serverp.acfg file service consideration 47, 127
service 127
applying to z/OSMF 127
applying updates to z/OSMF 47
session status refreshing 65
sessiontimeout setting modifying 263
shell command removing aliases 64
Software Deployment plug-in post-configuration tasks 93
Software Deployment task post-configuration tasks 86
software upgrade installation considerations 5, 6, 23, 61
startServer.sh script using 77
Summary of Changes xiii
superuser authority 33
required for user ID 33, 119
SURROGAT class profile checking 107, 109
SYS1.MIGLIB data set
APF-authorized 249
SYS1.SAMPLIB data set CEASNPLG member 233, 239
sysplex dump directory creating 243
migrating to a larger directory 244
renaming dumps in the directory 248
space shortage 244
using the BLSCDDIR CLIST 243
verifying setup 75
SYSEX
See System REXX (SYSEX) component
system authorization facility description 4
system log (SYSLOG)
capturing data from 240
system logger couple data set creating 233
system prerequisites for z/OSMF overview 24
System REXX (SYSEX) component ensuring that it is active 247
System Status task overview 18
required z/OS setup 29
temporary directory modifying the default 45
text-only zoom 299
tools for troubleshooting 144
trace data
using 153
troubleshooting
browser problems 144
certificate error 168, 170
checking the About page 152
common problems 155
Configuration Assistant task 174
calibration issues 155
EJBROLE class
must be defined 173
enabling tracing 153
Firefox 146
Incident Log task 176
information for 143
ISPF task 175
logon errors 173
online help not available 173
overview 143
Send Diagnostic Data wizard 178
user interface problems 168
using the Incident Log IVP 161
using the runtime logs 152
workstation problems 144
TRUSTED attribute
assigning to the CEA address space 26, 245
TSO/E user consideration 27

S
SAF
See system authorization facility
SAF Authorization Mode conversion to 99
description 50
specifying 36
using 52, 55
script izuaauthuser.sh script 120
izumigrate.sh script 104
izusetup.sh script -add option 124
-addlink option 131
-config option 65
-finish option 75
-prime option 73
-service option 127
-verify all option 123
-verify core option 123
-verify log option 123
-verify racf option 72
izupdate.sh script 263
startServer.sh script 77
where to find 61
script mode choosing 34
security administration task links 55, 58
overview 52, 55
security administrator managing links 55, 58
tasks performed by 52, 55
security concepts 49
security setup
authorizing users to z/OSMF 120
default for z/OSMF 227
verifying the RACF actions 72
Send Diagnostic Data wizard troubleshooting 178
server side log data description 267
ServerPac order configuration file 47, 127
considerations xi, 5, 6, 23, 61
serverp.acfg file service consideration 47, 127
service 127
applying to z/OSMF 127
applying updates to z/OSMF 47
session status refreshing 65
sessiontimeout setting modifying 263
shell command removing aliases 64
Software Deployment plug-in post-configuration tasks 93
Software Deployment task post-configuration tasks 86
software upgrade installation considerations 5, 6, 23, 61
startServer.sh script using 77
Summary of Changes xiii
superuser authority 33
required for user ID 33, 119
SURROGAT class profile checking 107, 109
SYS1.MIGLIB data set
APF-authorized 249
SYS1.SAMPLIB data set CEASNPLG member 233, 239
sysplex dump directory creating 243
migrating to a larger directory 244
renaming dumps in the directory 248
space shortage 244
using the BLSCDDIR CLIST 243
verifying setup 75
SYSEX
See System REXX (SYSEX) component
system authorization facility description 4
system log (SYSLOG)
capturing data from 240
system logger couple data set creating 233
system prerequisites for z/OSMF overview 24
System REXX (SYSEX) component ensuring that it is active 247
System Status task overview 18
required z/OS setup 29
temporary directory modifying the default 45
text-only zoom 299
tools for troubleshooting 144
trace data
using 153
troubleshooting
browser problems 144
certificate error 168, 170
checking the About page 152
common problems 155
Configuration Assistant task 174
calibration issues 155
EJBROLE class
must be defined 173
enabling tracing 153
Firefox 146
Incident Log task 176
information for 143
ISPF task 175
logon errors 173
online help not available 173
overview 143
Send Diagnostic Data wizard 178
user interface problems 168
using the Incident Log IVP 161
using the runtime logs 152
workstation problems 144
TRUSTED attribute
assigning to the CEA address space 26, 245
TSO/E user consideration 27

U
user
authorizing to z/OSMF tasks 120, 121
defining in z/OSMF 57, 140
log in 173
user ID
authorizing through a REXX exec 121

V
verification script
results 123

W
web browser
common problems 148, 168
enabling prompting for file downloads 151
recommended settings 146, 148, 151
troubleshooting
Internet Explorer 148
z/OSMF supported browsers 46
WebSphere Application Server changing the logging level 154, 155
WebSphere Application Server response file values for z/OSMF 261
WebSphere servant log 153
Welcome page
customizing the content for guests 128
Workload Management task
  input for configuration  44
  overview  19
  post-configuration tasks  95
  required z/OS setup  31
worksheets
  for z/OSMF  35
workstation
  logon errors  173
  required software  46
wsadmin.traceout
  using  159

Z
z/OS Basic Skills information center  xi
z/OS jobs REST interface
  cancelling a job on z/OS  196
  changing the class of a job  198
  description  181
  listing the jobs for an owner, prefix, or
  job ID  187
  listing the spool files for a job  189
  obtaining the status of a job  185
  purging a job from the JES spool  200
  retrieving the contents of a job spool
  file  191
  submitting a job to run on z/OS  194
z/OSMF administrator
  ASSIZEMAX value  76
  creating  69, 278
  defining to the Incident Log
  plug-in  283
  defining to the Incident Log task  69
  priming  73
  setting password for  75
  setting the PROCUSERMAX
  value  160
  storage allocation  76
  tasks performed by  8, 135, 137
ZMFAPLA resource class
  description  50
  zooming text  299
ZOSMFAD user ID
  creating password for  75
  defined to data file system  73
  defining through a REXX exec  69,
  278
  storage allocation  76