z/OS

IBM z/OS Management Facility Configuration Guide

Version 2 Release 2

SC27-8419-02

Note
Before using this information and the product it supports, read the information in "Notices" on page 245.

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

© Copyright IBM Corporation 2009, 2016.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures v

Tables vii

About this document ix
Who should use this document ix
Where to find more information ix

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

Summary of changes xiii
Summary of changes for z/OS Version 2 Release 2 (V2R2), as updated June 2016 xiii
Summary of changes for z/OS Version 2 Release 2 (V2R2), as updated March 2016 xiii
Changes made in z/OSMF Version 2 Release 2, SC27-8419-00 xiv
Changes made in z/OSMF Version 2 Release 1, SA38-0657-04 xv
Changes made in z/OSMF Version 2 Release 1, SA38-0657-03 xv
Information applicable to all releases xvi

Part 1. Introduction 1

Chapter 1. Overview of z/OSMF. 3
z/OSMF and related system components 4
Software delivery options for z/OSMF 5
Software prerequisites for z/OSMF 5
What setup is needed for z/OSMF? 6
Receiving service updates for z/OSMF 6

Chapter 2. Project plans for configuring z/OSMF 7

Part 2. Configuration 11

Chapter 3. Configuring z/OSMF for the first time 13
The configuration process 13
Security concepts in z/OSMF 15
Preparing your workstation for z/OSMF 16
Installing the z/OSMF cataloged procedures . . . 16
Updating your system for the z/OSMF started procedures 17
Updating your system for the z/OS data set and file REST interface 18
Updating the BPXPRMxx member of parmlib . . . 19
Optionally creating a IZUPRMxx parmlib member 22
Creating a base z/OSMF configuration 27
Before you begin 27
Step 1: Run the security commands for the z/OSMF resources 28
Step 2: Allocate and mount the z/OSMF file system 29
Step 3: Start the z/OSMF server 31
Step 4: Access the z/OSMF Welcome page . . . 35
Step 5: Log into z/OSMF. 36

Chapter 4. Migrating to a new release of z/OSMF 39
Configuring the new release of z/OSMF. 39
Migrating your configuration values to member IZUPRMxx 41

Chapter 5. Selecting which optional z/OSMF plug-ins to add 45
Overview of z/OSMF system management tasks . . 46
Capacity Provisioning task overview 47
Configuration Assistant task overview 48
Incident Log task overview 49
ISPF task overview 51
Notifications in z/OSMF 52
Notification Settings task overview 53
Resource Monitoring task overview 55
Software Management task overview 57
System Status task overview. 59
Workflows task overview. 60
Workload Management task overview 61

Chapter 6. Setting up security for the z/OSMF plug-ins 63
Managing user access to z/OSMF tasks and links . 63
Managing guest user access in z/OSMF 66

Chapter 7. Adding plug-ins to a z/OSMF configuration 67

Chapter 8. Using z/OSMF in a multi-system environment 71
Configuring z/OSMF for availability 71
Restart z/OSMF processing on another system in the same sysplex 73
Additional considerations for a multi-system environment 73
Configuring a primary z/OSMF for communicating with secondary instances 74
Enabling single sign-on between z/OSMF instances 77

Part 3. Post-configuration 79

© Copyright IBM Corp. 2009, 2016

Chapter 9. Customizing the Welcome page for guest users 81

Chapter 10. Linking z/OSMF tasks and external applications 83

Chapter 11. Configuring your system for asynchronous job notifications . . 85
Creating the CIM indication provider subscription 85
Procedure for creating a subscription 87
Enabling secure job completion notifications for your programs 91

Chapter 12. Adding links to z/OSMF . . 95
Managing security for links in z/OSMF 97

Chapter 13. Deleting incidents and diagnostic data 99

Chapter 14. Troubleshooting problems 103
Resources for troubleshooting 103
Tools and techniques for troubleshooting 104
Verifying your workstation with the environment checker 104
Finding information about z/OSMF 113
Working with z/OSMF messages 113
Working with z/OSMF runtime log files . . . 114
Examples of working with z/OSMF runtime logs 115
Common problems and scenarios. 117
Problems during configuration 117
Problems when accessing the user interface . . 118
Problems when using Configuration Assistant 124
Problems when using the ISPF task 125
Problems when using the Incident Log task . . 126
Problems when attempting to send data . . . 127

Chapter 15. Configuration messages 129
IZUG000-IZUG399 129

Part 4. Appendixes 179

Appendix A. Security configuration requirements for z/OSMF 181

Appendix B. Customizing your z/OS system for the z/OSMF plug-ins . . . 201
Using FTP in your network. 201
Reviewing your CIM server setup 201
Updating z/OS for the Capacity Provisioning plug-in 203
Enabling PassTicket creation for Capacity Provisioning task users 203
Updating z/OS for the Configuration Assistant plug-in 205
Updating z/OS for the Incident Log plug-in . . . 205
Defining a couple data set for system logger 208
Setup considerations for log snapshots 210
Enabling the operations log (OPERLOG) . . . 211
Defining and activating the LOGREC log stream 213
Defining diagnostic snapshot log streams . . . 214
Enabling SYSLOG for diagnostic snapshots . . 215
Configuring automatic dump data set allocation 215
Configuring dump analysis and elimination . . 216
Creating the sysplex dump directory 217
Ensure that common event adapter (CEA) is configured and active 219
Ensuring that System REXX is set up and active 221
Ensuring that dump data set names are correct 222
Updating z/OS for the ISPF plug-in. 223
Updating z/OS for the Resource Monitoring Plug-in 224
Enabling PassTicket creation for Resource Monitoring task users 225
Browser consideration for the Resource Monitoring task 226
Updating z/OS for the Software Deployment plug-in 227
Creating access controls for the Software Management task 227
Creating product information files for the Software Management task. 233
Updating z/OS for the Workload Management plug-in 235

Appendix C. Common event adapter (CEA) reason codes 239

Appendix D. Accessibility 243
Using assistive technologies 243
Accessibility features for the z/OSMF GUI . . . 243

Notices 245
Policy for unsupported hardware. 246
Minimum supported hardware 247
Trademarks 247

Index 249

Figures

1. Introducing z/OSMF: The Welcome page 3
2. z/OSMF and related system components 4
3. User authorizations in z/OSMF 15
4. RACF commands for defining the started procedures to the STARTED class 18
5. Expected result from the **D A,IZUANG1** command 34
6. Expected result from the **D A,IZUSVR1** command 34
7. Expected result from the **STOP** command 35
8. z/OSMF Welcome page (before login). . . . 36
9. z/OSMF Welcome page (after login) 37
10. Capacity Provisioning task main page. . . . 47
11. Configuration Assistant task main page 48
12. Incident Log task sample view 50
13. ISPF task main page 51
14. Notifications main page 53
15. Notification Settings main page 54
16. Resource Monitoring task sample view 55
17. Software Management page 57
18. System Status sample view 59
19. Workflows task main page 60
20. Workload Management task main page 61
21. SAF authorizations in z/OSMF: A simplified view 64
22. SAF authorizations in z/OSMF: The default setup. 65
23. RACF commands for authorizing the users of the Configuration Workflow 68
24. z/OSMF Welcome page (after optional plug-ins are added) 69
25. Trust relationship when server certificates are signed by the same CA certificate 76
26. Trust relationship when the server certificates are signed by different CA certificates. . . . 77
27. Customizable areas of the z/OSMF Welcome page 81
28. Content of the Welcome page properties file 82
29. Example of the Welcome page properties file 82
30. Key components in the application linking process 83
31. Sample RACF commands for creating CIM authorizations. 87
32. Subscription values for asynchronous job notification. 87
33. Content of the link properties file 95
34. Example of a link definition 97
35. Example: Defining a link resource name and permitting a group to it 98
36. Format of the **ceatool** command 100
37. Example output from the environment checker tool 106
38. Portion of z/OSMF server side log data 115
39. Example of z/OSMF client side log data 116
40. Digital ring information for the z/OSMF server user ID 121
41. z/OS components that are used in Incident Log task processing 206
42. Expected results from the **D XCF,COUPLE,TYPE=LOGR** command 209
43. Expected results from the **D C,HC** command 211
44. Expected results from the D LOGREC operator command. 213
45. Expected results from the **D LOGGER** command 215
46. RACF commands to enable CEA to access SYSLOG 215
47. Expected results from the **D A,CEA** command 220
48. Expected result from the **D A,AXR** command 222
49. Sample JCL to rename SVC dumps in the sysplex dump directory 222
50. Sample product information file for the Software Management task 234

© Copyright IBM Corp. 2009, 2016

Tables

1. Planning checklist for a first-time installation 7
2. Planning checklist for migrating to a new release 8
3. Planning checklist for adding optional plug-ins to a configuration 9
4. Security authorizations for the z/OS data set and file REST interface 19
5. Sample MOUNT command for the z/OSMF file system 20
6. Actions and performers for configuring z/OSMF 27
7. Parmlib values that result from running the izumigrate.sh script 41
8. z/OSMF optional plug-ins and associated tasks 45
9. Resource authorizations for the Configuration Workflow 67
10. Sample **ceatool** commands 101
11. Summary of tools and information for troubleshooting problems with z/OSMF . . 103
12. Columns in the environment checker tool results page 104
13. Recommended settings for Firefox 107
14. Recommended settings for Internet Explorer 110
15. Class activations that z/OSMF requires 181
16. User IDs that z/OSMF creates during the configuration process 183
17. Security groups that z/OSMF creates during the configuration process 183
18. Security setup requirements for z/OSMF core functions 184
19. Security setup requirements for hardware compression with zEDC 188
20. Security setup requirements for hardware cryptography with ICSF 189
21. CIM groups that might be required for the optional plug-ins 190
22. Name information for a Capacity Provisioning domain 190
23. Security groups required for the Capacity Provisioning plug-in 190
24. Security setup requirements for the z/OS data set and file REST interface 191
25. Security setup requirements for the z/OS jobs REST interface 192
26. JESJOBS class authorizations needed for performing job modify operations. 192
27. Security group required for the Workload Management plug-in 193
28. Security setup requirements for the z/OSMF optional plug-ins 193
29. Default profiles, resource names, and group assignments for z/OSMF 198
30. z/OS setup actions for the Capacity Provisioning task 203
31. z/OS setup actions for the Incident Log task 207
32. z/OS setup actions for the Resource Monitoring and System Status tasks 224
33. Actions users can take against global zones by access authority. 228
34. Actions users can take against software instances by access authority 229
35. Actions users can take against deployments by access authority. 230
36. Actions users can take against categories by access authority. 231
37. Workload Management task authorizations for z/OSMF 237
38. CEA reason codes related to Incident Log task processing 239
39. CEA reason codes related to z/OS jobs REST interface processing 242

© Copyright IBM Corp. 2009, 2016

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 person who is responsible for setting up z/OSMF on a z/OS system and for diagnosing problems with the product. This document assumes that the user is familiar with the z/OS operating system and its accompanying products.

For ServerPac installers, if you select the **ServerPac full system replacement installation type**, a base configuration is created through a ServerPac post-installation job, that uses IBM defaults. The default instance of z/OSMF does not include any of the optional plug-ins, such as Configuration Assistant, Incident Log, and so on. After you complete the ServerPac installation, you can add plug-ins to z/OSMF, as described in this document.

If you install z/OSMF from a Custom-Built Product Delivery Option (CBPDO) software delivery package, or from a ServerPac order using the **ServerPac software upgrade installation type** method of installation, must manually create an instance of z/OSMF, using the planning and configuration information in this document.

Where to find more information

For an overview of the information associated with z/OS, see *z/OS Information Roadmap*.

z/OSMF home page

Visit the z/OSMF home page at http://www.ibm.com/systems/z/os/zos/zosmf/.

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 z/OS 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): http://publib.boulder.ibm.com/infocenter/zos/basics/index.jsp.

© Copyright IBM Corp. 2009, 2016

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
2. Send an email from the "Contact us" web page for z/OS (http://www.ibm.com/systems/z/os/zos/webqs.html)
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
  SC27-8419-02
- 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 that are listed for sending comments. Instead, take one of the following actions:

- Contact your IBM service representative.
- Call IBM technical support.
- Visit the IBM Support Portal at z/OS support page (http://www.ibm.com/systems/z/support).

© Copyright IBM Corp. 2009, 2016

Summary of changes

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

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

This document contains information that was previously presented in *IBM z/OS Management Facility Configuration Guide*, SC27-8419-01, which supported z/OS Version 2 Release 2 (V2R2).

New

For information about using z/OSMF in a multi-system environment, see Chapter 8, "Using z/OSMF in a multi-system environment," on page 71.

If your installation uses hardware compression through IBM z Systems Data Compression (zEDC), the z/OSMF server requires an additional resource authorization. See "Resource authorizations for hardware compression" on page 188.

The full set of required resource authorizations is described in Appendix A, "Security configuration requirements for z/OSMF," on page 181.

For information about the new and changed tasks in z/OSMF, see the z/OSMF Welcome page in the online help that ships with z/OSMF, which includes the topics *What's new* and *z/OSMF tasks at a glance*. The z/OSMF online help is also available in IBM Knowledge Center at: http://www.ibm.com/support/knowledgecenter/SSLTBW_2.2.0/com.ibm.zos.v2r2.izu/izu.htm.

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

This document contains information that was previously presented in *IBM z/OS Management Facility Configuration Guide*, SC27-8419-00, which supported z/OS Version 2 Release 2 (V2R2).

New

The following SAF profiles are added for the Notification Settings task, which is new in this release:
- <*SAF-prefix*>.ZOSMF.NOTIFICATION.SETTINGS
- <*SAF-prefix*>.ZOSMF.NOTIFICATION.SETTINGS.ADMIN
- <*SAF-prefix*>.ZOSMF.NOTIFICATION.SETTINGS.MODIFY

The following SAF profile is added for the Workflows task. This authorization allows the user to take ownership of a workflow instance.
- <*SAF-prefix*>.ZOSMF.WORKFLOW.ADMIN

The full set of required resource authorizations is described in Appendix A, "Security configuration requirements for z/OSMF," on page 181.

For information about the new and changed tasks in z/OSMF, see the z/OSMF Welcome page in the online help that ships with z/OSMF, which includes the topics *What's new* and *z/OSMF tasks at a glance*. The z/OSMF online help is also available in IBM Knowledge Center at: http://www.ibm.com/support/

© Copyright IBM Corp. 2009, 2016

knowledgecenter/SSLTBW_2.2.0/com.ibm.zos.v2r2.izu/izu.htm.

Changes made in z/OSMF Version 2 Release 2, SC27-8419-00

This document contains information that was previously presented in *IBM z/OS Management Facility Configuration Guide,* SA38-0657-04, which supported IBM z/OS Management Facility Version 2 Release 1.

New information

In z/OS V2R2, z/OSMF is a base element of z/OS.

z/OSMF requires the following level of Java™:

- IBM 64-bit SDK for z/OS, Java Technology Edition, V7.1 (SR3) (5655-W44)

For information about the new and changed tasks in z/OSMF, see the z/OSMF Welcome page in the online help, which includes the topics *What's new* and *z/OSMF tasks* at a glance.

The most current information about the z/OSMF tasks are provided in the online help that ships with z/OSMF. The z/OSMF online help is also available in IBM Knowledge Center at: http://www.ibm.com/support/knowledgecenter/SSLTBW_2.2.0/com.ibm.zos.v2r2.izu/izu.htm.

Changed information

In z/OS V2R2, the process for configuring z/OSMF is changed to provide a smoother configuration experience.

The highlights are summarized, as follows:

- As a base element of z/OS V2R2, z/OSMF is installed on your system when you SMP/E install z/OS V2R2.
- z/OSMF includes a simplified set of options for creating a configuration, with default values that are suitable for most installations. You might find the defaults to be sufficient for your environment; if so, use them for a quick-start experience with z/OSMF.

  If z/OSMF requires customization, you can modify settings by using the IZUPRMxx parmlib member, which is new in this release. A sample member is provided in SYS1.SAMPLIB(IZUPRM00) with settings that match the z/OSMF defaults. Using IZUPRM00 as a model, you can create a customized IZUPRMxx parmlib member for your environment.

  In previous releases, you ran an interactive UNIX shell script, called **izusetup.sh**, to create a z/OSMF base configuration on your z/OS system. Then, you used the script again to modify the configuration by adding optional plug-ins and links. In this release, the **izusetup.sh** script is removed.
- In this release, security authorizations for z/OSMF are created using sample jobs in SYS1.SAMPLIB. The sample jobs are described in "IZUxxSEC jobs in SYS1.SAMPLIB" on page 63. The full set of required resource authorizations is described in Appendix A, "Security configuration requirements for z/OSMF," on page 181. In previous releases, the configuration scripts created one or more REXX execs with sample RACF® commands for creating authorizations.
- After you create the base configuration, you can add plug-ins to z/OSMF to expand its function. Enabling the optional plug-ins in z/OSMF requires some customization of the z/OS host system, as described in this document.
- As in previous releases, starting z/OSMF is done through the MVS™ **START** command. Processing is managed through the z/OSMF server, which runs as a pair of started tasks on your system: `IZUANG1` and `IZUSVR1`. IBM supplies cataloged procedures for these tasks with your order.
- As in previous releases, migrating to the new release of z/OSMF includes running the script **izumigrate.sh**. In this release, however, the script is enhanced to create a customized IZUPRMxx parmlib member, based on the configuration settings from your current (old) system.

For ServerPac installers, if you select the **ServerPac full system replacement installation type**, a base configuration is created through a ServerPac post-installation job, that uses IBM defaults. As in previous releases, the default instance of z/OSMF does not include any of the optional plug-ins, such as Configuration Assistant, Incident Log, and so on. For details, see "Software delivery options for z/OSMF" on page 5. If you select the **ServerPac software upgrade installation type**, you must create an instance of z/OSMF, using the planning and configuration information in this document.

For an overview of migration activities, see Chapter 4, "Migrating to a new release of z/OSMF," on page 39. The migration actions for z/OSMF V2R2 and prior releases are described in *z/OS Migration, GA32-0889*.

Moved information

The following information is moved to other z/OS publications:

- The publication *Program Directory for IBM z/OS Management Facility* is discontinued in this release. Information about installing z/OSMF is moved to *z/OS V2R2 Program Directory*.
- The migration actions for z/OSMF are moved to *z/OS Migration, GA32-0889*.
- The summary of new, changed, and deleted messages for z/OSMF is moved to *z/OS Summary of Message and Interface Changes, SA23-2300*.

Changes made in z/OSMF Version 2 Release 1, SA38-0657-04

This document contains information previously presented in *IBM z/OS Management Facility Configuration Guide,* SA38-0657-03, which supported IBM z/OS Management Facility Version 2 Release 1.

This document contains new or revised information for maintenance.

Changes made in z/OSMF Version 2 Release 1, SA38-0657-03

This document contains information previously presented in *IBM z/OS Management Facility Configuration Guide,* SA38-0657-02, which supported IBM z/OS Management Facility Version 2 Release 1.

New functionality is available for z/OSMF V2R1 when you install the PTFs for APAR PI32148 and the corequisite APARs. For instructions on installing this service on a z/OSMF V2R1 system, check the ++HOLD actions for the associated PTFs.

This document contains new or revised information for APAR PI32148 and the corequisite APARs.

New information

If your enterprise has multiple z/OSMF instances running, z/OSMF adds support for establishing a single sign-on (SSO) environment between those z/OSMF instances. For more information, see "Enabling single sign-on between z/OSMF instances" on page 77.

The amount of text you can specify for the header area and footer area of the z/OSMF Welcome page is increased to 256 characters from 128 characters. For more information, see Chapter 9, "Customizing the Welcome page for guest users," on page 81.

The following topic is new: "CEA reason codes for the z/OS jobs REST interface services" on page 242.

Changed information

Previously, z/OSMF-to-z/OSMF communication was supported by the Software Management task only. In this release, z/OSMF provides the multisystem routing services, which allow you to create z/OSMF tasks that route requests between z/OSMF instances. To that end, references to the Software Management task were removed.

Information about the multisystem routing services is provided in *IBM z/OS Management Facility Programming Guide* .

Information applicable to all releases

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

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

Part 1. Introduction

An introduction to z/OSMF includes the following topics:

- Chapter 1, "Overview of z/OSMF," on page 3
- Chapter 2, "Project plans for configuring z/OSMF," on page 7.

© Copyright IBM Corp. 2009, 2016

Chapter 1. Overview of z/OSMF

IBM z/OS Management Facility (z/OSMF) provides system management functions in a task-oriented, web browser-based user interface with integrated user assistance, so that you can more easily manage the day-to-day operations and administration of your mainframe z/OS systems. By streamlining some traditional tasks and automating others, z/OSMF can help to simplify some areas of z/OS system management.

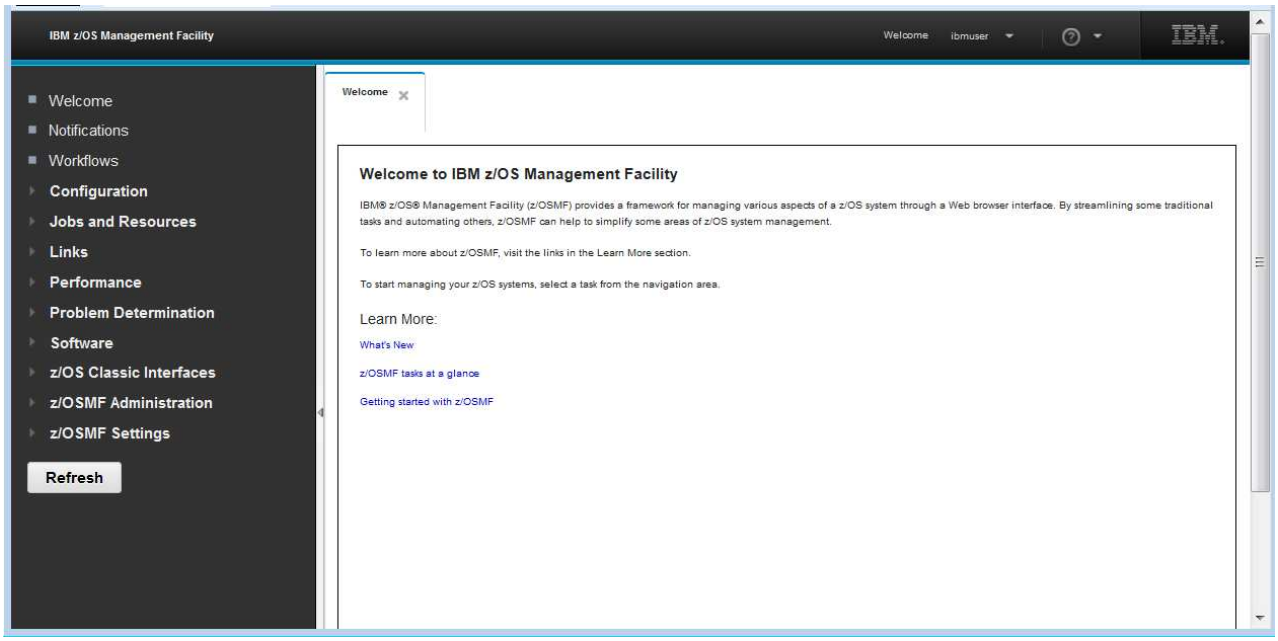


Figure 1. Introducing z/OSMF: The Welcome page

z/OSMF provides a framework for managing various aspects of a z/OS system through a web browser interface

z/OSMF provides you with a single point of control for:

- Viewing, defining, and updating policies that affect system behavior
- Monitoring the performance of the systems in your enterprise
- Managing your z/OS software
- Performing problem data management tasks
- Consolidating your z/OS management tools.

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. Multiple users can log into z/OSMF using different computers, different browsers, or multiple instances of the same browser.

This chapter introduces you to the major functions, architecture, and facilities of z/OSMF. Later chapters provide more details about configuration, administration, and troubleshooting. Usage information is provided in the z/OSMF online help.

© Copyright IBM Corp. 2009, 2016

z/OSMF and related system components

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 those tasks. The z/OS components make up the environment necessary for using the z/OSMF functions. z/OSMF does not provide a separate client installation. You need only a compatible browser to access the z/OSMF web application on your system.

z/OSMF includes the following software:

- z/OSMF server.
- WebSphere® Liberty profile, which provides an application server runtime environment for z/OSMF.
- Set of optional, system management functions or *plug-ins*, which you can enable when you configure z/OSMF.
- Technologies for serving the web browser interface, such as JavaScript and Dojo.

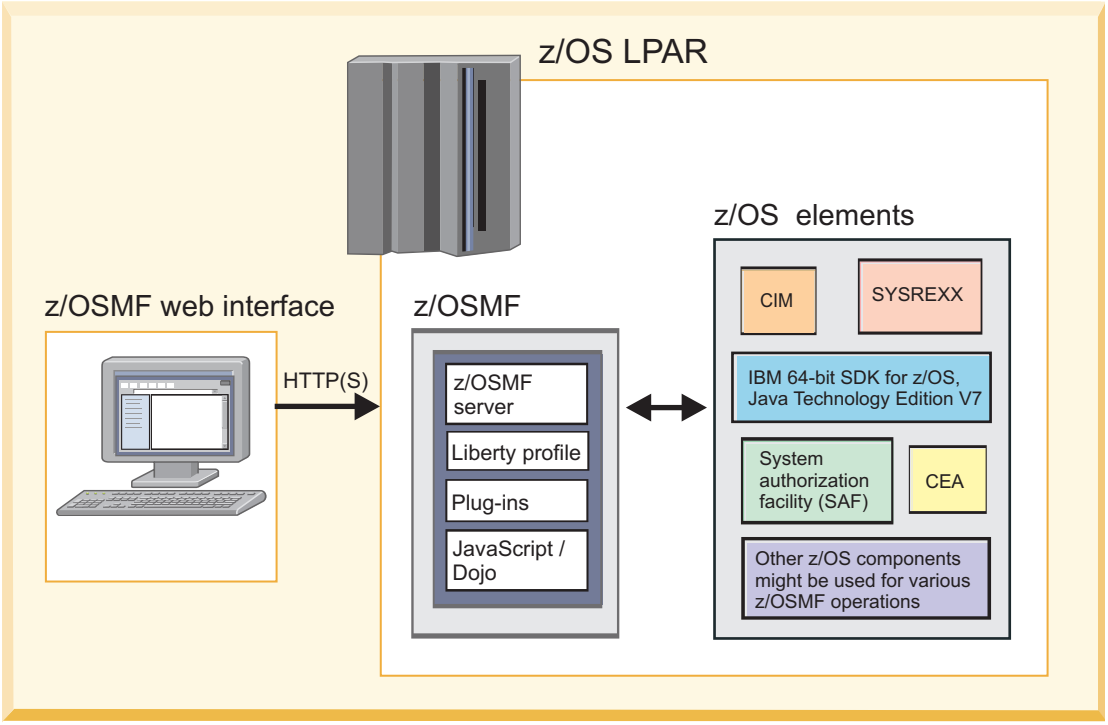


Figure 2. z/OSMF and related system components

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, with information passed to various z/OS system components as needed.

Depending on the particular task being performed, z/OSMF makes use of various enabling technologies on z/OS, such as the following:

- IBM 64-bit SDK for z/OS, Java Technology Edition, V7.1 (SR3) (5655-W44). This IBM software development kit (SDK) contains the Java Runtime Environment (JRE) and other tools that support Java applications.
- 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.

Software delivery options for z/OSMF

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

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, a base z/OSMF configuration is created through a ServerPac post-installation job, using IBM-supplied defaults. The default instance of z/OSMF does not include any of the optional plug-ins, such as Configuration Assistant, Incident Log, and so on. Enabling the optional plug-ins in z/OSMF requires some customization of the z/OS host system, as described in Chapter 7, "Adding plug-ins to a z/OSMF configuration," on page 67.
- If you select the software upgrade installation type, you require the planning and configuration information in this document to create a z/OSMF configuration. Your system programmer can create a customized version of the IZUPRMxx member on your system, and define plug-ins to it.

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 can create a customized IZUPRMxx member to define an instance of z/OSMF on your system.

Software prerequisites for z/OSMF

Ensure that the following product is installed and operational on your system:

IBM 64-bit SDK for z/OS, Java Technology Edition, V7.1 (SR3) (5655-W44) . For the required PTFs, see *z/OS V2R2 Program Directory*.

This set-up must be done before you configure z/OSMF. By default, the SDK resides in the directory `/usr/lpp/java/J7.1_64` on your system. If you installed it in another location, be sure to include the JAVA_HOME statement in your IZUPRMxx parmlib member, as shown in "Optionally creating a IZUPRMxx parmlib member" on page 22.

It is recommended that you complete the planning for z/OSMF before attempting to configure it. Also, be sure to obtain the latest PTFs; see "Receiving service updates for z/OSMF" on page 6.

For ServerPac users, use the jobs and documentation supplied with your ServerPac order to create an initial instance of z/OSMF. During the ServerPac process, you will need sections of this document to

complete certain actions. Thereafter, you can refer to this document for information about performing various post-configuration actions, such as configuring the optional plug-ins.

The following web browsers are supported by z/OSMF, and are recommended for best results:
- Microsoft Internet Explorer Version 9 or later
- Mozilla Firefox Version 17 or later.

What setup is needed for z/OSMF?

When you install the z/OS operating system, you install z/OSMF as a base element. When you run the jobs that are described in the *z/OS Program Directory*, you install z/OSMF into the z/OS root file system, in the directory `/usr/lpp/zosmf`, by default.

Enabling z/OSMF on your system will involve the following phases:
- Planning for z/OSMF.
- Installing z/OSMF, as described in *z/OS V2R2 Program Directory*.
- Configuring an instance of z/OSMF in your sysplex, and adding optional plug-ins. This phase requires certain z/OS resources to be set up, commands to be run, and security setup to be performed for RACF (or the equivalent). Information for these activities is provided in this document.

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 the authorizations in your security management product. z/OSMF provides sample jobs in SYS1.SAMPLIB, and the information in this document to assist your security administrator. Information about security setup is provided in Chapter 6, “Setting up security for the z/OSMF plug-ins,” on page 63 and Appendix A, “Security configuration requirements for z/OSMF,” on page 181.

When you migrate to a new release of z/OSMF, you can re-use much of the customization from your current configuration. For an overview of migration activities, see Chapter 4, “Migrating to a new release of z/OSMF,” on page 39. The migration actions for z/OSMF V2R2 and the prior release are described in the publication, *z/OS Migration, GA32-0889*.

Receiving service updates for z/OSMF

As with other z/OS elements, IBM ships service for z/OSMF in the form of program temporary fixes (PTFs). When planning for service updates, consider that z/OSMF consists of multiple functional modification identifiers (FMIDs), as follows:
- All z/OSMF core functions are provided together as one FMID
- Each optional plug-in is provided as a separate FMID.

For the most current information on APAR fixes and service updates, check the z/OS Preventive Service Planning (PSP) bucket, as referenced in *z/OS V2R2 Program Directory*. You can also use the IBM Support for z/OS web page or the IBMLink web site http://www.ibm.com/ibmlink/servicelink. For a list of fix category (FIXCAT) values and descriptions, visit the SMP/E web site: http://www.ibm.com/systems/z/os/zos/smpe/fixcategory.html.

When working with service updates, check the PTF ++HOLD action for specific instructions for deploying the updated code, such as whether you must restart the z/OSMF server to have the updates take effect.

Chapter 2. Project plans for configuring z/OSMF

Are you setting up z/OSMF for the first time? Or, are you migrating an existing z/OSMF configuration to the latest release? Or, perhaps, you only want to add another plug-in to an existing configuration? Depending on what you want to do, you will follow a sequence of topics in this document to complete your objective.

System planners and installation managers collaborate with specialized IT personnel to plan, configure, and manage z/OSMF. The following checklists provide a task summary, identify the IT role or skill that is required for each task, and provide links to further details.

- "First-time installation"
- "Migrating to a new release" on page 8
- "Adding plug-ins to your configuration" on page 9
- "Post-configuration" on page 9.

First-time installation

This configuration phase encompasses first-time setup tasks for a base z/OSMF configuration. At this phase, z/OSMF operates in a minimal mode, with a UI framework and the core functions, but without any of the optional plug-ins enabled.

Table 1. Planning checklist for a first-time installation

✓	**Task summary:**	**IT role / skills:**	**Where to find instructions:**
	Learn what z/OSMF is—a framework for web-based, system management tasks on z/OS.	System planners and installation managers	Chapter 1, "Overview of z/OSMF," on page 3
	Verify that your installation meets the prerequisites for using z/OSMF.	System programmer	"Software prerequisites for z/OSMF" on page 5
	Learn about the z/OSMF configuration process.	System programmer	"The configuration process" on page 13
	Verify that your workstation meets the prerequisites for using z/OSMF.	System programmer	"Preparing your workstation for z/OSMF" on page 16
	Set up the z/OSMF started procedures.	System programmer	"Updating your system for the z/OSMF started procedures" on page 17
	Optionally, gather information about your environment, to be used for creating a configuration parmlib member, IZUPRMxx.	System programmer	"Optionally creating a IZUPRMxx parmlib member" on page 22
	Follow a procedure to create a base z/OSMF configuration (core functions only).	Security administrator and system programmer	"Creating a base z/OSMF configuration" on page 27
	Learn what authorities are needed to create a base configuration.	Security administrator and system programmer	"Selecting a user ID for configuration" on page 28
	Activate z/OSMF by starting the z/OSMF server.	System programmer	"Step 3: Start the z/OSMF server" on page 31
	Verify the results of your work by opening a web browser to the Welcome page of z/OSMF.	System programmer	"Step 4: Access the z/OSMF Welcome page" on page 35
	After you are satisfied with the base configuration, you can add function to it through the addition of one or more optional plug-ins.	System programmer	See the steps in Table 3 on page 9 for "Adding plug-ins to your configuration" on page 9.

© Copyright IBM Corp. 2009, 2016

Migrating to a new release

During this stage, you configure a new release of z/OSMF with the objective of making it functionally compatible with the previous release. After a successful migration, z/OSMF functions in the same way (or similar to the way) it did on the old system.

Table 2. Planning checklist for migrating to a new release

✓	Task summary:	IT role / skills:	Where to find instructions:
	Learn about the z/OSMF migration process.	System programmer	Chapter 4, "Migrating to a new release of z/OSMF," on page 39
	Perform the migration actions for the z/OSMF element.	System programmer	*z/OS Migration, GA32-0889*
	Migrate the z/OSMF configuration values from your current (old) system to the new system by running the **izumigrate.sh** script. The script creates a customized member, IZUPRMxx, with installation-specific data.	System programmer	• "Configuring the new release of z/OSMF" on page 39 • "Migrating your configuration values to member IZUPRMxx" on page 41
	Edit the IZUPRMxx parmlib member to specify the Java home directory and other settings for the new system.	System programmer	• "Configuring the new release of z/OSMF" on page 39 • "Optionally creating a IZUPRMxx parmlib member" on page 22
	If you are migrating from z/OSMF V1R13, edit and run a copy of the IZUSEC sample job in SYS1.SAMPLIB to create the security authorizations for your configuration.	Security administrator and system programmer	• "Configuring the new release of z/OSMF" on page 39 • "Step 1: Run the security commands for the z/OSMF resources" on page 28
	Edit and run a copy of the IZUMKFS sample job to allocate the z/OSMF file system and directory.	System programmer	• "Configuring the new release of z/OSMF" on page 39 • "Step 2: Allocate and mount the z/OSMF file system" on page 29
	Install the latest versions of the cataloged procedures for the z/OSMF started tasks. Transfer any customizations that you require to the new procedures.	System programmer	• "Configuring the new release of z/OSMF" on page 39 • "Installing the z/OSMF cataloged procedures" on page 16
	Activate z/OSMF on the new system by starting the z/OSMF server.	System programmer	• "Configuring the new release of z/OSMF" on page 39 • "Step 3: Start the z/OSMF server" on page 31
	Verify the results of your work by opening a web browser to the Welcome page of z/OSMF.	System programmer	"Step 4: Access the z/OSMF Welcome page" on page 35
	Review the **START** command for z/OSMF in the COMMNDxx parmlib member or your automation product for possible updates.	System programmer	"Specifying a job name and other parameters" on page 32

Adding plug-ins to your configuration

This configuration phase encompasses adding function to a z/OSMF configuration through the addition of optional plug-ins.

Table 3. Planning checklist for adding optional plug-ins to a configuration

✓	Task summary:	IT role / skills:	Where to find instructions:
	Learn about the optional z/OSMF plug-ins; determine which plug-ins to configure.	System programmer	Chapter 5, "Selecting which optional z/OSMF plug-ins to add," on page 45
	Plan the security requirements for users of the z/OSMF tasks.	Security administrator and system programmer	Chapter 6, "Setting up security for the z/OSMF plug-ins," on page 63
	Perform the z/OS system customization for each z/OSMF plug-in.	System programmer	Appendix B, "Customizing your z/OS system for the z/OSMF plug-ins," on page 201
	Define the plug-ins to the IZUPRMxx parmlib member.	System programmer	See the description of the PLUGINS statement in "Optionally creating a IZUPRMxx parmlib member" on page 22.
	Authorize users and groups to access the z/OSMF tasks.	Security administrator and system programmer	Chapter 6, "Setting up security for the z/OSMF plug-ins," on page 63
	Complete the deployment of the plug-ins by restarting the z/OSMF server.	System programmer	"Step 3: Start the z/OSMF server" on page 31

Post-configuration

In this phase, you can optionally perform additional tasks to enhance your z/OSMF configuration. z/OSMF administrators are the most likely IT personnel to participate in these activities.

Topics in the following parts describe these ongoing activities and other occasional administrative tasks:

- Chapter 9, "Customizing the Welcome page for guest users," on page 81
- "Configuring a primary z/OSMF for communicating with secondary instances" on page 74
- "Enabling single sign-on between z/OSMF instances" on page 77
- Chapter 10, "Linking z/OSMF tasks and external applications," on page 83
- Chapter 11, "Configuring your system for asynchronous job notifications," on page 85
- Chapter 12, "Adding links to z/OSMF," on page 95
- Chapter 13, "Deleting incidents and diagnostic data," on page 99
- Chapter 14, "Troubleshooting problems," on page 103
- Chapter 15, "Configuration messages," on page 129.

Part 2. Configuration

Configuring z/OSMF includes the following topics:

- Chapter 3, “Configuring z/OSMF for the first time,” on page 13
- Chapter 4, “Migrating to a new release of z/OSMF,” on page 39
- Chapter 5, “Selecting which optional z/OSMF plug-ins to add,” on page 45
- Chapter 6, “Setting up security for the z/OSMF plug-ins,” on page 63
- Chapter 7, “Adding plug-ins to a z/OSMF configuration,” on page 67

© Copyright IBM Corp. 2009, 2016

Chapter 3. Configuring z/OSMF for the first time

For a new installation of z/OSMF, it is recommended that you begin by creating a base configuration. Here, z/OSMF operates in a minimal mode, with a UI framework and core functions, but without any of the optional plug-ins enabled. This topic describes the first-time setup tasks for creating a base configuration.

Observe the following considerations:

- Review all of the steps in this chapter before performing the configuration.
- If you are upgrading from a previous release of z/OSMF, skip ahead to Chapter 4, "Migrating to a new release of z/OSMF," on page 39.

The configuration process

In short, configuring an instance of z/OSMF is done by running the IBM-supplied jobs IZUSEC and IZUMKFS, and then starting the z/OSMF server.

The z/OSMF configuration process occurs in three stages, and in the following order:

Stage 1 - Security setup

Stage 2 - Configuration

Stage 3 - Server initialization

This sequence is critical to a successful configuration. This document assumes that you will carry out the steps in the order in which they are presented.

Security setup stage

During this stage, you establish security for z/OSMF through traditional SAF-based authorizations. IBM supplies a sample job, SYS1.SAMPLIB(IZUSEC), which contains RACF commands for creating the security definitions. Your security administrator should review the IZUSEC job before submitting it. If your system uses a security management product other than RACF, your security administrator can refer to the sample job for examples when creating equivalent authorizations for your system.

Configuration stage

During this stage, you allocate and mount the z/OSMF file system and create the z/OSMF user directory. IBM supplies a sample job, SYS1.SAMPLIB(IZUMKFS), which contains commands for performing this setup.

You might choose to substitute your own configuration values for the z/OSMF default settings. If so, you can create an IZUPRMxx parmlib member for your system or sysplex. IBM supplies a sample parmlib member, SYS1.SAMPLIB(IZUPRM00), which you can use as a model.

Server initialization

During this stage, you start the z/OSMF server, making z/OSMF active. On the **START** command, you can specify options that control the operation of the z/OSMF server on your system.

To have the server started automatically at IPL, add the START command to your active COMMNDxx parmlib member.

© Copyright IBM Corp. 2009, 2016

Overview of the configuration steps

The following steps are described in more detail in the topics that follow:

1. Set up the security for z/OSMF (once per sysplex or security domain). For a quick setup, run the sample job IZUSEC to create a base set of security groups, user IDs, and resource profiles for your z/OSMF configuration. Before running the job, have your security administrator review it to ensure that the appropriate authorizations are created.

   For information, see "Step 1: Run the security commands for the z/OSMF resources" on page 28.
2. Allocate the z/OSMF file system, which is used by the z/OSMF server. Here, you will edit and run the job IZUMKFS. Do this once for each z/OS system for which you want to configure z/OSMF.

   For information. see "Step 2: Allocate and mount the z/OSMF file system" on page 29.
3. Start the z/OSMF server (once per z/OS system). Processing is managed through the z/OSMF server, which runs as a pair of started tasks on your system: `IZUANG1` and `IZUSVR1`. IBM supplies cataloged procedures for these tasks with your order.

   To start z/OSMF manually, enter MVS **START** commands to start each procedure in the following sequence:

   ```
   S IZUANG1
   S IZUSVR1
   ```

   On the **START** command for IZUSVR1, you can specify options to control the processing of the server, such as the IZUPRMxx members to use, and tracing options for recording configuration-time errors.

   On start-up, the z/OSMF server reads in the persistance data from the user directory and creates a z/OSMF instance on your system.

   For information, see "Step 3: Start the z/OSMF server" on page 31.

Additional tasks might include:

- Customizing the configuration settings for z/OSMF. See "Optionally creating a IZUPRMxx parmlib member" on page 22.
- Updating parmlib members for subsequent IPLs, for example:
  - Copy the mount commands from the sample mount job to your BPXPRMxx parmlib member
  - Add the **START** commands for the started procedures to your COMMNDxx parmlib member.
  - Add the started procedure names to the AUTOLOG statement in your TCP/IP profile.
- Adding the optional plug-ins. When you are satisfied with the base configuration, you can add function to z/OSMF by adding plug-ins to the configuration. Sample commands for creating resource authorizations for the plug-ins are provided in the IZUxxSEC jobs in SYS1.SAMPLIB. Sample commands for authorizing users to the plug-ins are provided in the IZUAUTH job in SYS1.SAMPLIB.

  For information, see Chapter 7, "Adding plug-ins to a z/OSMF configuration," on page 67.

For ServerPac installers, if you select the **ServerPac full system replacement installation type**, a base configuration is created through a ServerPac post-installation job, using IBM-supplied defaults. The default instance of z/OSMF does not include any of the optional plug-ins, such as Configuration Assistant, Incident Log, and so on. After completing a ServerPac install, you can add plug-ins to z/OSMF. If you select the **ServerPac software upgrade installation type**, you must create an instance of z/OSMF, using the planning and configuration information in this document.

Security concepts in z/OSMF

As with other z/OS elements, 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 login, 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 3).

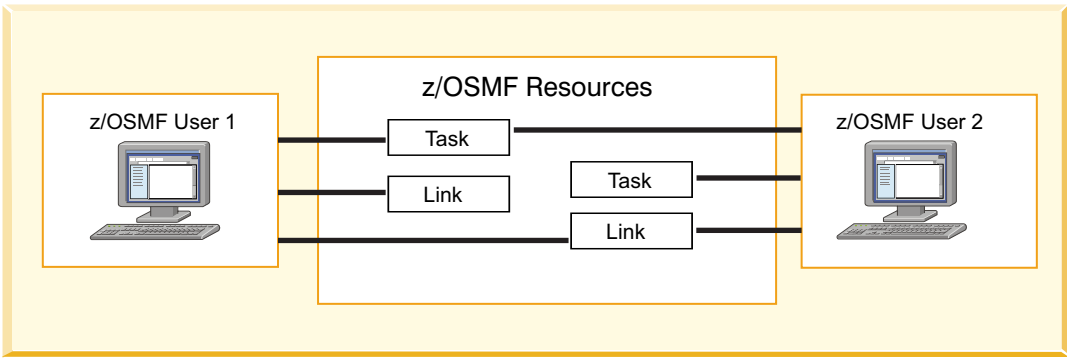


Figure 3. User authorizations in z/OSMF

Establishing security in z/OSMF requires the help of your security administrator. This person is responsible for ensuring that users and resources are defined in accordance with the security policies in use at your installation. This work includes running security commands to protect z/OSMF resources (tasks) and authorizing users to these resources.

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.

Help with setting up security

IBM provides a set of jobs in SYS1.SAMPLIB with sample RACF commands to help with your z/OSMF configuration. The IZUSEC job represents the authorizations that are needed for the z/OSMF core functions. Each of the other IZUxxSEC jobs is associated with an optional plug-in. Your security administrator can edit and run these jobs to secure various resources on the z/OS system. To create user authorizations for the optional plug-ins, your security administrator can use the IZUAUTH job in SYS1.SAMPLIB. It is assumed that your security administer has a user ID with the RACF SPECIAL attribute. For information, see Chapter 6, “Setting up security for the z/OSMF plug-ins,” on page 63.

If your installation uses a security management product other than RACF, your security administrator can refer to the SAMPLIB jobs for examples when creating equivalent commands for the security management product on your system.

z/OSMF does not support multilevel security

If the z/OSMF server is running in a *multilevel secure (MLS)* z/OS system, some z/OSMF functions might fail to work properly. The failures can occur because z/OSMF does not assign a SECLABEL to its started task address space. As a result, the functions that use inter-address space communication might fail because of a SECLABEL mismatch.

For example, a failure can occur in the ISPF task because it starts a TSO address space with the SECLABEL of the current z/OSMF user. Other z/OSMF functions that might fail include the z/OS data set and file REST interface and the TSO/E address space services.

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 lesser resolution, you might experience some clipping of content.
- Ensure that your browser is enabled for JavaScript. For instructions, see Table 13 on page 107 or Table 14 on page 110, 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 use the Internet Explorer 8 browser, you might experience:
  - Browser memory issues, if you open multiple tabs. If so, close some unneeded tabs to use less memory.
  - Slow responsiveness for certain data-intensive operations. If so, consider using another supported browser.

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 104.

Installing the z/OSMF cataloged procedures

z/OSMF requires that several cataloged procedures be installed on your system, as described in this topic.

z/OSMF requires that the following cataloged procedures be installed on your system:

- **Started procedures for the z/OSMF server:** z/OSMF processing is managed through the z/OSMF server, which runs as a pair of started tasks on your system, IZUANG1 and IZUSVR1.
- **Logon procedure for the z/OS data set and file REST interface:** z/OSMF requires that a TSO logon procedure be installed in your system proclib. The procedure is used internally by the z/OS data set and file REST interface services.

  IBM supplies a default procedure, IZUFPROC, which you must install prior to configuration. The default procedure should be sufficient for most z/OS installations. Review the procedure before installing it, however, to ensure that it is suitable for use in your environment.

  If you prefer, you can use a different logon procedure, if it provides the same function as the shipped IZUFPROC procedure. Specifically, the logon procedure must contain, at a minimum:
  - All of the DD statements from IZUFPROC; these must reference your system data sets that contain the z/OS UNIX REXX exec programs and ISPF libraries.

– The PROC statement must specify the z/OSMF root code directory path on the ROOT variable, for example:

  ```
  ROOT='/usr/lpp/zosmf'
  ```

  If your installation configured z/OSMF to use another path for the root code directory, specify that path instead. The path must be enclosed in quotation marks, begin with a forward slash ('/'), and be fully qualified (it cannot be relative). Mixed-case file system names are allowed.
– If your installation uses an actual (non-temporary) data set for ISPFPROF, the logon procedure must be configured to allow profile sharing.

IBM supplies the z/OSMF catalogued procedures in your order, as follows:

- **ServerPac and CustomPac orders:** For a ServerPac order, IBM supplies the cataloged procedures in SYS1.IBM.PROCLIB. For a CustomPac order, you can rename this data set through the installation dialog.
- **CBPDO orders:** For a CBPDO order, the data set name is SYS1.PROCLIB; you can rename this data set. During installation, you can optionally catalog the data set, or you can defer this step.

Ensure that the z/OSMF catalogued procedures reside in the SMP/E defined PROCLIB, as follows:

- **ServerPac and CustomPac users:** Ensure that SYS1.IBM.PROCLIB (or whatever you renamed it to) resides in the JES PROCLIB concatenation. Or, copy its contents to a data set in the JES PROCLIB concatenation.
- **CBPDO users:** Ensure that SYS1.PROCLIB (or whatever you renamed it to) resides in the JES PROCLIB concatenation (and is catalogued). Or, copy its contents to a data set in the JES PROCLIB concatenation.

Note that these steps are the same as you would do for any SMP/E installed cataloged procedure that is provided with z/OS.

Updating your system for the z/OSMF started procedures

z/OSMF processing is managed through the z/OSMF server, which runs as a pair of started tasks on your system, IZUANG1 and IZUSVR1. This topic explains how to update your system for the z/OSMF started tasks.

The following setup actions are required:

- "Verify that the z/OSMF server has sufficient authorization"
- "Add the started procedure names to the AUTOLOG statement" on page 18
- "Defining the z/OSMF started procedures to RACF" on page 18

Verify that the z/OSMF server has sufficient authorization

To ensure that the z/OSMF server can perform as required, verify that the z/OSMF started task user ID has sufficient permissions for your environment. By default, this user ID is `IZUSVR`, but you might have specified another user ID during the configuration process; see "Step 1: Run the security commands for the z/OSMF resources" on page 28.

By default, both of the z/OSMF started tasks (IZUANG1 and IZUSVR1) run under the started task user ID, IZUSVR. To assign a user identity to the started tasks, you can specify a job name (`JOBNAME=`) on the START command. Here, the job name is used as part of the SAF resource name that is passed to the your security product. If you omit the `JOBNAME=` specification, the default member names will be used: IZUANG1 and IZUSVR1. Ensure that the job name is defined in the security profiles for the started tasks. For considerations, see "Defining the z/OSMF started procedures to RACF" on page 18.

Information about starting the started tasks and setting them up to start after every IPL, is provided in "Step 3: Start the z/OSMF server" on page 31.

Add the started procedure names to the AUTOLOG statement

You must ensure that TCP/IP services are available to the z/OSMF server at initialization. To do so, add the z/OSMF started procedure names IZUANG1 and IZUSVR1 to the AUTOLOG statement in your TCP/IP profile (PROFILE.TCPIP).

For information about the AUTOLOG statement, see *z/OS Communications Server: IP Configuration Reference* .

Defining the z/OSMF started procedures to RACF

The IZUSEC job contains sample RACF commands for defining the z/OSMF started procedures to the STARTED class. Figure 4 shows the commands that are provided in the job.

```
//* Define the STARTED profiles for the z/OSMF server               *
 RDEFINE STARTED IZUSVR1.* UACC(NONE) STDATA(USER(IZUSVR) +
   GROUP(IZUADMIN) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))
 RDEFINE STARTED IZUANG1.* UACC(NONE) STDATA(USER(IZUSVR) +
   GROUP(IZUADMIN) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))
```

Figure 4. RACF commands for defining the started procedures to the STARTED class

You can create more specific profiles to associate the started tasks with particular job names. Doing so allows you to run the started tasks under another user ID, as needed, based on job name. Use this method to control the started tasks behavior, rather than modifying the started procedures directly. Note that any user ID that is used for running the started tasks must have the same security authorizations as the started task user ID. By default, this user ID is IZUSVR.

With the STARTED class, you can modify the security definitions for started procedures dynamically, using the RDEFINE, RALTER, and RLIST commands. For more information, see the topic on using started procedures in *z/OS Security Server RACF Security Administrator's Guide*.

Updating your system for the z/OS data set and file REST interface

z/OSMF requires that a default TSO logon procedure be included in your configuration. The procedure is used internally by the z/OS data set and file REST interface, and z/OSMF users must be authorized to it.

For your planning purposes, this topic describes the configuration settings and security set-up that are required for the logon procedure during the configuration process. As described in "Installing the z/OSMF cataloged procedures" on page 16, IBM supplies a default procedure named IZUFPROC, which should be sufficient for use at most installations.

Specifying the z/OS data set and file REST interface properties during configuration

The topic "Optionally creating a IZUPRMxx parmlib member" on page 22 describes the options for configuring z/OSMF. Included are options for the TSO logon procedure that is used by the z/OS data set and file REST interface.

The configuration process supplies default values; you can accept the defaults or supply installation-supplied alternative values in the IZUPRMxx parmlib member. You can specify the TSO logon procedure name, along with a corresponding TSO account number and address space region size.

It is recommended that you accept the defaults, which should be adequate for most z/OS installations. If you specify alternative values, you must ensure that the z/OSMF users and z/OSMF administrators security groups are authorized to the logon procedure name and account number that you specify. Also, ensure that the address space region size is at least 65536 (kilobytes) and that this setting is acceptable in your environment, to avoid a possible system memory exception error.

All z/OSMF users must have a TSO segment defined in your installation's security database. Failure to have a TSO segment causes some z/OSMF functions not to work.

Authorizing users to the z/OS data set and file REST interface

The IZUSEC job includes sample RACF commands for:

- Defining the TSO logon procedure and the associated account number to the TSOPROC and ACCTNUM classes, respectively.
- Authorizing z/OSMF users to the TSO logon procedure and account number.
- Authorizing z/OSMF users and the z/OSMF server to CEA TSO/E address space services.

Table 4 describes the authorizations that are created by the IZUSEC job.

Table 4. Security authorizations for the z/OS data set and file REST interface

Resource class	Resource name	Who needs access?	Type of access required	Why
ACCTNUM	IZUACCT	IZUADMIN IZUUSER	READ	Allows callers to access the account number that is used for the procedure for the z/OS data set and file REST interface services.
SERVAUTH	CEA.CEATSO.TSOREQUEST	IZUADMIN IZUUSER	READ	Allows callers to access the CEA TSO/E address space services. This setting allows HTTP client applications on your z/OS system to start and manage TSO/E address spaces.
SERVAUTH	CEA.CEATSO.TSOREQUEST	IZUSVR	READ	Allows the z/OSMF server to access the CEA TSO/E address space services. This setting allows the z/OSMF server to start and manage TSO/E address space services.
TSOPROC	IZUFPROC	IZUADMIN IZUUSER	READ	Allows callers to access the procedure for the z/OS data set and file REST interface services.

Updating the BPXPRMxx member of parmlib

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

This topic contains the following information:

- "Ensuring that the user file system is mounted at IPL time"
- "Using the automount facility" on page 20
- "Reviewing the IPCMSGQBYTES option of BPXPRMxx" on page 20

Ensuring that the user file system is mounted at IPL time

To have the z/OSMF user file system automatically mounted at IPL time, you must update your automount process or BPXPRMxx parmlib member. By default, the user file system uses the name IZU.SIZUUSRD. The user file system is mounted in read/write mode at the location `/var/zosmf`.

To have this file system mounted automatically at IPL time, add MOUNT command for the file system to your currently active BPXPRMxx parmlib member. For your reference, Table 5 on page 20 provides a sample MOUNT command.

Table 5. Sample MOUNT command for the z/OSMF file system

z/OSMF file system to be mounted	MOUNT command example
User file system	MOUNT FILESYSTEM('IZU.SIZUUSRD') TYPE(ZFS) MODE(RDWR) MOUNTPOINT('/var/zosmf') PARM('AGGRGROW') UNMOUNT

When you use the IZUMKFS job to allocate and mount the user file system, the job uses your installation defaults. If AUTOMOVE=Y is in effect for your installation, the following message might be displayed when the system is shut down:

```
BPXM048I BPXOINIT FILESYSTEM SHUTDOWN INCOMPLETE.
1 FILESYSTEM IS 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 example.

For more information about the AUTOMOVE setting, see *z/OS UNIX System Services Planning*.

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.

By default, the z/OSMF started task user ID home directory is `/var/zosmf/data/home/izusvr`. It is recommended that you do not auto-manage this directory. If the z/OSMF started task user ID home directory must reside in an auto-managed directory, however, you must pre-create the directory before you run the IZUMKFS job.

If the z/OSMF started task user ID home directory is controlled by the automount facility, you must either disable the automount rule for this mount point before you run the IZUMKFS job, or perform the following steps manually before you run the job:

1. Configure your automount policy for the z/OSMF started task user ID home directory.
2. Allocate the data set that contains the z/OSMF started task user ID home directory. In this example, assume that you want to place the z/OSMF started task user ID home directory in `/u/izusvr`
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 /u/izusvr`
   b. `chown IZUSVR:IZUADMIN /u/izusvr`

For more information about the automount facility, see *z/OS UNIX System Services Planning*.

Reviewing the IPCMSGQBYTES option of BPXPRMxx

The z/OS data set and file REST interface uses the z/OS UNIX System Services interprocess communications (IPC) message queue for communications between TSO and z/OSMF. The maximum message size is controlled by the size of the queue that is defined by the IPCMSGQBYTES option of parmlib member BPXPRMxx.

Message sizes that are used by the z/OS data set and file REST interface services vary based on the request type and amount of data that is returned in the response. Review the setting of IPCMSGQBYTES

on your system (by using the D OMVS,O operator command) to ensure that it is large enough for the messages that are sent by the z/OS data set and file REST interface services.

It is recommended that the IPCMSGQBYTES value be at least 16777216 (16 M). To set this value, you can enter the following command:

```
SETOMVS IPCMSGQBYTES=16777216
```

For more information, see the topic about BPXPRM*xx* in *z/OS MVS Initialization and Tuning Reference*.

Optionally creating a IZUPRMxx parmlib member

You might find that the z/OSMF configuration defaults are sufficient for your environment; if so, use the defaults for a quick-start experience with z/OSMF. If your z/OSMF set-up requires customization, you can provide a customized member, IZUPRMxx, with installation-specific values for your configuration. IBM provides a sample member, IZUPRM00, which you can use as a model.

IZUPRMxx is optional. Before you create this member, review the z/OSMF defaults, which are described in this topic, to determine whether the values are sufficient for your installation. Provide an IZUPRMxx member only if you need to override one or more of the z/OSMF defaults.

To create an IZUPRMxx parmlib member, follow these steps:
1. Copy the sample parmlib member into the desired parmlib data set with desired suffix.
2. Update the parmlib member as needed.
3. Specify the parmlib member suffix on the command that is used to start the z/OSMF server. For information, see "Specifying a job name and other parameters" on page 32.

Tip: Specify values only for those defaults that you want to override. Omit any statement for which the default value is acceptable. Doing so will ensure that you always obtain the default values, even if they happen to change in a future release.

Syntax rules for IZUPRMxx

For general rules of parmlib member syntax, see *z/OS MVS Initialization and Tuning Reference* .

Additionally, the following rules apply to the creation of IZUPRMxx parmlib members:

- Use columns 1-71 for data; columns 72-80 are ignored.
- If a statement is omitted, the default is used.
- Enter one or more statements on a line, or use several lines for one statement.
- Use blanks as delimiters. The system interprets multiple blanks as a single blank. You can use blanks between parameters and values. For example, all of the following parameter specifications are equally valid:

  ```
  SESSION_EXPIRE(495)
  SESSION_EXPIRE     (495)
  SESSION_EXPIRE ( 495 )
  ```
- Comments can appear in columns 1-71 and must begin with slash-asterisk and end with asterisk-slash. Any number of blank lines can appear between statements to improve readability.
- Enter values in uppercase, lowercase, or mixed case. The system converts input to uppercase, unless the values are enclosed in single quotation marks, which are processed without altering the case.

  These values might require mixed casing, and should therefore be enclosed in single quotation marks:
  - INCIDENT_LOG UNIT
  - JAVA_HOME
  - KEYRING_NAME
  - LOGGING
  - SAF_PREFIX
  - TEMP_DIR
- Enclose any value that contains special characters in single quotation marks.
- You can use system symbols in IZUPRMxx. Suppose, for example, that your installation defines a symbol in IEASYMxx for the Java directory, such as `JAVA71='/usr/lpp/java/J7.1_64'`. To reference this symbol on the JAVA_HOME parameter in IZUPRMxx, specify the symbol as follows: `JAVA_HOME(&JAVA71)`.
- Enclose any value that is the same as a keyword in single quotation marks, so that the system interprets the value as a value and not as a keyword.

- Enclose values in single quotation marks, according to the following rules:
  - Two single quotation marks next to each other on the same line are processed as a single quotation mark. For example, the system interprets `Jane''s file` as `Jane's file`.
  - If a value is longer than 72 characters, it requires multiple lines. Specify the value in columns 1-71 and use as many subsequent lines as necessary in columns 1-71. For a value that spans multiple lines, place one quotation mark at the beginning of the value, stop the value in column 71 of the line, continue the value in column 1 of the next line, and complete the value with one quotation mark. Use as many lines as necessary to define the value.
- You can specify multiple IZUPRMxx parmlib members by using concatenation. If the same statement is used more than once, either in the same member or in multiple members, the value from the last occurrence is used. For example, suppose that your installation uses two members, IZUPRM01 and IZUPRM02. If the HOSTNAME parameter is specified in both IZUPRM01 and IZUPRM02, the system uses the HOSTNAME value from IZUPRM02.

Syntax format of IZUPRMxx

```
HOSTNAME('*')
HTTP_SSL_PORT(443)
INCIDENT_LOG UNIT('SYSALLDA')
JAVA_HOME('&JAVA71_HOME')     /* System symbol used to define home */
KEYRING_NAME('IZUKeyring.IZUDFLT')
LOGGING('*=warning:com.ibm.zoszmf.*=info:com.ibm.zoszmf.environment.ui=finer')
RESTAPI_FILE ACCT(IZUACCT) REGION(65536) PROC(IZUFPROC)
SAF_PREFIX('IZUDFLT')
SEC_GROUPS USER(IZUUSER),ADMIN(IZUADMIN),SECADMIN(IZUSECAD)
SESSION_EXPIRE(495)
TEMP_DIR('/tmp')
UNAUTH_USER(IZUGUEST)
WLM_CLASSES DEFAULT(IZUGHTTP)
            LONG_WORK(IZUGWORK)

/* Uncomment the following statement and any plugins that are desired */
/* PLUGINS( INCIDENT_LOG,COMMSERVER_CFG,WORKLOAD_MGMT,RESOURCE_MON,CAPACITY_PROV, SOFTWARE_MGMT,ISPF)   */
```

IBM-supplied defaults for IZUPRMxx

There is no default IZUPRMxx parmlib member. SYS1.SAMPLIB provides a sample parmlib member, IZUPRM00.

"Syntax format of IZUPRMxx" shows the IBM-supplied IZUPRM00 member. Note that the PLUGINS statement is commented out; to use it, you must remove the comment characters.

Statements and parameters for IZUPRMxx

HOSTNAME(*hostname*)

Specifies the host name, as defined by DNS, where the z/OSMF server is located. To use the local host name, enter asterisk (*), which is equivalent to `@HOSTNAME` from previous releases. Or, you can specify a dynamic VIPA (DVIPA) that resolves to the correct IP address.

Rules:
- Consists of alphabetic letters (A-Z), numeric digits (0-9), hyphens(-), and periods (.)
- Consists of 1 to multiple sections (labels) of 1-63 characters that are separated by a period (.)
- The maximum length of this value, including periods, is 253 characters
- Alphabetic characters are case insensitive
- Each section must start and end with either an alphabetic character (A-Z) or numeric digit (0-9). For example: `WWW.IBM.COM`

Default: *

HTTP_SSL_PORT(*nnn*)
Identifies the port number that is associated with the z/OSMF server. This port is used for SSL encrypted traffic from your z/OSMF configuration. The default value, 443, follows the Internet Engineering Task Force (IETF) standard.

Value range: 1 - 65535 (up to 5 digits)

Default: `443`

INCIDENT_LOG UNIT('*device-name*')
Specifies the device to be used for storing data sets and z/OS UNIX files for the FTP jobs. This parameter is applicable if your configuration includes the Incident Log plug-in.

Rules:
- Must consist of 1 to 72 characters, including alphanumeric characters (A-Z, a-z, and 0-9)
- Can include the following special characters: hyphens(-), parentheses (), commas (,), equal signs (=), or forward slash (/)

Default: `SYSALLDA`

JAVA_HOME('*directory-name*')
Specifies the home directory (the fully qualified path name) for IBM 64-bit SDK for z/OS, Java Technology Edition V7 on your system.

Rules:
- Must contain no more than 1024 characters, case sensitive
- Must begin with a forward slash (/)
- Must include the full or absolute path name, and a maximum of 255 characters between slashes
- Cannot contain a null

Default: `/usr/lpp/java/J7.1_64`

KEYRING_NAME('*keyring-name*')
Specifies the key ring name for the z/OSMF server. The format is `IZUKeyring.<SAF_PREFIX>`.

Rules:
- Must consist of 1-237 characters, case sensitive
- Can contain any characters, except ampersand (&), asterisk (*), or percent (%)

Note: The IZUSEC job contains statements that include the generation of digital certificates and the key ring. The value that is specified here must match the key ring name that you defined for z/OSMF in the IZUSEC job or by entering equivalent commands.

Default: `IZUKeyring.IZUDFLT`

LOGGING('*trace_specification*')
Initial trace state for the z/OSMF server. These settings are read when the server is started. This value is provided by IBM Support. If there is a problem with starting the server, this value is used to enable tracing for server startup.

Rules: Limited to 2048 characters, case sensitive.

Default: `*=warning:com.ibm.zoszmf.*=info:com.ibm.zoszmf.environment.ui=finer`

RESTAPI_FILE ACCT(*account-number*) REGION(*region-size*) PROC(*proc-name*)
Specifies values for the TSO logon procedure that is used internally by the z/OS data set and file REST interface services. It is recommended that you use the defaults, which should be adequate for most z/OS installations. If you specify alternative values, you must ensure that the z/OSMF user and

z/OSMF administrator security groups are authorized to the logon procedure name and account number that you specify, and that the region size is at least 65536 kilobytes (KB). For information, see "Updating your system for the z/OS data set and file REST interface" on page 18.

All z/OSMF users must have a TSO segment that is defined in the security management product, such as RACF. Failure to have a TSO segment prevents some z/OSMF functions from working.

ACCT(*account-number*)
TSO account number to be used for the logon procedure for the z/OS data set and file REST interface services.

Rules: 1 - 40 alphanumeric characters (A-Z, a-z, 0-9) or special characters (#, $, or @).

Default: IZUACCT

REGION(*region-size*)
Region size (in kilobytes) to be used for the logon procedure for the z/OS data set and file REST interface services.

Value range: 65536 – 2096128

Default: 65536

PROC(*proc-name*)
TSO logon procedure to be used for operations with the z/OS data set and file REST interface services. It is recommended that you accept the default procedure, IZUFPROC, which is supplied by IBM as a cataloged procedure in proclib.

Rules: 1 to eight alphanumeric characters (A-Z, a-z, 0-9) or special characters (#, $, or @).

Default: IZUFPROC

SAF_PREFIX('IZUDFLT')
SAF profile prefix that is prepended to the names of any resource profile names to be used for the z/OSMF core functions and optional plug-ins.

Note: The IZUxxSEC sample jobs contain commands that include the SAF profile prefix for creating resource profile names. The value that is specified here must match the prefix name that you define for z/OSMF in the IZUxxSEC jobs or by entering equivalent commands.

Default: IZUDFLT

SEC_GROUPS USER(*group-name*),ADMIN(*group-name*),SECADMIN(*group-name*)
Specifies group names for the base set of z/OSMF security groups: user, administrator, and z/OS security administrator.

USER(*group-name*)
Security group to be used for the z/OSMF user role. The user IDs that are connected to this group are considered to be z/OSMF users.

Default: IZUUSER

ADMIN(*group-name*)
Security group to be used for the z/OSMF administrator role. The user IDs that are connected to this group are considered to be z/OSMF administrators.

Default: IZUADMIN

SECADMIN(*group-name*)
Group name to be used for the z/OS Security Administrator role. This group is permitted to the Workflows task.

Default: IZUSECAD

SESSION_EXPIRE(*nnn*)
Amount of time (in minutes) for the session timeout. z/OSMF user sessions expire when this period elapses. For information, see "Re-authenticating in z/OSMF" on page 122.

Value range: 30-999999

Default: 495

TEMP_DIR('*path-name*')
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 Incident Log plug-in.

Rules:
- Must contain no more than 1024 characters, case sensitive
- Must begin with a forward slash (/)
- Must include the full or absolute path name, and a maximum of 255 characters between slashes
- Cannot contain a null

Default: `/tmp`

UNAUTH_USER(*user-id*)
Represents an unauthenticated user. Provides an unknown user with basic privileges to access the Welcome page, but nothing more.

Default: `IZUGUEST`

WLM_CLASSES DEFAULT(*class-name*)
Specifies the WLM transaction classes for managing z/OSMF work.

DEFAULT(*class-name*)
WLM transaction class to be used for managing z/OSMF work, except for long-running work, which is managed through the LONG_WORK(*class-name*) statement.

Rules:
- Each class name is 1-8 characters, not case sensitive
- First character must be an alphanumeric
- Remaining characters must be alphanumeric or special characters

Default: `IZUGHTTP`

LONG_WORK(*class-name*)
WLM transaction class to be used for managing the execution of long-running work. This setting is applicable when your configuration includes the Software Deployment optional plug-in.

Rules:
- Each class name is 1-8 characters, not case sensitive
- First character must be an alphanumeric
- Remaining characters must be alphanumeric or special characters

Default: `IZUGWORK`

PLUGINS(plugin-id,plugin-id,plugin-id,...)
Specifies the plug-ins for your configuration. Enter one or more of the following plug-in identifiers:

- INCIDENT_LOG
- COMMSERVER_CFG
- WORKLOAD_MGMT
- RESOURCE_MON
- CAPACITY_PROV
- SOFTWARE_MGMT
- ISPF

Default: No optional plug-ins are specified.

Example of IZUPRMxx parmlib member

In the example that follows, an IZUPRMxx parmlib member is used to set these values:

- Port 30443
- System symbol for the Java home directory. The symbol must also be defined in your IEASYMxx member.

```
HTTP_SSL_PORT(30443)
JAVA_HOME('&JAVA71_HOME')     /* System symbol used to define Java home */
```

Creating a base z/OSMF configuration

For a new installation of z/OSMF, it is recommended that you begin by creating a base configuration of z/OSMF. Here, you create a minimal instance of z/OSMF without enabling any of the optional plug-ins.

Before you begin

Before continuing with the z/OSMF configuration process, ensure that the following work is done.

1. z/OSMF is installed on your z/OS system and the appropriate program directory jobs have been run. See *z/OS V2R2 Program Directory* .

   The examples in this document assume that your installation used the default product directories when installing z/OSMF.
2. You completed the planning checklist for a first time installation in Chapter 2, “Project plans for configuring z/OSMF,” on page 7.
3. You reviewed the z/OSMF configuration default values to ensure that they are acceptable for your environment. If not, you can specify alternative values by using an installation-supplied IZUPRMxx parmlib member, as described in “Optionally creating a IZUPRMxx parmlib member” on page 22.

Who is needed to configure z/OSMF?

Most of the steps involved in configuring z/OSMF are performed by the z/OSMF installer and the security administrator. In this document, it is assumed that your security administer has a user ID with the RACF SPECIAL attribute. Also involved in the configuration process are the system programmer and the z/OS operator.

Table 6 shows the performer for each step of the z/OSMF configuration process.

Table 6. Actions and performers for configuring z/OSMF

Step to perform	Performed by
“Step 1: Run the security commands for the z/OSMF resources” on page 28.	Security administrator
“Step 2: Allocate and mount the z/OSMF file system” on page 29.	z/OSMF installer
“Step 3: Start the z/OSMF server” on page 31.	z/OS operator

Table 6. Actions and performers for configuring z/OSMF (continued)

Step to perform	Performed by
"Step 4: Access the z/OSMF Welcome page" on page 35.	Any authorized z/OSMF user or the z/OSMF installer
"Step 5: Log into z/OSMF" on page 36	Any authorized z/OSMF user or the z/OSMF installer

Selecting a user ID for configuration

Select a user ID to use for running the IZUMKFS job on your system. This user ID requires superuser authority.

Superuser authority is required so that you can update your system by:
- Creating directories
- Allocating and mounting the z/OSMF user file system
- Changing directory ownership and permissions.

Besides superuser authority, the installer user ID also requires update authority to the parmlib data set for any members that are to be modified during the z/OSMF configuration process.

After z/OSMF is configured, remember the installer user ID and keep it active for future operations with z/OSMF. You will use this same user ID for all subsequent work with the administration tasks that you perform, such as adding links and modifying the Welcome page.

About superuser authority

There are three ways to assign superuser authority in z/OS:
- Using UNIXPRIV class profiles, which is the recommended way. To run the IZUMKFS job, your user ID requires the following UNIXPRIV class profile privileges:
  - CONTROL access to SUPERUSER.FILESYS
  - UPDATE access to SUPERUSER.FILESYS.MOUNT
  - READ access to SUPERUSER.FILESYS.CHOWN
  - READ access to SUPERUSER.FILESYS.CHANGEPERMS
  - READ access to SUPERUSER.FILESYS.PFSCTL
- 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*. 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*.

Step 1: Run the security commands for the z/OSMF resources

In this step, your security administrator runs the job IZUSEC to create security authorizations for the z/OSMF core functions. It is strongly recommended that your security administrator review the contents of the job before running it.

About this step

The job IZUSEC contains RACF commands for creating profiles for resources that are used by the z/OSMF core functions. The job also contains commented sections for additional authorizations that might be applicable for your installation.

During this step, you will:

- Select a started task user ID to use for running the z/OSMF server. In the job IZUSEC, the server user ID is IZUSVR, by default.
- Define the security groups for z/OSMF users. At a minimum, the groups should include the following:
  - Administrator group
  - User group
  - z/OS security administrator group.

If your installation uses a security management product other than RACF, ask your security administrator to create equivalent commands for your security product.

Before running the job

Have your security administrator review the job and modify it as necessary for your security environment.

For a RACF installation, ensure that the following security classes are active before you run the job:
- APPL
- EJBROLE
- FACILITY
- SERVER
- STARTED
- ZMFAPLA

To list the currently active security classes, your security administrator can enter the **SETROPTS LIST** command.

Commands for activating the classes are included in commented sections in the IZUSEC job. To have the commands issued when the job runs, uncomment the sections. Or, your security administrator can enter the commands directly, as shown in "Class activations that z/OSMF requires" on page 181.

A user connected to the z/OSMF administrator group or the z/OSMF user group might be connected to other security groups. To allow such users to access z/OSMF without having to log in under a specific group, it is recommended that you have list-of-groups authority checking (GRPLIST option) active. For more information, see *z/OS Security Server RACF Security Administrator's Guide*.

Running the job

Authority
This job is run by your security administrator. It is assumed that this user ID has the SPECIAL attribute, which gives the user full control over all of the RACF profiles in the RACF database.

Location
The job resides in SYS1.SAMPLIB(IZUSEC).

Invocation
Submit IZUSEC as a batch job.

Results

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

If the job is run more than once, message IKJ56702I INVALID *data* is issued for any user IDs or groups that were defined previously. You can ignore this message.

Step 2: Allocate and mount the z/OSMF file system

In this step, you run the job IZUMKFS to define, format, and temporarily mount the z/OSMF user file system.

About this step

The job IZUMKFS initializes the z/OSMF user file system, which contains configuration settings and persistence information for z/OSMF.

The job performs the following actions:

- Allocates the z/OSMF user file system as `/var/zosmf`.
- Mounts the file system at mount point `/var/zosmf`:
  - As a zFS type file system
  - With the option PARM('AGGRGROW') to allow the file system to grow dynamically, as needed
  - With the option UNMOUNT to ensure that it is unmounted if the z/OS system becomes unavailable
- Creates the home directory for the z/OSMF started task. By default, the directory is `/var/zosmf/data/home/izusvr`.
- Changes the ownership and permissions and ownership of the directories and files in the z/OSMF user file system, as follows:
  - The file system is owned by the IZUSVR user ID and the IZUADMIN security group
  - The file system is protected with the permissions 755

Storage consideration for the Workflows task

Each workflow instance on your z/OS system uses a portion of the storage allocated to the z/OSMF user file system. This storage remains allocated until the instance is deleted by the user, and the storage is later released by a z/OSMF cleanup process.

In general, larger workflows consume more system resources than smaller workflows. The use of complex workflows with many steps and variables can cause the user file system to expand significantly beyond its initial allocation. If your installation plans to use large or complex workflows, consider specifying a larger initial allocation for the user file system. By default, the initial allocation is 200 cylinders.

Also, be aware that user activities with workflows, such as creating an instance or performing workflow steps, use some additional pageable memory in the z/OSMF server address space. The amount varies, based on the number and size of the workflow instances on your system.

Before running the job

Create a copy of the job SYS1.SAMPLIB(IZUMKFS). In your copy of the IZUMKFS job, do the following:

1. Note that the data set name for the new file system is IZU.SIZUUSRD. If you select another name for this data set, be sure to rename all occurrences of the data set name in the job.
2. Select a volume for allocating the new file system. Replace *volser* in the following specification with an appropriate volume:

   ```
   VOLUMES(volser)
   ```
3. Note that the job mounts the z/OSMF file system at mount point `/var/zosmf`. To support running z/OSMF in a sysplex-wide scope, update the job to ensure that it mounts the user directory at a shared mount point.

   If you have an existing file system from a previous release of z/OSMF, you can transfer your data to the new file system. If so, you have additional changes, as described in "Configuring the new release of z/OSMF" on page 39.

Running the job

Authority

To run this job, you require a user ID with superuser authority, so that the job can mount the

z/OSMF user file system and issue the **MKDIR** and **CHMOD** commands. It is recommended that you use a user ID from the z/OSMF administrator group, such as IZUSVR. For more information, see "Selecting a user ID for configuration" on page 28.

Location
The job resides in SYS1.SAMPLIB(IZUMKFS).

Invocation
Submit IZUMKFS as a batch job.

Results

On completion, the z/OSMF file system is mounted and the directories are created.

If the job ends with errors, see the troubleshooting actions listed in "Problems during configuration" on page 117.

Adding IPL-time mount commands for the newly created file system

Add the mount commands for the z/OSMF file system data sets to the BPXPRMxx member of your system parmlib. Use the IZUMKFS sample mount commands as a model. For a sample command, see "Ensuring that the user file system is mounted at IPL time" on page 19.

Step 3: Start the z/OSMF server

In this step, you start the z/OSMF server. This topic describes the commands that you can use to control the z/OSMF server and verify that it is running.

Starting the z/OSMF server manually

Before users can access z/OSMF, the z/OSMF server must be active. To start the z/OSMF server manually, you can enter the **START** command from the operator console. The **START** command specifies the procedure name to start and, optionally, the job name to use. For example:

```
START IZUANG1, JOBNAME=jobname
START IZUSVR1, JOBNAME=jobname
```

Start the tasks in the following sequence: IZUANG1 followed by IZUSVR1. Otherwise, z/OSMF users might encounter authorization errors later when they attempt to log in to z/OSMF.

On server initialization, a number of messages are written to the operator console, as follows.

```
  SY1  $HASP100 IZUANG1  ON STCINRDR
- SY1  $HASP373 IZUANG1  STARTED
  SY1  CWWKB0056I INITIALIZATION COMPLETE FOR ANGEL

⋮

  SY1  $HASP100 IZUSVR1  ON STCINRDR
- SY1  $HASP373 IZUSVR1  STARTED

⋮

- SY1  IZUG400I: The z/OSMF Web application services are initialized.
  SY1  +CWWKF0011I: The server zosmfServer is ready to run a smarter planet.
```

When initialization is complete, the z/OSMF server writes message IZUG349I to its job log. Check this message for the link (a URL) for accessing z/OSMF after it is started on your system. Be sure to provide

users with the new URL to use for accessing z/OSMF, as described in "Step 4: Access the z/OSMF Welcome page" on page 35. Users can add the URL to the browser bookmarks list.

In the message, the URL is based on the configured host name. In some installations, a network alteration such as dynamic VIPA (DVIPA) might invalidate this URL. If your network administrator established another means for accessing the z/OSMF application, check with this person on the correct URL to use.

Notes:

1. Consider having the server start automatically at system IPL time. For instructions, see "Ensuring that z/OSMF is started at IPL time" on page 34.
2. If the server cannot be started, ensure that it is set up correctly. For instructions, see "Updating your system for the z/OSMF started procedures" on page 17.

Specifying a job name and other parameters

On the **START** command, you can include program parameters to be passed to the started procedures. It is recommended that you use this method to control the started task behavior, rather than modifying the started procedures directly.

For example, you might choose to specify a job name to give the started procedures a user identification. To do so, include the JOBNAME= parameter on the **START** command, as follows:

```
START IZUANG1, jobname=myjob
```

When you specify a job name for the started procedure, the job name is used as part of the resource name that is passed to your security management product, such as RACF. If you plan to run the z/OSMF started tasks under a job name, ensure that the job name is defined in a security profile in your security management product.

If you omit the JOBNAME= specification, the default member names are used: IZUANG1 and IZUSVR1.

In addition to job name, you can also specify the following settings on the **START** command:

IZUPRM=(*nn*, *nn*, *nn*)
: Suffixes of one or more IZUPRMxx parmlib members that set the configuration options for z/OSMF. This keyword defaults to `NONE`; no parmlib members are specified and the z/OSMF defaults are used. If you specify a suffix, the member must exist in your parmlib concatenation. Otherwise, the start command fails. Multiple suffixes must be enclosed in parentheses.

  The following syntax forms are valid:

  ```
  IZUPRM=(xx,yy,...)
  IZUPRM=xx
  IZUPRM=NONE
  ```

  Default: `NONE`

ROOT='*directory-path*'
: z/OSMF root code directory path. By default, the procedures use directory path `/usr/lpp/zosmf`. If your installation configured z/OSMF to use another path for the root code directory, specify that value here, for example: ROOT='/the/new/code/root'.

  The directory path must:
  - Be enclosed in quotation marks
  - Begin with a forward slash ('/')
  - Be fully qualified (it cannot be relative)

  Mixed-case file system names are supported.

  Default: `/usr/lpp/zosmf`

OUTCLS='*output-class*'
Suitable output class for writing system output. By default, the z/OSMF procedures use output class `*`. If you prefer another destination, such as `A`, you can include a OUTCLS= specification on the **START** command:

```
START IZUANG1,OUTCLS='A'
START IZUSVR1,OUTCLS='A'
```

The value must be in quotation marks.

Default: `*`

USERDIR='*directory-path*'
z/OSMF user directory path. This value is used by the IZUSVR1 procedure only; it is not used by the IZUANG1 procedure. By default, the IZUSVR1 procedure uses the directory `/var/zosmf`. If your installation configured z/OSMF to use another path for the user directory, specify that value here, for example: USERDIR='/the/new/config/dir'.

The directory path must:
- Be enclosed in quotation marks
- Begin with a forward slash ('/')
- Be fully qualified (it cannot be relative)

Mixed-case file system names are supported.

Default: `/var/zosmf`

IZUMEM='*maxmemlimit* | NOLIMIT'
Maximum amount (*maxmemlimit*) of usable, above-the-bar, virtual storage for the z/OSMF server address space. This value is used by the IZUSVR1 procedure only; it is not used by the IZUANG1 procedure. This value can be expressed in megabytes (M), gigabytes (G), terabytes (T), or petabytes (P). *nnnnn* can be a value 0 - 99999, with a maximum value of 16384P. By default, the limit is 4 gigabytes (4G).

To select another storage limit, such as 8 gigabytes (8G), you can include an IZUMEM= specification on the **START** command, for example:

```
START IZUSVR1,IZUMEM='8G'
```

Observe the following considerations:
- Your installation SMF setting might override the limit that you set here.
- To indicate no limit to the amount of above-the-bar virtual storage, specify `NOLIMIT`.

Default: `4G`

TRACE='Y | N'
Enables tracing for configuration-time errors, such as parmlib parsing errors. The error data is written to the server job log. Use this option only at the direction of IBM Support.

Do not confuse this option with the LOGGING statement in the IZUPRMxx parmlib member, which is used to trace errors that occur during server operation.

Default: `N`

How to verify that the z/OSMF server is running

To verify that the z/OSMF server is running, you can enter the **DISPLAY** command for the z/OSMF started tasks, IZUANG1 and IZUSVR1.

To verify that started task IZUANG1 is running, enter the following **DISPLAY** command:

```
D A,IZUANG1
```

Figure 5 shows an example of the expected result:

```
- SY1  D A,IZUANG1
     SY1  IEE115I 15.01.02 2012.317 ACTIVITY 021                              C
      JOBS     M/S    TS USERS    SYSAS    INITS   ACTIVE/MAX VTAM     OAS
     00003    00015    00001      00031    00006    00001/00020       00010
      IZUANG1  IZUANG1  STEP1    OWT  SO  A=0036   PER=NO   SMC=000
                                        PGN=N/A  DMN=N/A  AFF=NONE
                                        CT=000.015S  ET=070.712S
                                        WUID=STC00058 USERID=IZUSVR
                                        WKL=SYSTEM   SCL=SYSSTC   P=1
                                        RGP=N/A      SRVR=NO  QSC=NO
                                        00 ADDR SPACE ASTE=01D0DD80
```

Figure 5. Expected result from the **D A,IZUANG1** *command*

To verify that started task IZUSVR1 is running, enter the following **DISPLAY** command:

```
D A,IZUSVR1
```

Figure 6 shows an example of the expected result:

```
    - SY1  D A,IZUSVR1
      SY1  IEE115I 15.01.36 2012.317 ACTIVITY 024                              C
       JOBS     M/S    TS USERS    SYSAS    INITS   ACTIVE/MAX VTAM     OAS
      00003    00015    00001      00031    00006    00001/00020       00010
       IZUSVR1  IZUSVR1  STEP1    IN   SO  A=0037   PER=NO   SMC=000
                                        PGN=N/A  DMN=N/A  AFF=NONE
                                        CT=020.760S  ET=104.749S
                                        WUID=STC00057 USERID=IZUSVR
                                        WKL=SYSTEM   SCL=SYSSTC   P=1
                                        RGP=N/A      SRVR=NO  QSC=NO
                                        00 ADDR SPACE ASTE=01D0DDC0
```

Figure 6. Expected result from the **D A,IZUSVR1** *command*

Ensuring that z/OSMF is started at IPL time

To ensure that z/OSMF is started automatically at IPL time, you can include the start commands for the two procedures in the active COMMNDxx parmlib member for your system. Depending on your system requirements, you might also need to update an automation program to take the appropriate actions in response to starting and stopping the z/OSMF server.

If you choose to defer this step, you must manually start z/OSMF after each system IPL.

Stopping the z/OSMF server

To stop the z/OSMF server, you can use the **STOP** command from the operator console. Enter **STOP** command for each started task in the following sequence:

```
STOP IZUSVR1
STOP IZUANG1
```

Figure 7 on page 35 shows an example of the expected result:

```
stop izusvr1
+CWWKB0001I: Stop command received for server zosmfServer.
$HASP395 IZUSVR1  ENDED

 stop izuang1
 CWWKB0057I WEBSPHERE FOR Z/OS ANGEL PROCESS ENDED NORMALLY
 $HASP395 IZUANG1  ENDED
```

Figure 7. Expected result from the **STOP** *command*

On server shutdown, a number of BBG prefixed messages are written to the z/OSMF log file.

If the **STOP** fails, you can cancel the server by canceling the started tasks in the following sequence: IZUSVR1 followed by IZUANG1.

Step 4: Access the z/OSMF Welcome page

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

The URL for the Welcome page has the following format:

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

where:

- *hostname* is the hostname or IP address of the system in which z/OSMF is installed
- *port* is the secure application port for the z/OSMF configuration. *port* is optional. If you specified a secure port for SSL encrypted traffic during the configuration process (through parmlib statement HTTP_SSL_PORT), that value is required to log in. Otherwise, it is assumed that you are using port 443, the default.

Displaying the Welcome page

Open a web browser to the Welcome page. For the URL, see message IZUG349I, which was written to the z/OSMF server job log, as described in "Step 3: Start the z/OSMF server" on page 31.

Figure 8 on page 36 shows the Welcome page prior to login. Because you have not yet authenticated with z/OSMF by logging in, the header displays *Welcome guest*.

If you encounter errors when opening your browser to the Welcome page, you might need to modify your workstation setup. z/OSMF includes an environment checker, which is a tool you can run to check your browser settings and workstation configuration. For information, see "Verifying your workstation with the environment checker" on page 104.

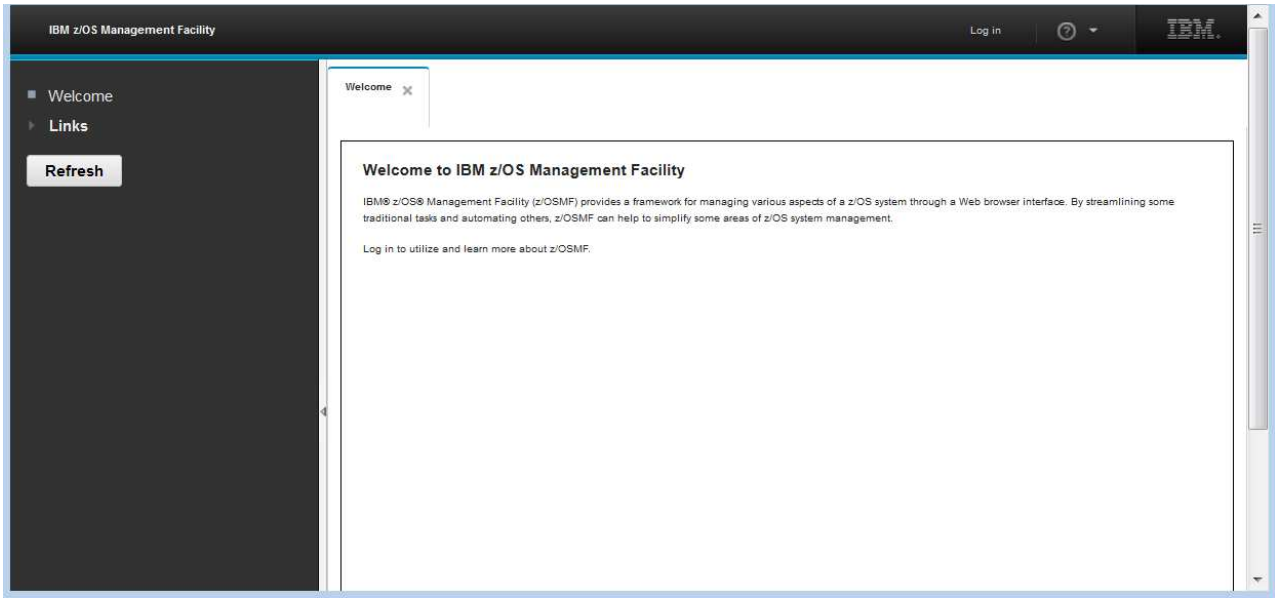


Figure 8. z/OSMF Welcome page (before login)

If you are using the Mozilla Firefox browser, you might see the error message: `Secure Connection Failed`. If so, see "Certificate error in the Mozilla Firefox browser" on page 120 for information.

Step 5: Log into z/OSMF

To log into z/OSMF, enter a valid z/OS user ID and password or pass phrase in the **Log in** field in the navigation area. By default, the z/OSMF configuration process creates security groups for administrator and users. You can use a user ID connected to either group to log in.

Procedure

1. In the **User ID** field in the navigation area, enter the z/OS user ID that you used to configure z/OSMF (the installer user ID).
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 **Log in**.

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.

Figure 9 on page 37 shows the Welcome page as it appears after you have logged in with the installer user ID. Shown are the base functions in the navigation area, such as Notifications and Workflows. In the figure, the z/OSMF Administration and z/OSMF Settings categories are expanded to show the tasks for these categories.

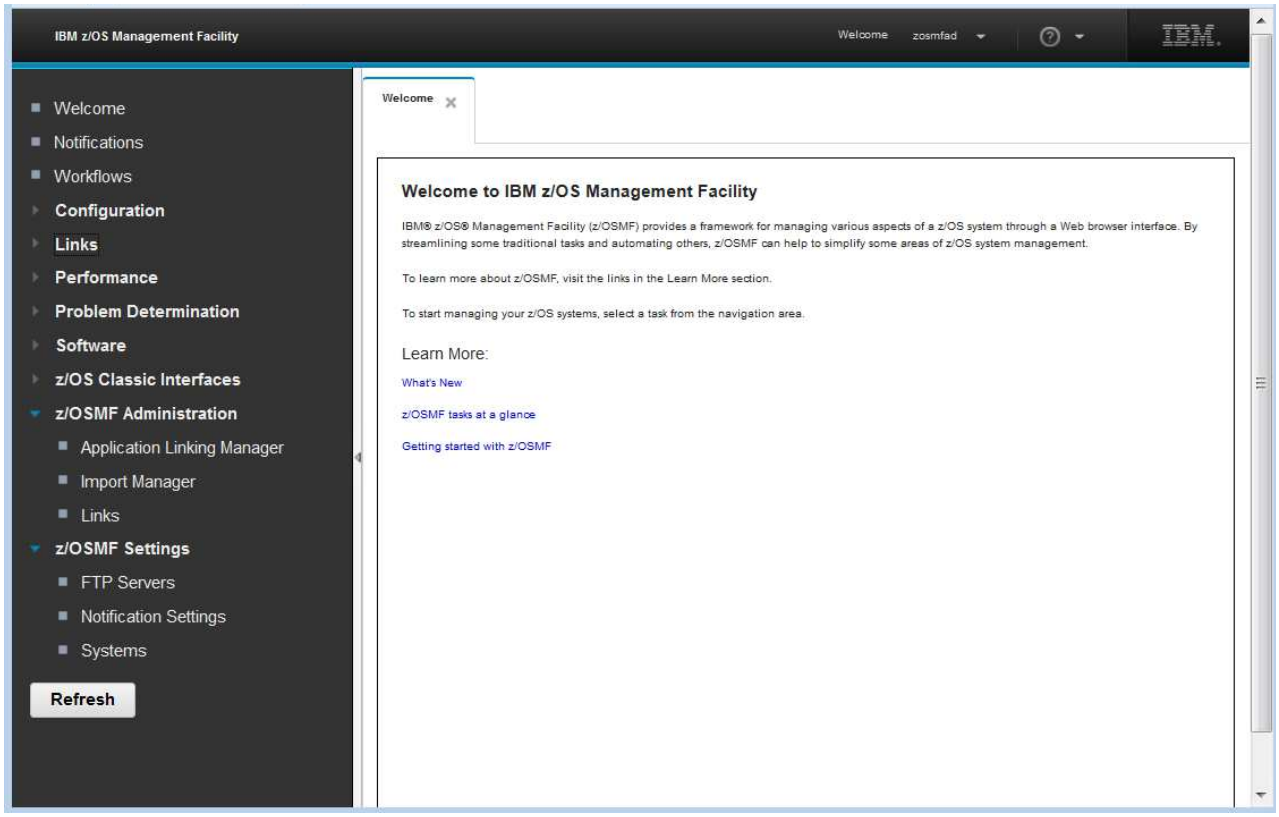


Figure 9. z/OSMF Welcome page (after login)

The Welcome page work area includes the introductory topics: *What's New*, *z/OSMF tasks at a glance*, and *Getting started with z/OSMF*. For an overview of the product, click any of these links to open the corresponding topic in the online help.

Figure 9 shows the Welcome page as it would appear to the installer, who has access to the z/OSMF Administration and z/OSMF Settings categories by default. A user without administrator access would not see these categories.

Later, when you are satisfied with the base configuration, you can add function to z/OSMF through the addition of one or more optional plug-ins. For a summary of the steps, see the project planning checklist "Adding plug-ins to your configuration" on page 9.

What to do next

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

Chapter 4. Migrating to a new release of z/OSMF

This chapter describes how to migrate to z/OSMF V2R2 from your current release. During this stage, you configure a new release of z/OSMF with the objective of making it functionally compatible with the previous release. After a successful migration, the z/OSMF tasks function the same way (or similar to the way) they did on the old system.

This chapter does not explain how to add the new functions in z/OSMF V2R2. After the new release of z/OSMF is established, you can add function through the addition of optional plug-ins, as described in Chapter 7, "Adding plug-ins to a z/OSMF configuration," on page 67.

Configuring the new release of z/OSMF

In this topic, you configure the new release of z/OSMF, supplying the configuration file from your current (old) system as input to the **izumigrate.sh** script. You also allocate and mount the new z/OSMF user file system and start the z/OSMF server.

To migrate your system to the new release of z/OSMF, follow these steps:

1. Perform the migration actions for the z/OSMF element. Depending on whether you are migrating from z/OS V2R1 or V1R13, you might have z/OSMF migration actions to perform on your current (old) system. For example, z/OSMF V1R13 installations are advised to convert to SAF authorization mode before migrating to the new release. For information, see *z/OS Migration*.
2. Run the **izumigrate.sh** script on the new system using the configuration file from your current (old) system as input. The script completes quickly. Instructions for running the script are provided in "Migrating your configuration values to member IZUPRMxx" on page 41.

   The script checks the z/OSMF configuration settings on your current (old) system. If it detects any customized (non-default) settings in your configuration, the script creates an IZUPRMxx member that reflects the configuration settings from your old system. Otherwise, the script completes without creating a member.
3. If an IZUPRMxx parmlib member was created in the previous step, it contains one or more non-default settings for z/OSMF. Browse the member to ensure that its contents are correct for your new system. If the IZUPRMxx member includes a setting for the HOSTNAME parameter, for example, verify that the host name it specifies is correct for your new system. Similarly, verify any other settings in the IZUPRMxx parmlib member.

   Tip: Delete any setting in IZUPRMxx for which the default value is acceptable. The default values are shown in "Statements and parameters for IZUPRMxx" on page 23. If all of the defaults are acceptable, you can skip using the IZUPRMxx parmlib member. Doing so will ensure that you always obtain the default values, even if they happen to change in a future release.
4. If your current (old) system does not include the PTFs for APAR PI32148 and its associated APARs, you might not have the latest set of recommended SAF security authorizations for z/OSMF. IBM provides the IZUSEC job and the IZUxxSEC jobs in SYS1.SAMPLIB to help you create the new authorizations. For a RACF installation, make copies of the jobs and edit and run them as appropriate. The jobs include commented sections for more authorizations that might be needed for your environment. If applicable, update the relevant security commands, based on the contents on the IZUPRMxx member that was created in the previous step. For example, your old system might have specified a unique SAF profile prefix for the resource profile names.

   If your installation uses a security product other than RACF, ask your security administrator to create equivalent commands for your security product.

© Copyright IBM Corp. 2009, 2016

The IZUSEC job is described in "Step 1: Run the security commands for the z/OSMF resources" on page 28. The IZUxxSEC jobs are described in Chapter 6, "Setting up security for the z/OSMF plug-ins," on page 63.

5. Create a copy of the job SYS1.SAMPLIB(IZUMKFS). You can use this job to allocate the z/OSMF file system. In your copy of the IZUMKFS job, do the following:
   a. Note that the data set name for the new file system is IZU.SIZUUSRD. If you select another name for this data set, be sure to rename all occurrences of the data set name in the job.
   b. Select a volume for allocating the new file system. Replace *volser* in the following specification with an appropriate volume: `VOLUMES(volser)`
   c. Ensure that the old file system is remounted at a different mount point; you cannot use `/var/zosmf/data` because that mount point will be used for the new file system.
   d. Enter the mount point of old file system in place of the value `/OldDataFileSystemMountPoint`.
   e. Locate the job step `MIGRATE`, which is commented out. This step contains JCL that you can use to copy the data file system from your old system to the user file system on the new system. Uncomment the step and update it so that it references the data file system to be copied. In previous releases, you specified this directory on the <IZU_DATA_DIR> configuration variable, which, by default, was `/var/zosmf/data`.
6. Stop the z/OSMF server on your system, if it is running:

   ```
   P IZUSVR1
   P IZUANG1
   ```
7. Run the IZUMKFS job. For more information about running this job, see "Step 2: Allocate and mount the z/OSMF file system" on page 29.
8. IBM supplies cataloged procedures for the z/OSMF started tasks, `IZUANG1` and `IZUSVR1`. You must use the z/OS V2R2 versions of these procedures, in place of any previous versions you might have. Ensure that the procedures reside in the JES PROCLIB concatenation for your system, as described in "Installing the z/OSMF cataloged procedures" on page 16. If you use edited versions of these procedures on your old system, use the V2R2 versions of the procedures on your new system and transfer your changes to the new procedures.
9. Start the z/OSMF server on the new system. The server runs as a pair of started tasks on your system: `IZUANG1` and `IZUSVR1`. To start z/OSMF manually, enter **START** commands for the IZUANG1 and IZUSVR1 procedures, in that order.

   On the **START** command for IZUSVR1, you can specify options to control the processing of the server, such as the IZUPRMxx members to use, and tracing options for recording configuration-time errors. In the following example, an IZUPRMxx parmlib member is included on the **START** command:

   ```
   S IZUANG1
   S IZUSVR1,IZUPRM=xx
   ```

   For more information, see "Step 3: Start the z/OSMF server" on page 31.

   On initialization, the server reads in the persistance data from the user directory and creates a z/OSMF instance on your system. The server also writes message IZUG349I to its job log, with the link (a URL) for accessing the z/OSMF Welcome page.
10. Verify the results of your work by opening a web browser to the z/OSMF Welcome page. For information, see "Step 4: Access the z/OSMF Welcome page" on page 35. If you are using the Mozilla Firefox browser, you might see the error message: `Secure Connection Failed`. If so, see "Certificate error in the Mozilla Firefox browser" on page 120 for information.
11. Review the **START** command for z/OSMF in the COMMNDxx parmlib member or your automation product to determine whether additional parameters need to be specified, such as the IZUPRMxx parmlib member to use.

Migrating your configuration values to member IZUPRMxx

This topic describes how to transfer the configuration values from your current (old) system to the new system (z/OS V2R2). To perform this step, you use the IBM-supplied script **izumigrate.sh**. The script creates an IZUPRMxx member for your new system, based on the configuration values from your current (old) system.

About this script

This script migrates your z/OSMF configuration values from your current (old) system to a IZUPRMxx parmlib member on the new system. Perform this step on the new system. The script takes as input the configuration file from your old system. When possible, the script retains your current settings. For any values that are no longer valid for z/OSMF, the script omits the values when it creates the IZUPRMxx parmlib member. For values that already match the z/OSMF defaults, the script omits the values from the IZUPRMxx parmlib member.

If your existing configuration file contains commented sections (it should not; the configuration is not intended to be edited), the script removes this information from the IZUPRMxx parmlib member.

If an IZUPRMxx member already exists at the specified location, the script prompts you for a response to overwrite the existing member. To avoid this prompt, you can include the option -noprompt on the script invocation.

The script can be run on a system with z/OSMF V2R1 or V1R13. Earlier releases are not supported.

Notes on migrating from z/OSMF V1R13

For a z/OSMF V1R13 migration, observe the following considerations:

- If your current (old) system is running z/OSMF V1R13 in Repository Authorization Mode, it is recommended that you convert your existing security setup to SAF Authorization Mode before you migrate your settings to the new system. Doing so requires you to repeat the steps of the z/OSMF configuration process, and specify `IZU_AUTHORIZATION_MODE=SAF` as a configuration property.
- z/OSMF V1R13 included an instance of IBM WebSphere Application Server OEM Edition for z/OS. The **izumigrate.sh** script does not attempt to transfer any customization that your installation might have done for IBM WebSphere Application Server OEM Edition for z/OS.

For the steps, see the edition of *z/OSMF Configuration Guide* for your release of z/OSMF.

Converting properties to parmlib statements

The **izumigrate.sh** script scans the configuration properties and environment variables from your old system. The script uses this input to create comparable settings in the IZUPRMxx parmlib member.

Table 7. Parmlib values that result from running the izumigrate.sh script

Configuration property or environment variable in current (old) release	Parmlib value in the new release
• IZU_APPSERVER_HOSTNAME • izu.hostname in the bootstrap.template file	HOSTNAME
IZU_HTTP_SSL_PORT	HTTP_SSL_PORT
IZU_UNIT_TYPE	INCIDENT_LOG UNIT
IZU_TEMP_DIR	TEMP_DIR
IZU_UNAUTHENTICATED_NAME	UNAUTH_USER
IZU_SAF_PROFILE_PREFIX	SAF_PREFIX

Table 7. Parmlib values that result from running the izumigrate.sh script (continued)

Configuration property or environment variable in current (old) release	Parmlib value in the new release
IZU_WISPF_CONFIGURE IZU_RMF_CONFIGURE IZU_DM_CONFIGURE IZU_WLM_CONFIGURE IZU_CA_CONFIGURE IZU_CP_CONFIGURE	PLUGINS
IZU_RESTAPI_FILE_TSOPROC, IZU_RESTAPI_FILE_ACCTNUM, IZU_RESTAPI_FILE_REGION	RESTAPI_FILE ACCT, REGION, PROC
IZU_ADMIN_GROUP_NAME, IZU_USERS_GROUP_NAME, IZU_ZOS_SECURITY_ADMIN_GROUP_NAME	SEC_GROUPS USER, ADMIN, SECADMIN
izu.ssl.key.store.saf.keyring	KEYRING_NAME
The following izuadmin.env settings: • ltpatimeout • ltpacachetimeout • sessiontimeout	SESSION_EXPIRE
com.ibm.ws.logging.trace.specification	LOGGING
izu.long.transaction.class	WLM_CLASSES DEFAULT, LONG_WORK

Running this script

Run the script from your new system.

Authority
Run this script from a user ID with superuser authority.

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

Location
The script resides in the `/bin` subdirectory of the z/OSMF product directory. By default, this is `/usr/lpp/zosmf/bin`.

Syntax
The script options can be specified, as follows:

```
izumigrate.sh -configDir directory -configFilePath file-path
              -izuprmSuffix nn -parmlibDsn dsname [-noprompt ]
```

Where:

-configDir *directory*
Specifies the name of the z/OSMF configuration directory.

-configFilePath *file-path*
Specifies the name of the configuration file to be used as input for this migration.

-izuprmSuffix *nn*
Specifies the two-character suffix for the IZUPRMxx member to be created.

-parmlibDsn *dsname*
Specifies the parmlib data set name for the IZUPRMxx member to be created or replaced. Specify the fully qualified name of a cataloged data set.

-noprompt
If an IZUPRMxx member already exists at the specified location, the script prompts you for a response to overwrite the existing member. To avoid this prompt, you can include the -noprompt option on the script invocation.

Examples

In the examples that follow, the **izumigrate.sh** script is used to create parmlib member IZUPRM01, based on your current configuration settings. As input, the script uses an existing configuration file (izuconfig1.cfg) from the user directory (/etc/zosmf).

```
izumigrate.sh -configDir /etc/zosmf -configFilePath /etc/zosmf/izuconfig1.cfg
              -izuprmSuffix 01 -parmlibDsn SYS1.PARMLIB
```

If an IZUPRMxx member already exists in the target data set, the script normally prompts you to allow the replacement. You can avoid the prompt by including the noprompt option, as follows.

```
izumigrate.sh -configDir /etc/zosmf -configFilePath /etc/zosmf/izuconfig1.cfg
              -izuprmSuffix 01 -parmlibDsn SYS1.PARMLIB
              -noprompt
```

In these examples, SYS1.PARMLIB is used as the target data set. It is recommended, however, that the IZUPRMxx be placed in the parmlib concatenation for your system, for easier maintenance.

Tip: By default, no log file is created by the script. If you want to save the script output, you can use the z/OS UNIX command, **tee**, to direct the output from the script to a file. For techniques, see *z/OS UNIX System Services User's Guide*. In this example, the output is written to the file izumigrate.sh.output:

```
izumigrate.sh -configDir /etc/zosmf -configFilePath /etc/zosmf/izuconfig1.cfg
                 -izuprmSuffix 01 -parmlibDsn SYS1.PARMLIB
           | tee /var/zosmf/configuration/logs/izumigrate.sh.output
```

Results

On completion, the **izumigrate.sh** script creates an IZUPRMxx member for the new release of z/OSMF. The member is placed in the parmlib data set that you specified on the option -parmlibDsn.

What to do next

Configure z/OSMF, as described in "Configuring the new release of z/OSMF" on page 39.

Chapter 5. Selecting which optional z/OSMF plug-ins to add

In z/OSMF, a *plug-in* is a collection of one or more system management tasks that add function to z/OSMF. When you configure a plug-in, you make its tasks available to users in the z/OSMF navigation area.

z/OSMF includes a number of base functions, which are always enabled when you configure the product. A base configuration of z/OSMF contains only these functions (referred to as *core functions* in this document).

The core functions of z/OSMF include the following:
- Welcome task
- Notifications and Notification Settings tasks
- Workflows task
- Application Linking Manager task
- Import Manager task
- Links task
- FTP Servers task
- Systems task
- The z/OSMF online help system.

For a ServerPac installation, if you select the full system replacement installation type, a base configuration of z/OSMF is set up for you. Here, the configuration is created through a ServerPac post-installation job, using IBM-supplied defaults.

You can add significant function to z/OSMF through the addition of optional plug-ins. Table 8 shows which optional plug-ins are available for configuration in z/OSMF. By default, z/OSMF does not include any of the optional plug-ins.

Table 8. z/OSMF optional plug-ins and associated tasks

Plug-in name	Tasks provided by plug-in	Task description
Capacity Provisioning	Capacity Provisioning	Query the status of the Capacity Provisioning Manager.
Configuration Assistant	Configuration Assistant	Configure TCP/IP policy-based networking functions.
Incident Log	Incident Log	Diagnose system problems, and send diagnostic data to IBM or other vendors for further diagnostics.
ISPF	ISPF	Access traditional ISPF applications.
Resource Monitoring	Resource Monitoring	Monitor the performance of the z/OS, AIX®, Linux, and Windows systems in your enterprise.
	System Status	Quickly assess the workload performance on the systems in your enterprise, and define the systems to be monitored.
Software Deployment	Software Management	Manage your z/OS software inventory, deploy SMP/E packaged and installed software, and generate reports about your software.
Workload Management	Workload Management	Administer and operate WLM, and manage WLM service definitions and policies.

© Copyright IBM Corp. 2009, 2016

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 the plug-ins, review the system setup requirements for each plug-in, as described in Appendix B, "Customizing your z/OS system for the z/OSMF plug-ins," on page 201.

Besides the optional plug-ins that are supplied with z/OSMF, your installation can choose to add applications from other sources (IBM or other vendors) to your configuration. In such cases, a z/OSMF administrator can use the Import Manager task to import the applications into z/OSMF. For more information, see the online help for the Import Manager task.

As an example, z/OS System Display and Search Facility (SDSF) supplies a plug-in for use with z/OSMF. For the installation and customization requirements for a particular application, see the documentation that is provided with the application. For example, the set-up requirements for the SDSF plug-in are described in the topic about z/OSMF considerations in *z/OS SDSF Operation and Customization*.

Further, your installation can create its own applications for use with z/OSMF. For information, see *IBM z/OS Management Facility Programming Guide*.

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" on page 47
- "Configuration Assistant task overview" on page 48
- "Incident Log task overview" on page 49
- "ISPF task overview" on page 51
- "Notifications in z/OSMF" on page 52
- "Notification Settings task overview" on page 53
- "Resource Monitoring task overview" on page 55
- "Software Management task overview" on page 57
- "System Status task overview" on page 59
- "Workflows task overview" on page 60
- "Workload Management task overview" on page 61.

For authenticated users, context sensitive help is accessible at all times to assist with these tasks. In each page, you can click on the help 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 6, "Setting up security for the z/OSMF plug-ins," on page 63.

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. Role definitions can be managed entirely through your security product, based on your installation's requirements and policies. Information about the z/OSMF profiles and resources is provided in Chapter 6, "Setting up security for the z/OSMF plug-ins," on page 63.

Capacity Provisioning task overview

The z/OS Capacity Provisioning Manager can help you to monitor your systems for capacity bottlenecks, and manage the physical capacity of your servers and the defined capacity and group capacity limits in use. Based on On/Off Capacity on Demand (CoD), temporary capacity is activated and deactivated with a policy that you define. The Capacity Provisioning task in z/OSMF provides a browser-based user interface for working with the z/OS Capacity Provisioning Manager. Through this task, you can manage your domain configurations and policies and request various reports on the status of the z/OS Capacity Provisioning Manager.

Figure 10 shows the main page for the Capacity Provisioning task.

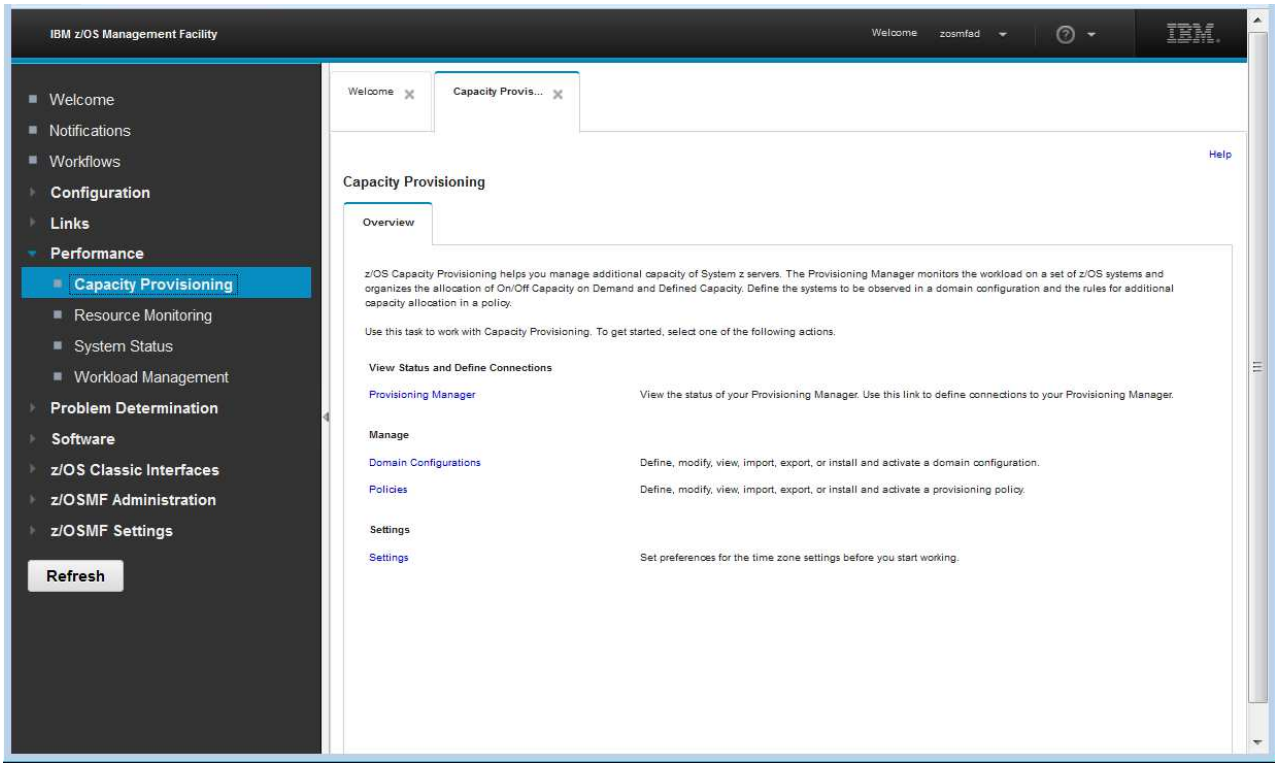


Figure 10. Capacity Provisioning task main page

To open the Capacity Provisioning task, in the navigation area, expand the Performance category and select **Capacity Provisioning**. In the Capacity Provisioning task, the Overview tab provides the launch point for the actions for which your user ID is authorized. If you are authorized to work with domain configurations and policies (*Edit* authorization), the Manage section on the Overview tab is shown. Otherwise, this section is hidden.

Key features

With the Capacity Provisioning task, you can:

- **Manage domain configurations and policies.** You can manage domain configurations and policies. Specifically, you can define new domain configurations and policies, or view or modify existing domain configurations or policies.
- **Install domain configurations and policies.** You can transfer a domain configuration or policy from the z/OSMF repository to the domain configuration or policy repository of your domain.
- **Activate domain configurations and policies.** You can:

  - Change the domain configuration that the provisioning manager uses to control the domain. To do so, select a different configuration from the domain configuration repository.
  - Activate policies from the policy repository.

  You can activate a domain configuration or a policy immediately after it has been installed.
- **Import and export domain configurations and policies.** You can import a domain configuration into z/OSMF from your local workstation or from a domain configuration repository. You can use an export operation to transfer the data in the reverse direction. Similarly, you can import and export policies, but these are stored in the policy repository on the domain.
- **Manage connections to your Provisioning Manager.** You can manage connections to the Provisioning Manager, and use them to transfer provisioning policies and domain configurations to the Provisioning Manager, or to query various status reports. To connect to the Provisioning Manager, you must connect to the CIM server on the system on which the Provisioning Manager runs. You can use the Provisioning Manager running on the same system in which z/OSMF is running, or connect to a remote Provisioning Manager.
- **View the status of your Provisioning Manager.** You can request the following report types:
  - Domain status. This report contains information about the current set-up of the domain that is managed by the Provisioning Manager.
  - Active configuration. This report contains information about the active domain configuration and the status of its elements. Besides the name and the status of the active configuration, you can inspect details about the CPCs and systems that belong to the active configuration.
  - Active policy. This report contains information about the active policy and its status. You can view detailed information about each policy element.

For information about using this task, see the online help.

Configuration Assistant task overview

The Configuration Assistant task can help to simplify the configuration of the TCP/IP policy-based networking functions. This task provides centralized configuration of TCP/IP networking policies and can help reduce the amount of time required to create network configuration files.

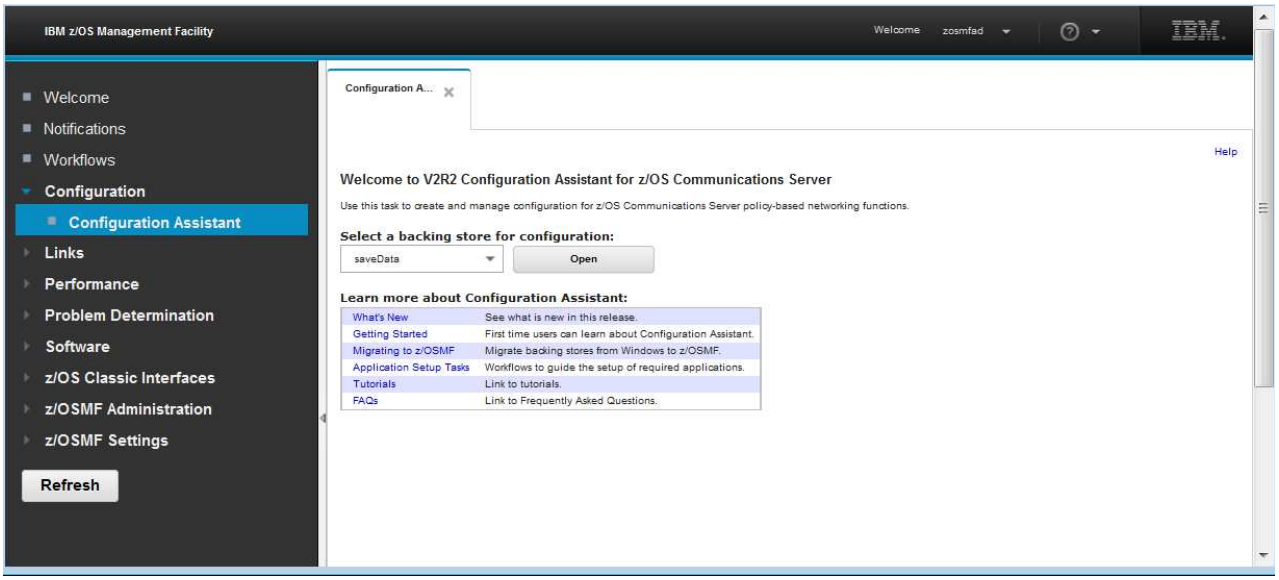


Figure 11. Configuration Assistant task main page

To open the Configuration Assistant task, in the navigation area, expand the Configuration category and select **Configuration Assistant**. The main page for the Configuration Assistant task is displayed, as shown in Figure 11 on page 48.

Key features

With the Configuration Assistant task, you can:

- Create and manage 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 in 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/commserver/zos/support/.

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 12 on page 50 shows a sample view from the Incident Log task.

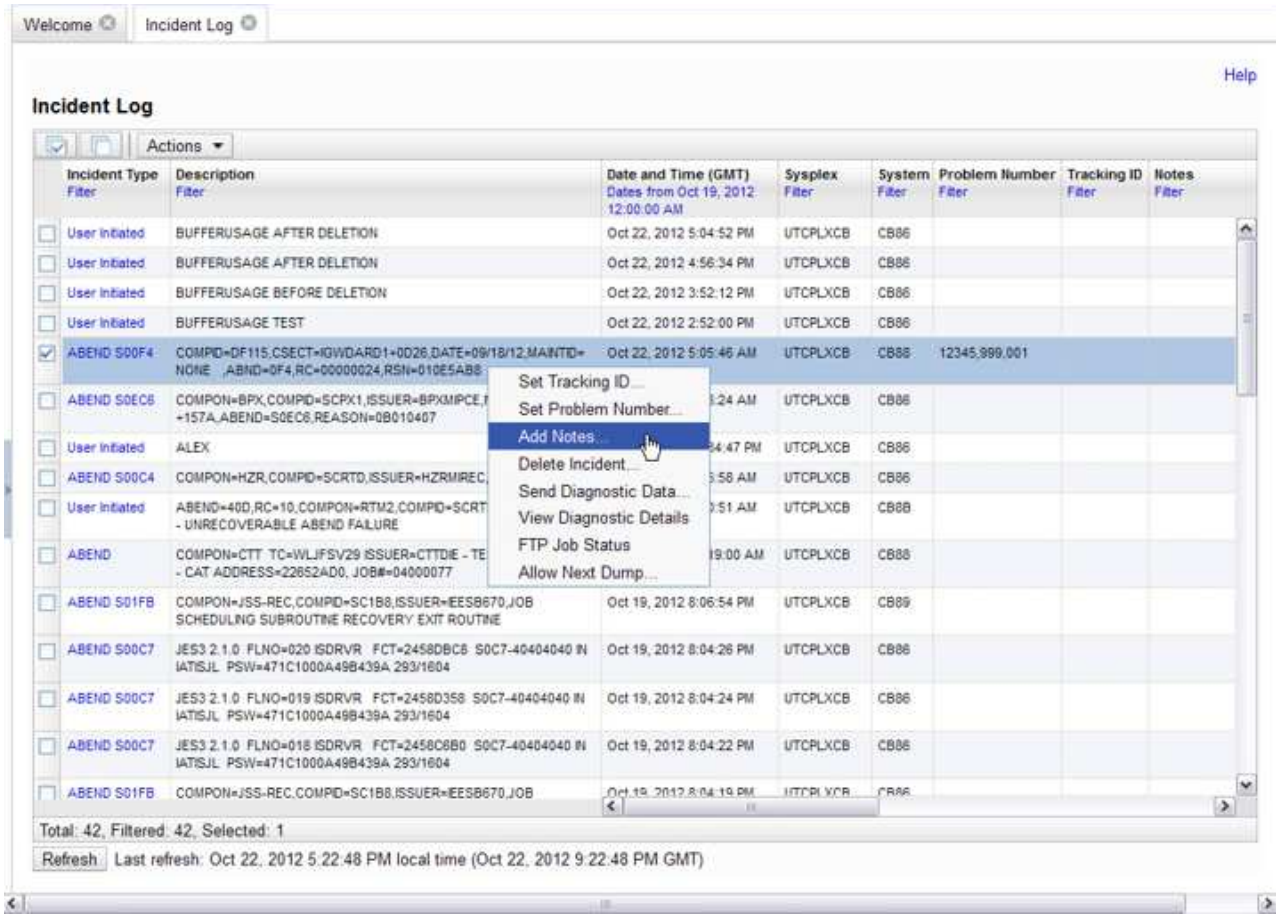


Figure 12. Incident Log task sample view

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

For information about using this task, see the online help.

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.

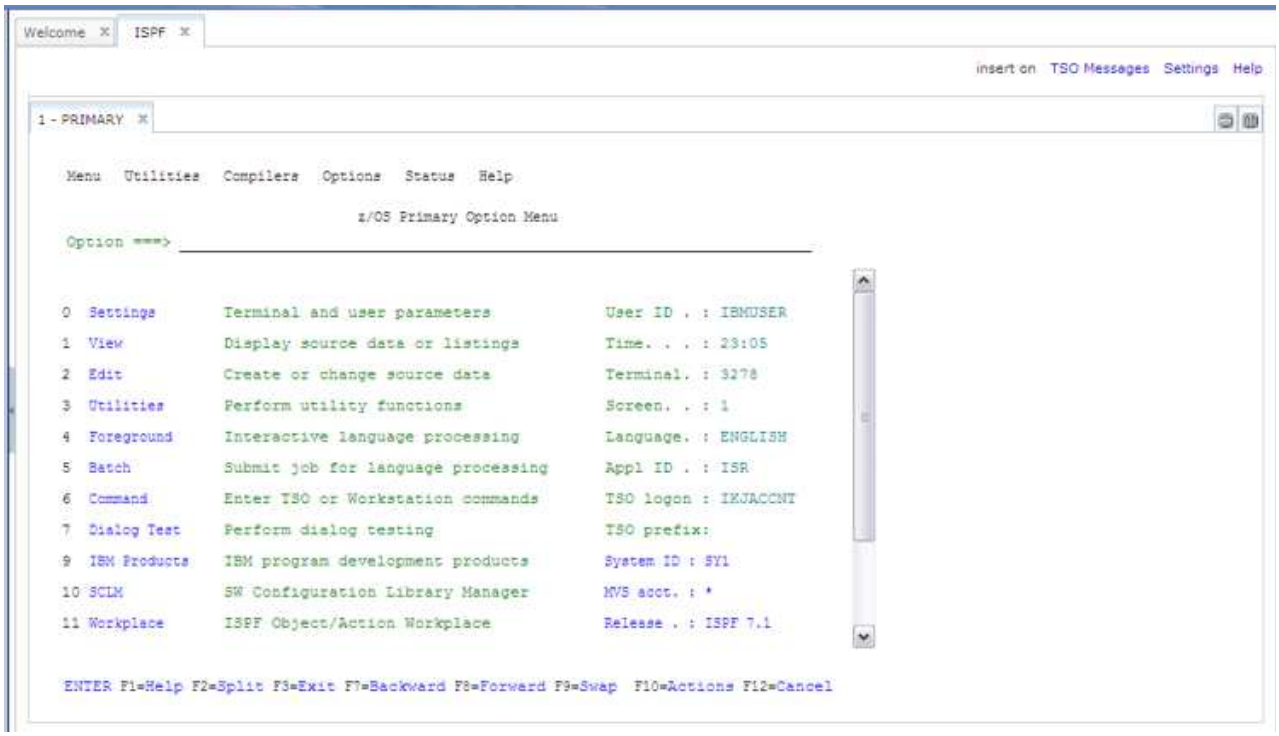


Figure 13. ISPF task main page

Through the ISPF task, you can:

- Access any applications that you usually access through z/OS ISPF on the host system, such as 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.

To open the ISPF task, in the navigation area, expand the z/OS Classic Interfaces category and select **ISPF**. The main page for the ISPF task is displayed, as shown in Figure 13 on page 51.

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, your system is limited to a total of 50 active ISPF task sessions 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.
  - Log in without specifying a valid TSO/E account number in the Account Number field of the ISPF task.
  - 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 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 (SYSTERMID) variable is blank for z/OSMF ISPF task sessions.

For information about using this task, see the online help.

Notifications in z/OSMF

In z/OSMF, a notification is a notice of something that requires your awareness or attention. Notifications might be informational in nature, or might be requests for action from other z/OSMF tasks. The Notifications task of z/OSMF allows you to view and work with the notifications that are assigned to you.

When you have unread notifications, the Notifications task is shown in bold in the navigation area with the number of unread notifications in the form '(*x*).' For example, **Notifications (3)** indicates that you have three unread notifications. When no unread notifications await your attention, the Notifications task is shown without emphasis in the navigation area.

You might receive notifications that have been assigned to:

- Your user ID specifically
- A SAF security group to which your user ID is connected, as defined through your security management product, such as RACF

- One of the predefined z/OSMF roles to which your user ID can be assigned:
  - z/OSMF User
  - z/OSMF Administrator
  - z/OS Security Administrator.

For some notifications, a hyperlink is provided to a z/OSMF task that requires further action. If a notification is displayed as a hyperlink, you can click it to launch the task in a new tab or window.

To display the Notifications task, select **Notifications** in the navigation area. The Notifications task main page is displayed, as shown in Figure 14. The Notifications task is displayed for all authenticated users. Unauthenticated guest users cannot access this task.

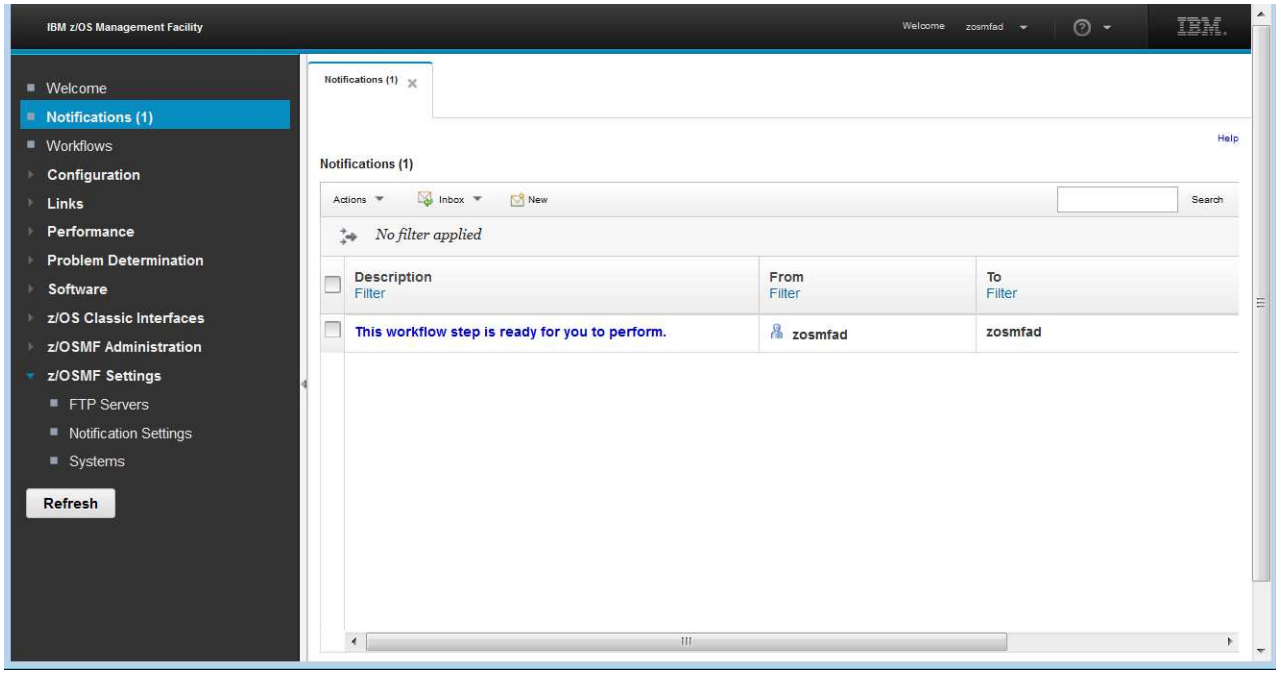


Figure 14. Notifications main page

z/OSMF defines the following limits for notifications, as follows:

Notification expiration
: Notifications expire after 30 days. When this limit is reached, z/OSMF deletes the expired notifications.

Notification maximum
: You can retain a maximum number of 500 notifications. When this limit is reached, new notifications cause the oldest to be deleted.

More information about the Notifications task is provided in the online help.

Notification Settings task overview

Through the z/OSMF notification framework, users can send different forms of notifications to multiple recipients. A notification can be sent to a user's email account or mobile phone. These notifications are received through the Notifications task. You can use the Notification Settings task to define the configuration values that are used for notifications related to z/OSMF tasks and z/OS products.

The Notification Settings task is presented on three tabs, as follows:

User Define where you want to receive notifications, in addition to the Notifications task.

Mobile Configuration
Define devices, map z/OS products, and define push services.

Outgoing Email Configuration
Set the mail server properties.

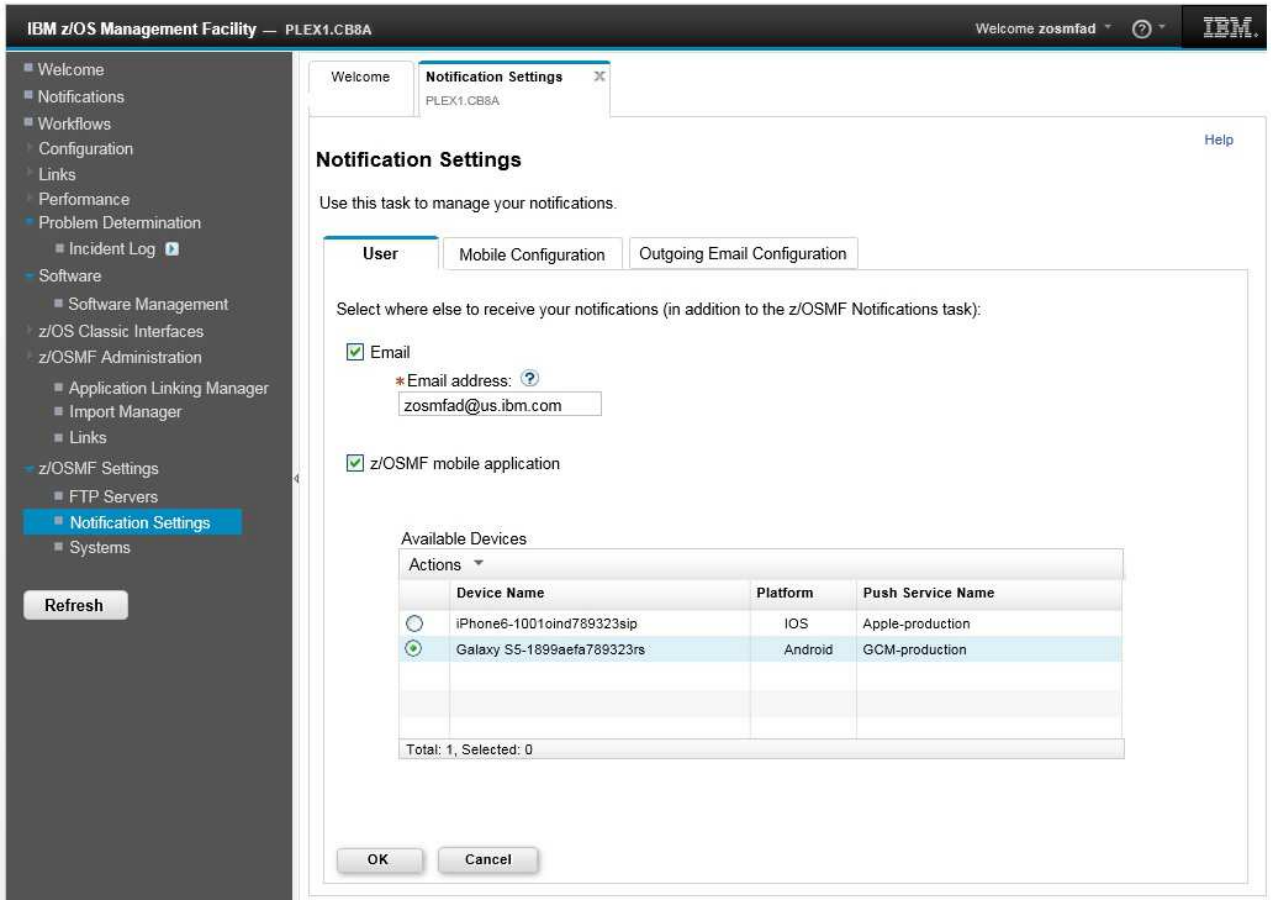


Figure 15. Notification Settings main page

You can use the Notification Settings task to:

- Add a mobile device in z/OSMF and link it with any z/OSMF user ID.
- Manage the mobile devices in groups.
- Define and manage push services and encryption keys in z/OSMF.
- Manage the mapping of product and eventGroup to mobile device or groups of mobile devices.

To display the Notification Settings task, expand the z/OSMF Settings category and select **Notification Settings** in the navigation area. The Notification SettingsNotifications Settings task main page is displayed, as shown in Figure 15.

More information about the Notification Settings task is available in the online help.

Resource Monitoring task overview

The Resource Monitoring task provides a web-based user interface that you can use to monitor the performance of the z/OS, AIX, Linux, and Windows systems in your enterprise. 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, AIX, or Windows 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).

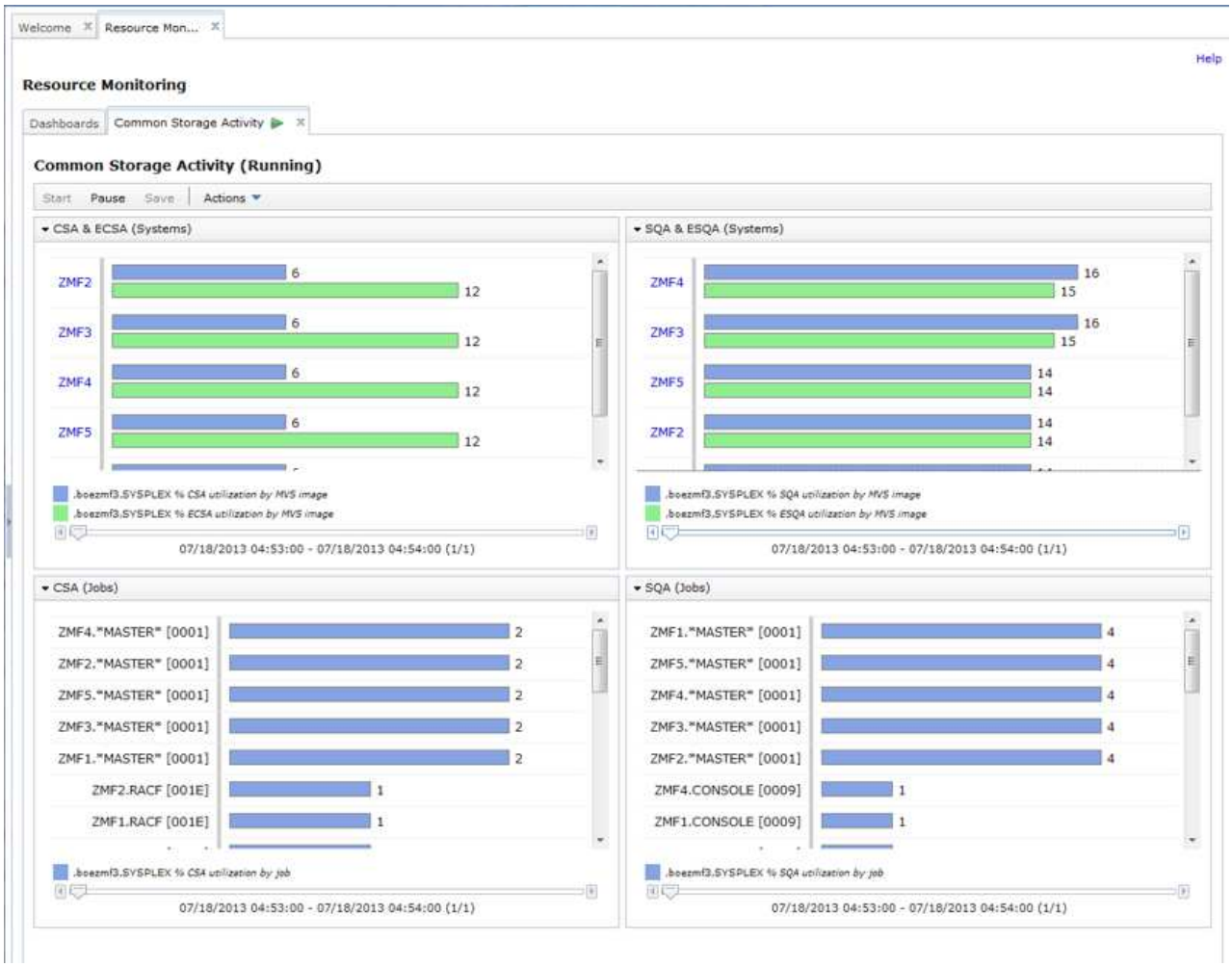


Figure 16. Resource Monitoring task sample view

When the Workload Management plug-in is enabled on your system, the Resource Monitoring task can link automatically to the Workload Management task for additional data. Thus, when the Resource

Monitoring task shows performance data related to a WLM workload, service class, or report class, you can view the corresponding WLM service definition in your z/OSMF session.

To display the Resource Monitoring task, expand the Performance category in the navigation area and select **Resource Monitoring**. Figure 16 on page 55 shows a sample view from the Resource Monitoring task.

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.
- **Retrieve historical data.** You can retrieve and view performance data that the RMF Distributed Data Server has collected in the past for the metric groups contained in a monitoring dashboard.
- **Export performance data to spreadsheet files.** You can export the data collected in monitoring dashboards into CSV format files on your local workstation. Doing so allows you to do further data evaluation using a spreadsheet application.

Before you can start using the Resource Monitoring task, in the System Status task, you must define the z/OS systems and sysplexes to be monitored, as well as any AIX, Linux, and Windows system complexes to be monitored. To display the System Status task, expand the Performance category in the navigation area and select System Status.

Software Management task overview

The Software Management task, previously named the Deployment task, contains the software deployment functions along with additional software management functions. The Software Management task helps you streamline the software management process by providing a centralized location that you can use to manage your z/OS software.

Getting started

To display the Software Management task, in the navigation area, expand the Software category and select Software Management. Figure 17 depicts the main page in the Software Management task.

To start using the capabilities provided in the Software Management task, at least one software instance must be defined. To define a software instance, select **Software Instances**. Then, select **Add** from the Actions menu on the Software Instances page.

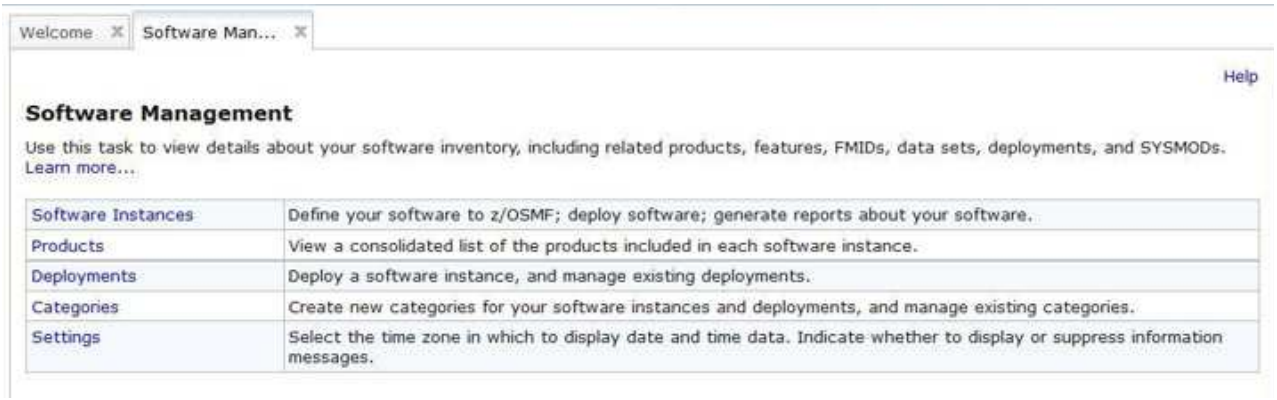


Figure 17. Software Management page

Key features

With the Software Management task, you can:

- **Define your software to z/OSMF.** To do so, you must create one or more software instances to represent your installed software. A software instance can contain any software that is SMP/E packaged and installed. For example, a software instance can contain:
  - IBM software installed from ServerPac, CBPDO, or fee-based installation offerings.
  - ISV software.
  - z/OS operating system and related products.
  - Subsystems and related products.

  It is recommended that a software instance contain a set of products that should be installed, maintained, migrated, and deployed as a group.

  Note that installation of software or service upgrades is outside the scope of the Software Management task. Use SMP/E to assist with the installation process.
- **View a list of the products, features, FMIDs, and data sets that are included in your software instances.** You can use this information to do the following:
  - Identify which software instances, data sets, or systems might be impacted if you upgrade a product
  - Determine if you have the prerequisites installed for a specific function
  - Determine which data sets will be deployed during a deployment
  - Determine whether the data sets conform to your installation's policies for naming conventions, placements, and so on
  - Provide evidence of what is installed to an auditor, procurement team, or operations staff.

- **View details about your installed products.** For example, you can do the following:
  - Obtain a list of all the products contained in any of your software instances.
  - Determine which products are nearing or have reached end of service support.
  - Identify which software instances contain a product and will be affected by any changes to the product.
  - Identify which systems might potentially be affected by changes to a product.

  You can use this information to identify which products need to be ordered for a future upgrade and to provide evidence of what is installed to an auditor or procurement team.
- **Generate reports about your software.** For example, you can generate the following reports:
  - **End of Service**. Helps you determine if any of the products contained in your software instances are approaching or have reached end of service support.
  - **Missing Critical Service**. Helps you determine if any unresolved PE PTFs, HIPERs, or other exception SYSMODs identified by ERROR HOLDDATA are contained in your software instances, and helps you identify the SYSMODs that will resolve those exceptions.
  - **Missing FIXCAT SYSMODs**. Helps you identify any unsatisfied hardware or software requisites that are required for a specific category of software fixes.
  - **Software Instance Comparison**. Helps you determine the functional and service differences between two software instances.
  - **Software Instance Validation**. Helps you verify that the software libraries that are associated with a software instance exist and contain the appropriate parts.
  - **SYSMOD Search**. Helps you determine if your software instances contain the SYSMODs in which you are interested. This could be useful in determining if you already installed a suggested fix or security APAR and how many software instances are affected by a specific PTF in Error.
- **Deploy SMP/E packaged and installed software.** You can use this capability to copy an instance of SMP/E installed software and save it on DASD volumes shared within the same sysplex (local deployment) or on DASD volumes accessible to another sysplex (remote deployment).

  You might perform a deployment to prepare to upgrade one or more of the contained products in a software instance to a new product release level or a higher maintenance level. Or, to create a copy of a software instance so that it can run in a different environment, such as test, development, or production.
- **Organize your software instances and deployments.** The Software Management 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.

For information about using this task, see the online help.

System Status task overview

The System Status task consolidates the performance data from an entire z/OS sysplex into one performance indicator, so that you can quickly assess the performance of the workloads running in your environment.

The System Status task also allows you to control the scope of monitoring that is performed by the Resource Monitoring task. You can specify the z/OS systems and sysplexes to be monitored, as well as the AIX, Linux, and Windows system complexes. Note that monitoring other platforms requires that the RMF Cross Platform Distributed Data Server be installed and configured on a system in your sysplex.

When the Workload Management plug-in is enabled on your system, the System Status task links automatically to the Workload Management task for more data. If the System Status task shows performance data related to system or sysplex, you can view the view the currently active WLM service definition in your z/OSMF session.

To display the System Status task, expand the Performance category in the navigation area and select **System Status**. Figure 18 shows a sample view from the System Status.

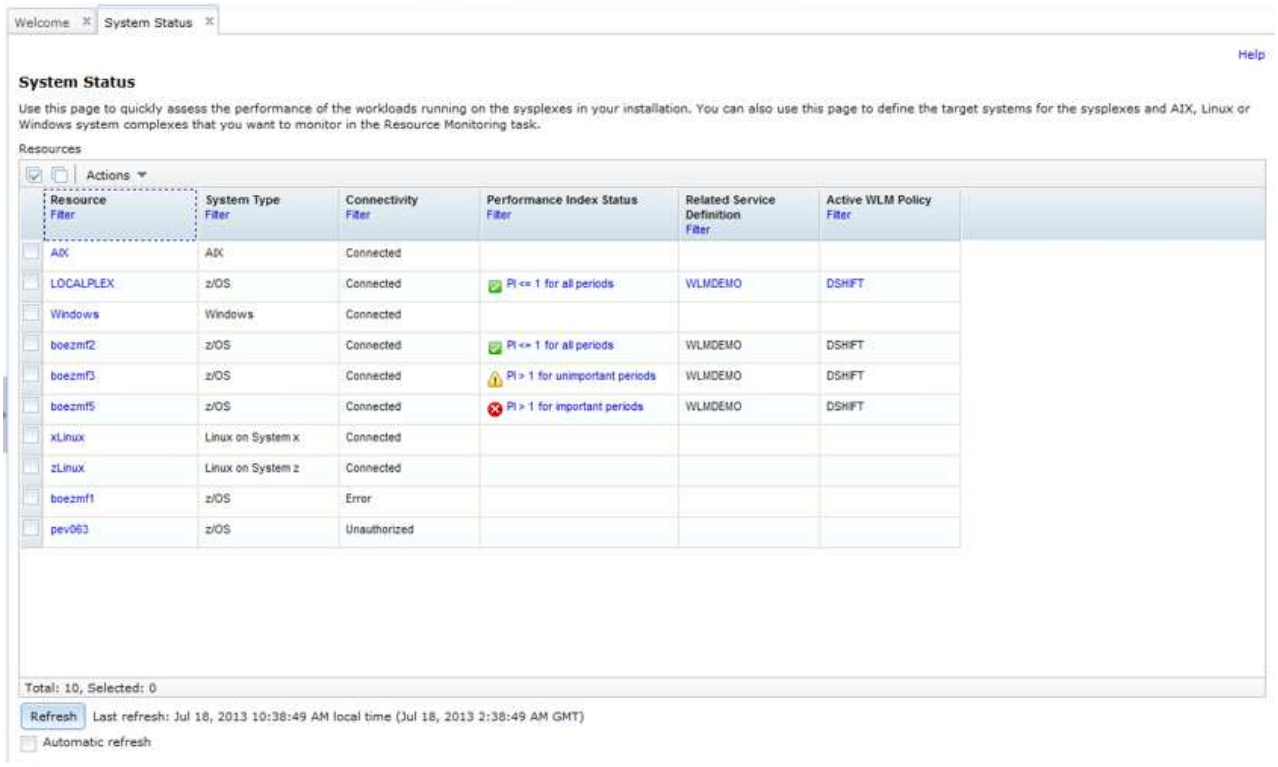


Figure 18. System Status sample view

For information about using this task, see the online help.

Workflows task overview

The Workflows task helps you to guide the activities of system programmers, security administrators and others at your installation who are responsible for managing the configuration of the z/OS system. The Workflows task provides a framework for these activities in the form of structured procedures known as *workflows*. The Workflows task of z/OSMF simplifies tasks through guided step-based workflows, and provides administrative functions for assigning workflow responsibilities and following progress.

To display the Workflows task, select **Workflows** in the navigation area. The Workflows task main page is displayed, as shown in Figure 19.

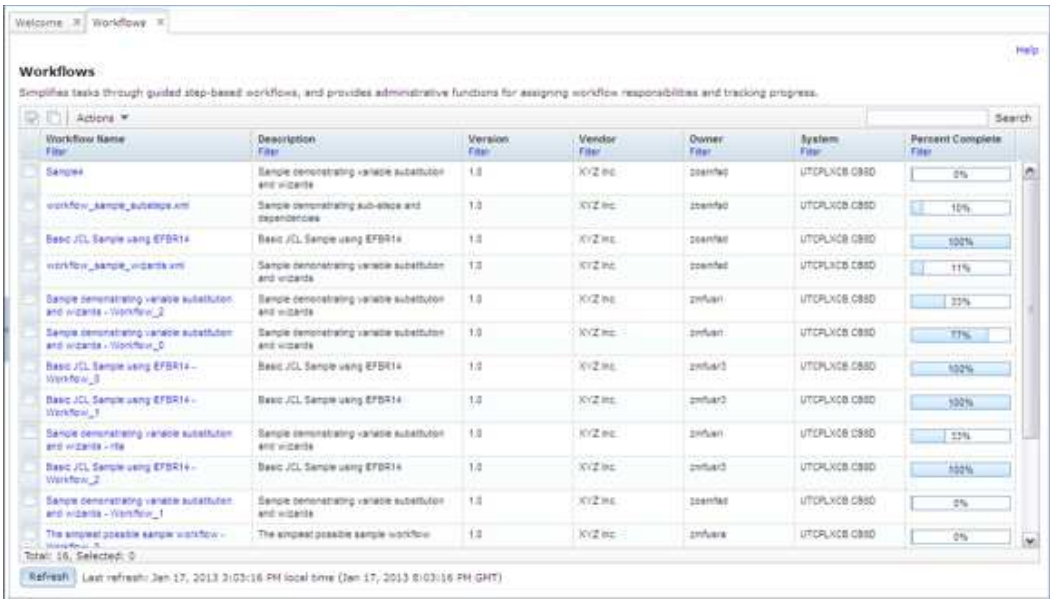


Figure 19. Workflows task main page

The Workflows task allows you to assign individual work items in the workflow (the "steps") to performers and track their progress. Based on the workflow, the Workflows task can offer wizards to assist your team with creating system objects (UNIX files and z/OS data set members) and submitting work to run on z/OS, such as batch jobs, REXX scripts, and UNIX shell scripts.

z/OSMF includes a number of sample workflow definition files in the following location: `<product-dir>/workflow/`, where the default for `<product_dir>` is `/usr/lpp/zosmf`. To get started with the Workflows task, try importing a sample workflow definition file into z/OSMF. To do so, open the Workflows task and select the **Create Workflow** action provided in the Workflows table. Then, enter the name of the workload definition file and the workflow variable input file, if one was supplied by the workflow provider.

More information about the Workflows task is provided in the online help. Information about creating workflow definitions for z/OSMF is provided in the IBM publication, *IBM z/OS Management Facility Programming Guide*.

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 Management (WLM) service definitions that 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.

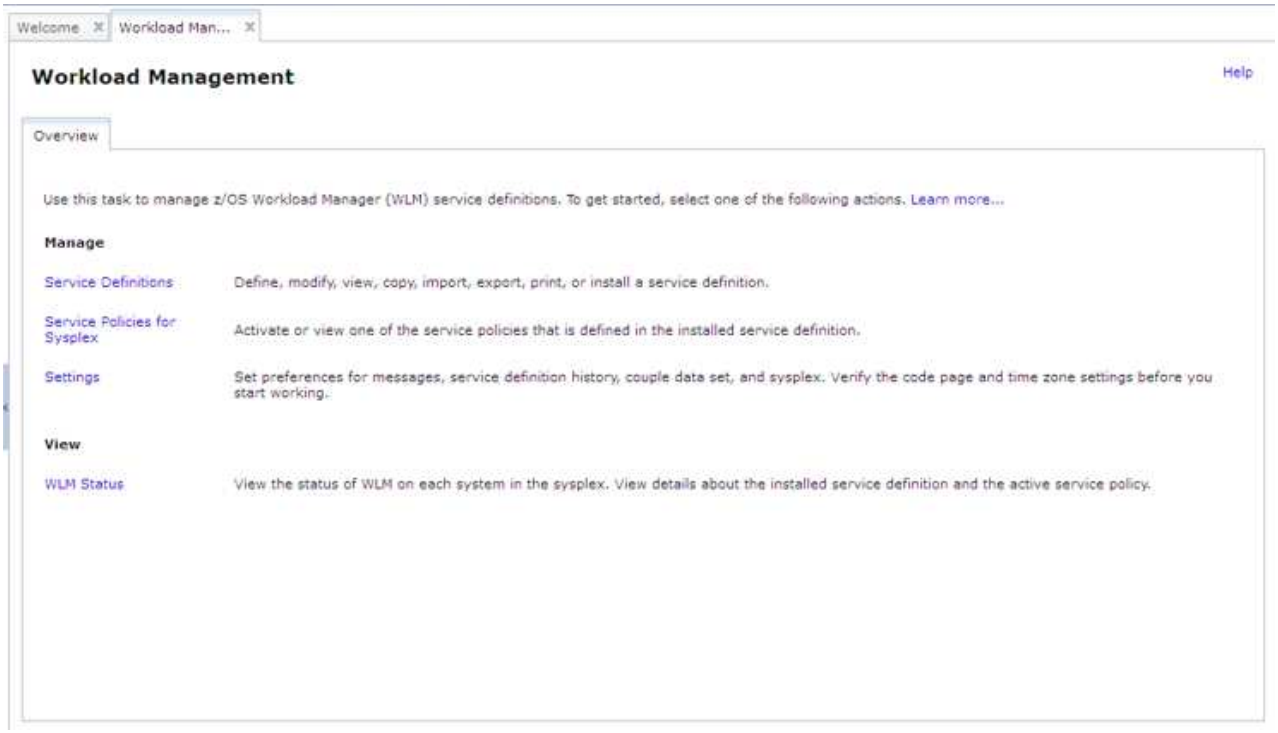


Figure 20. Workload Management task main page

When the Resource Monitoring plug-in is enabled on your system, the Workload Management task can link automatically to the Resource Monitoring task and the System Status task. This capability allows you to view performance data for the currently active service classes, service policies, and service definition in your sysplex.

To display the Workload Management task, expand the Performance category in the navigation area and select **Workload Management**. Figure 20 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.

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 user 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 system 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, and whether comments for service definition actions are required.
- Add comments. You can add comments to the service definition history, for example, to explain why a service definition was changed or what was changed. These comments can be added when a modification is made, or at a later time.

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.

For information about using this task, see the online help.

Chapter 6. Setting up security for the z/OSMF plug-ins

The authorization of users to z/OSMF functions (tasks and links) is based on traditional z/OS security controls, such as user IDs and groups, and SAF resource profiles. This topic describes the actions for setting up security for the z/OSMF tasks and links.

To perform work in z/OSMF, a user requires a valid user ID on the z/OS host system and authorization to one or more z/OSMF tasks on that system. Your security administrator authorizes users to z/OSMF resources through your security management product, such as RACF. After the required plug-ins are added to your system and the associated security controls are established, a user can begin using z/OSMF to perform system management tasks.

IZUxxSEC jobs in SYS1.SAMPLIB

IBM provides a set of jobs in SYS1.SAMPLIB with RACF commands to help with performing these changes. Each job represents a set of security profiles to be defined, based on the specific z/OSMF functions to be protected.

In SYS1.SAMPLIB, the IZUSEC job represents the authorizations that are needed for the z/OSMF core functions. All z/OSMF installations require at least the core functions security commands.

Each of the other IZU*xx*SEC jobs is associated with an optional plug-in, as follows:

IZUCPSEC
: Capacity Provisioning

IZUCASEC
: Configuration Assistant

IZUILSEC
: Incident Log

IZUISSEC
: ISPF

IZURMSEC
: Resource Monitoring

IZUDMSEC
: Software Deployment

IZUWMSEC
: Workload Management

Depending on which plug-ins you choose to enable, review the associated IZU*xx*SEC job to determine which security commands should be run for your installation.

SYS1.SAMPLIB also includes the IZUAUTH job, which your security administrator can use for authorizing user IDs to the z/OSMF plug-ins. Specifically, the job contains a number CONNECT statements for connecting user IDs to the z/OSMF security groups.

Managing user access to z/OSMF tasks and links

Your installation determines which z/OS users perform z/OSMF tasks, based on the z/OSMF plug-ins that you choose to add.

© Copyright IBM Corp. 2009, 2016

Figure 21 shows a typical security setup for z/OSMF. To conserve space, this figure includes only a subset of the available tasks.

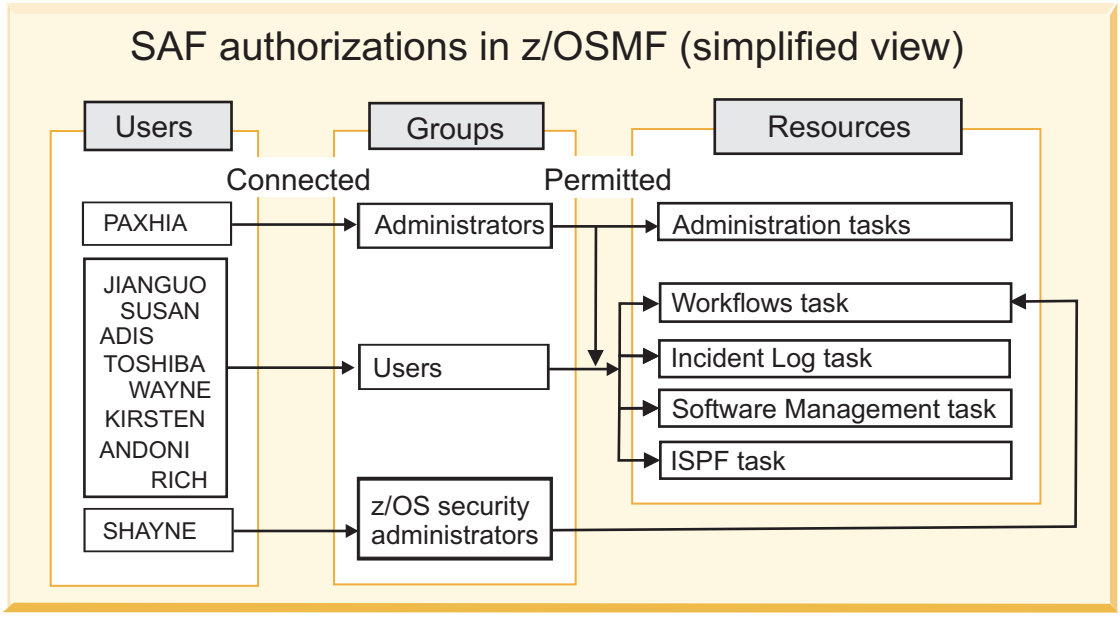


Figure 21. SAF authorizations in z/OSMF: A simplified view

For an installation that uses RACF as its security management product, the z/OSMF configuration process provides a basic set of security definitions. Specifically, z/OSMF provides the IZUxxSEC jobs with sample RACF commands that your security administrator can use to secure z/OSMF resources and users.

The IZUxxSEC jobs contain sample RACF commands for:

- 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, z/OSMF creates the groups IZUADMIN and IZUUSER, which correspond to the administrator and user roles. z/OSMF also creates the group IZUSECAD to allow your z/OS security administrator to perform the security-related steps in the Workflows task.

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 IZUxxSEC jobs for the authorizations that are needed. For the security structures that are created by the IZUxxSEC jobs, see Appendix A, “Security configuration requirements for z/OSMF,” on page 181.

Your security administrator can use the job SYS1.SAMPLIB(IZUAUTH) to authorize users to tasks and links. When used as provided, the IZUAUTH job connects the supplied user ID to the z/OSMF user group (IZUUSER). The job also contains commented commands for connecting the user to the z/OSMF administrator group and the z/OS Security Administrator group. Each group is permitted to a default set of z/OSMF resources (tasks and links). For the specific group permissions, see Table 29 on page 198.

You can create more user groups as needed, for example, one group per z/OSMF task. Note, however, that the IZUAUTH job is based on the default group assignments. If you create more groups, you must add commands for those groups to the IZUAUTH job.

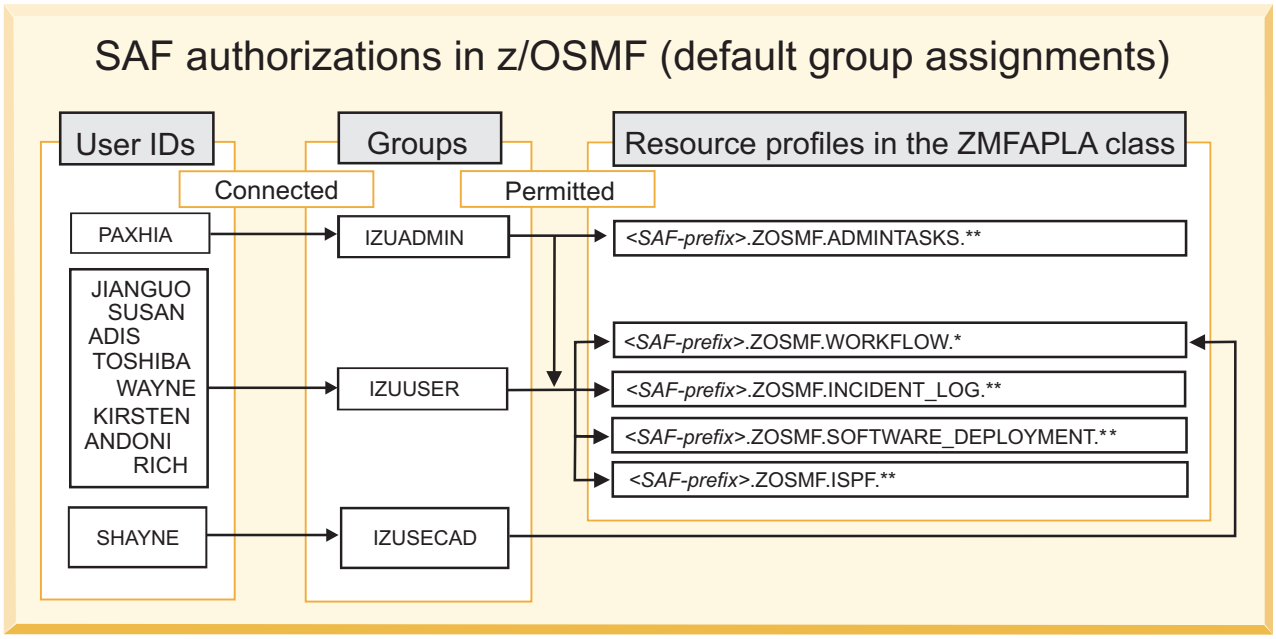


Figure 22. SAF authorizations in z/OSMF: The default setup

Depending on the plug-ins to be added, your installation might need to create more authorizations to various system resources. Your security administrator can use the commands in the IZUAUTH job for authorizing users to z/OSMF and to the z/OS components used in z/OSMF operations. A change to your security setup will likely require an applicable refresh of your security product and a restart of the z/OSMF server for the changes to take effect.

Figure 22 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. In the figure, the group names and profiles are shown with the 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 29 on page 198.

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

A user connected to the z/OSMF administrator group or the z/OSMF user group might be connected to other security groups. To allow such users to access z/OSMF without having to log in under a specific group, it is recommended that you have list-of-groups authority checking (GRPLIST option) active. For more information, see *z/OS Security Server RACF Security Administrator's Guide*.

As shown in Figure 22, the IZUDMSEC job provides a default authorization for the Software Management task through profile `<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.**`. Your installation can create more granular authorizations for this task through more profiles, as follows:

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.**
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.PRODUCT_INFO_FILE.*
```

For more information, see "Creating access controls for the Software Management task" on page 227.

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.

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.

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

Chapter 7. Adding plug-ins to a z/OSMF configuration

Enabling the optional plug-ins in z/OSMF requires some customization of the z/OS host system, as described in this document.

Appendix B, "Customizing your z/OS system for the z/OSMF plug-ins," on page 201 describes the z/OS system customization steps that are required for enabling the optional plug-ins in z/OSMF. Which steps you will need to complete depend on which plug-ins you plan to deploy on your system. Review the system setup requirements for each plug-in. When doing the work, you might find it easier to start with plug-ins that require little or no system customization, such as Configuration Assistant or ISPF, and then progress to plug-ins with more extensive requirements, such as Incident Log.

Alternatively, you can use the z/OSMF Configuration Workflow to perform the system customization for each plug-in. If you use the Configuration Workflow, you are guided through these steps. For more information, see "About the Configuration Workflow."

About the Configuration Workflow

For each plug-in to be added, the Configuration Workflow performs the following actions:

- Creates and updates parmlib members as needed for the plug-ins to be configured. For example, if you configure the Incident Log plug-in, the workflow creates members in the target parmlib data set.
- Prepares your z/OS system for running the tasks that are associated with the plug-ins.
- Verifies the setup for the z/OSMF tasks. If you configure the Incident Log plug-in, the workflow verifies the setup of the following z/OS system components:
  - Sysplex dump directory
  - System logger
  - Common event adapter (CEA)
  - System REXX.

  The workflow identifies any areas that might require further action on your part.
- Adds the names of the optional plug-ins to the PLUGINS statement in your IZUPRMxx member.
- Creates authorizations for the z/OSMF tasks. The workflow includes steps that create RACF commands for connecting users and groups to the appropriate SAF profiles. If your installation uses a security management product other than RACF, your security administrator can refer to the RACF commands as a reference.
- Completes the deployment of the plug-ins by restarting the z/OSMF server to make these changes effective.

If you prefer, you can manually perform the system customization for each plug-in. For descriptions of the customization that must be performed for each plug-in, see Appendix B, "Customizing your z/OS system for the z/OSMF plug-ins," on page 201.

Resource authorizations for the Configuration Workflow

The Configuration Workflow uses the IRRXUTIL program to retrieve profile information about users, groups, general resources, and general RACF settings administered by the SETROPTS command. Therefore, your user ID requires READ authorization to the resource names listed in Table 9.

Table 9. Resource authorizations for the Configuration Workflow

Resource name	Class	Access	Purpose
IRR.RADMIN.LISTUSER	FACILITY	READ	Read USER profiles

© Copyright IBM Corp. 2009, 2016

Table 9. Resource authorizations for the Configuration Workflow (continued)

Resource name	Class	Access	Purpose
IRR.RADMIN.LISTGRP	FACILITY	READ	Read group profiles
IRR.RADMIN.RLIST	FACILITY	READ	Read profiles of general resources
IRR.RADMIN.SETROPTS.LIST	FACILITY	READ	Read RACF SETROPTS settings

The IZUSEC job contains sample RACF commands for creating these authorizations. Figure 23 shows the commands that are provided in the job.

```
/* Allow users of the z/OSMF Configuration Workflow to extract profile information  */
RDEFINE FACILITY IRR.RADMIN.LISTUSER
RDEFINE FACILITY IRR.RADMIN.LISTGRP
RDEFINE FACILITY IRR.RADMIN.RLIST
RDEFINE FACILITY IRR.RADMIN.SETROPTS.LIST

/* Permit the z/OSMF administrator access   */
PERMIT IRR.RADMIN.LISTUSER CLASS(FACILITY) ID(IZUADMIN) ACCESS(READ)
PERMIT IRR.RADMIN.LISTGRP  CLASS(FACILITY) ID(IZUADMIN) ACCESS(READ)
PERMIT IRR.RADMIN.RLIST    CLASS(FACILITY) ID(IZUADMIN) ACCESS(READ)
PERMIT IRR.RADMIN.SETROPTS.LIST CLASS(FACILITY) ID(IZUADMIN) ACCESS(READ)

SETROPTS RACLIST(FACILITY) REFRESH
```

Figure 23. RACF commands for authorizing the users of the Configuration Workflow

Getting started

To view the configuration workflow, import the following workflow definition file into the Workflows task:

`<product_dir>/workflow/izu.config.setup.xml`

where `<product_dir>` is the z/OSMF product directory. By default, this is `/usr/lpp/zosmf`.

When creating the configuration workflow, also specify the accompanying variable input file, which was generated when you created the base z/OSMF configuration. This file, which is used to populate the workflow with your configuration values, resides in the following directory path:

`<user_dir>/configuration/workflow/izu.config.workflow.cfg`

where `<user_dir>` is the user directory. By default, this is `/var/zosmf`.

More information about the Workflows task is provided in the online help.

Steps for adding plug-ins to z/OSMF

To add plug-ins to z/OSMF, follow these steps:

1. Run the z/OSMF Configuration Workflow to customize your system for the plug-ins to be added.
2. Verify the results of your work by opening a web browser to the Welcome page. For information, see "Step 4: Access the z/OSMF Welcome page" on page 35.

Figure 24 on page 69 shows the Welcome page after you log in with the installer user ID. Notice that the navigation area now includes expandable categories for the optional plug-ins. Figure 24 on page 69 shows the Welcome page as it would appear to the installer, who has access to the z/OSMF Administration and

z/OSMF Settings categories by default. A user without administrator access would not see these categories.

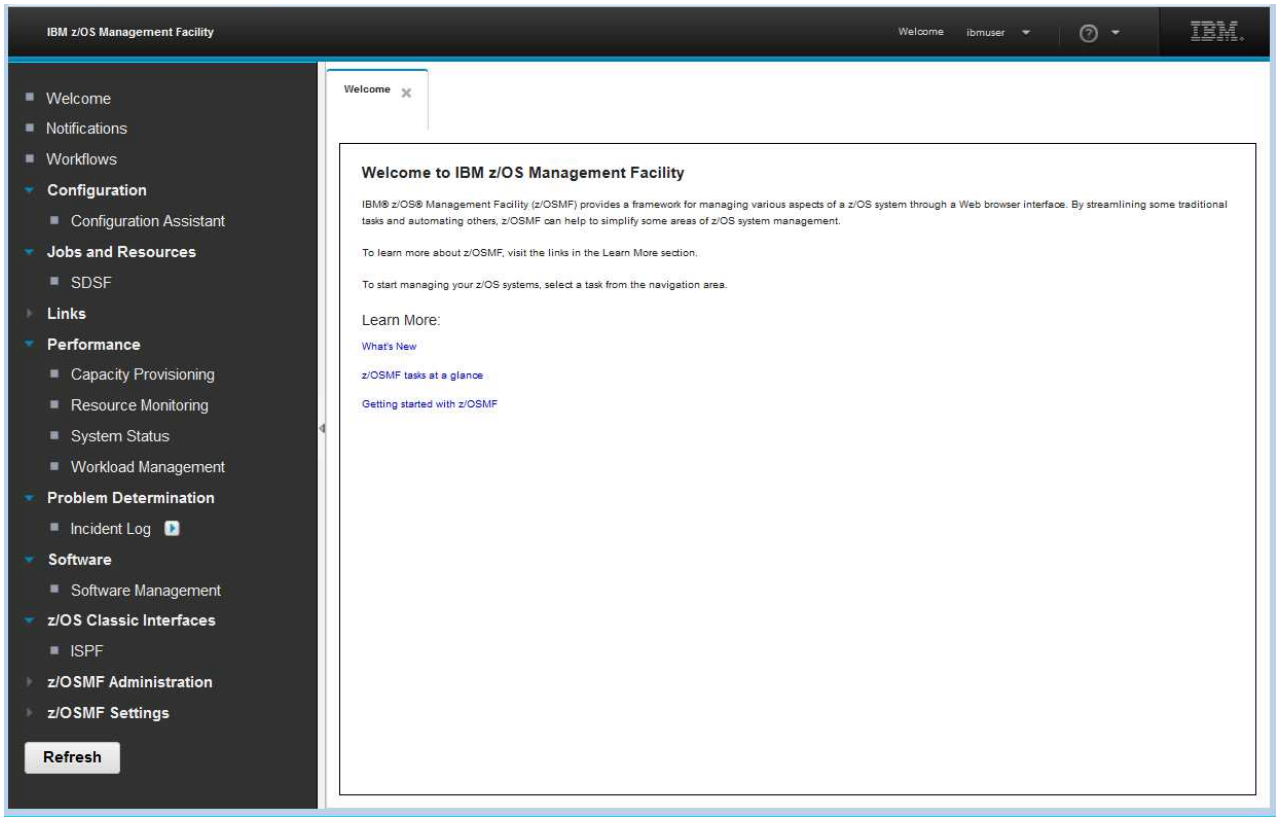


Figure 24. z/OSMF Welcome page (after optional plug-ins are added)

Chapter 8. Using z/OSMF in a multi-system environment

If you plan to use z/OSMF in a multi-system environment, or across sysplexes, the decisions you make during the configuration process can help to simplify the management of z/OSMF later. You can deploy z/OSMF in such a way that it can be started from any system in your sysplex for availability. This is an important consideration when deploying any application in a sysplex environment.

To support the use of z/OSMF in a multi-system environment:

- The IZUPRMxx member accepts system symbols as values for the configuration settings, such as the host name for z/OSMF.
- Different IZUPRMxx members can be selected on the START command for a particular system, for example, to allow for a different selection of plug-ins to be used on each system.
- As an alternative to specifying a unique hostname on each system through multiple parmlib members, you specify a dynamic VIPA (DVIPA) for the hostname that resolves to the correct IP address.

This chapter assumes that UNIX System Services runs in a shared file system environment in your sysplex. For information about how to establish an UNIX System Services shared file system environment in a sysplex, see *z/OS UNIX System Services Planning*.

Considerations for multi-system environments are described in the following topics:

- "Configuring z/OSMF for availability"
- "Restart z/OSMF processing on another system in the same sysplex" on page 73
- "Additional considerations for a multi-system environment" on page 73
- "Configuring a primary z/OSMF for communicating with secondary instances" on page 74
- "Enabling single sign-on between z/OSMF instances" on page 77.

Configuring z/OSMF for availability

In a z/OSMF context, *availability* refers to the ability to restart z/OSMF on another system in the sysplex, in the event of a failure in z/OSMF on the original system. Restarting the server is accomplished manually, though the START command. This topic describes how to configure z/OSMF for availability in a sysplex environment. Some considerations described here are applicable to any application that you might want to deploy in a sysplex environment.

Make the z/OSMF user directory shareable

Each active instance of z/OSMF requires its own user directory, which contains the persisted data for the instance. By default, the z/OSMF configuration process creates the user directory at the non-sharable mount point `/var/zosmf`, but you might have selected another mount point for it when you installed z/OSMF. The user directory is specified on the USERDIR= parameter of the START command for z/OSMF.

Generally, you should configure z/OSMF so that one instance can be started on any system in the sysplex. To allow the same instance z/OSMF to be started on other systems in the sysplex, ensure that the user directory mount point is shared by all of the systems on which you might want to start z/OSMF. Or, you can specify a common, root directory for this mount point, such as `/sharedapps` (with a shared mount point and volume) that is read/write accessible from other systems in the sysplex. Then, you can simply restart the z/OSMF server on another system. If you use a shared security database, this procedure is further simplified because the backup instance can use the same user IDs and groups as your primary instance. For information about mounting file systems, see *z/OS UNIX System Services Planning*.

© Copyright IBM Corp. 2009, 2016

If you plan to run more than one instance of z/OSMF in a sysplex, you require a unique user directory (and file system name) for each instance. Consider using the system name to qualify the name of the file system. For example: IZU.<*system-name*>.SIZUUSRD.

Ensure that the z/OSMF host name is unique

When using z/OSMF in a multi-system environment, each instance of z/OSMF must have a unique host name. Otherwise, users cannot log in to z/OSMF. This topic describes a technique for using system symbols to create unique host names for cloned z/OSMF configurations.

In the IZUPRMxx parmlib member, you can define a host name for your configuration. You can specify an installation-specific value, or accept the default, HOSTNAME(*), which instructs z/OSMF to do a host name lookup on the system.

In addition to using system symbols, you can use the z/OS Communications Server dynamic VIPA (DVIPA) function to create a DVIPA address for your sysplex, and use the DVIPA address as the z/OSMF host name. This approach allows users to connect to z/OSMF using the same IP address, regardless of which system is running z/OSMF. In a multiple sysplex environment, you might still use symbols, perhaps to represent a different DVIPA address for each sysplex. For considerations, see "Use a DVIPA address for the z/OSMF host name".

Use a DVIPA address for the z/OSMF host name

You can use the z/OS Communications Server TCP/IP sysplex networking dynamic VIPA (DVIPA) function to help ensure the availability of z/OSMF. Along with your primary z/OSMF instance, you can create a backup instance in your installation. The backup z/OSMF instance can be started if the primary instance becomes unavailable. With DVIPA, your installation can use the same connection information when your active instance moves from the primary system to the backup system. This action allows z/OSMF to bind again to the same DVIPA address, and resume operation at the same location.

The following example shows the TCP/IP configuration profile statements for the primary and backup systems on which z/OSMF is running. The statements should be identical for both systems. The IP addresses specified in these examples are for illustration purposes only. You should work with your network team to obtain the appropriate host name that resolves to the DVIPA address for your installation.

```
VIPADYNAMIC
VIPADEFINE MOVE IMMEDIATE 255.255.252.0 10.12.5.39 ; z/OSMF
VIPADISTRIBUTE DEFINE
SYSPLEXPORTS
10.12.5.39
PORT 443
DESTIP 10.1.100.74 10.1.100.75
ENDVIPADYNAMIC
```

In this example, the `VIPADEFINE` statement includes the subnet mask `255.255.255.255`, which is used as the mask for the single DVIPA that is being defined. You can also define a larger, less-specific, subnet mask. However if you only specify one DVIPA on the `VIPADEFINE` statement and its corresponding `VIPADISTRIBUTE` statements, then that DVIPA is the only IP address that is defined and distributed. The `PORT` parameter included in this example is used to bind the port reserved for the z/OSMF instance that you are configuring to the specified DVIPA. This binding enables z/OSMF to become eligible to receive connection requests.

For an overview of TCP/IP sysplex networking, see *z/OS Communications Server IP Configuration Guide*. For a description of the `VIPADYNAMIC` statement, see *z/OS Communication Server IP Configuration Reference*.

Restart z/OSMF processing on another system in the same sysplex

If the z/OSMF user directory is mounted at a shared mount point, as described in *"Configuring z/OSMF for availability,"* moving z/OSMF processing to another system in the same sysplex requires only that you restart the server on the other system.

Example:

1. Stop the z/OSMF server on System A:

   ```
   STOP IZUANG1
   STOP IZUSVR1
   ```

2. Start the z/OSMF server on System B. When starting the server on the new system, specify the user directory on the start command.

   ```
   START IZUANG1
   START IZUSVR1,USERDIR='/var/zosmf'
   ```

Configuration settings for z/OSMF are specified through the IZUPRMxx parmlib member. One or more members can be used in combination, and different combinations of members can be used on each system in the sysplex. If the same statement is used more than once, either in the same member or in multiple members, the value from the last occurrence is used. The IZUPRMxx members are specified on the START command for the z/OSMF server.

Examples:

- Start the z/OSMF server on System C with member IZUPRM00 concatenated with member IZUPRM01.

  ```
  START IZUANG1
  START IZUSVR1,IZUPRM=(00,01)
  ```

- Start the z/OSMF server on System D with member IZUPRM00 concatenated with member IZUPRM02.

  ```
  START IZUANG1
  START IZUSVR1,IZUPRM=(00,02)
  ```

Additional considerations for a multi-system environment

This topic describes additional considerations for using z/OSMF in a multi-system environment.

If you plan to run multiple instances of z/OSMF, observe the following considerations:

- The z/OSMF user directory 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 user directory system from being accessed by more than one instance of z/OSMF, z/OSMF locks the file system through a global resource serialization ENQ with QNAME ZOSMF. If you start a second instance of z/OSMF using the same file system, that z/OSMF will not be usable. Users who attempt to access the second instance of z/OSMF will encounter an error (message IZUG680E is written to the server job log on the system that fails to start). Further, all log messages from the second instance of z/OSMF are routed to the z/OSMF server job logs directory, rather than to the log in the z/OSMF user directory.
- Running multiple instances of z/OSMF simultaneously in a sysplex, using different z/OSMF user directory file systems, is not recommended for certain z/OSMF tasks. 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.

Configuring a primary z/OSMF for communicating with secondary instances

z/OSMF can be configured to communicate with another instance of z/OSMF in a remote sysplex. This capability is important because it allows z/OSMF tasks to work with systems on other sysplexes in your enterprise. To enable z/OSMF-to-z/OSMF communication, you must configure a primary z/OSMF for communicating with secondary instances, as described in this topic. The key requirement is to enable the sharing of digital certificates between instances.

This information assumes the use of RACF. If you use another security product, consult the vendor for more information.

Each z/OSMF instance includes a server runtime and digital certificates

During the configuration process, z/OSMF creates a certificate authority (CA), optionally, and a server certificate, to be used for enabling Secure Sockets Layer (SSL) connections between z/OSMF instances. z/OSMF also creates a SAF key ring, and stores the CA and server certificate in the key ring.

These constructs are named, as follows:

- Key ring name is `IZUKeyring.IZUDFLT`
- CA name is:

```
CN('z/OSMF CertAuth for Security Domain')
OU('SAF_PREFIX'))
WITHLABEL('zOSMFCA')
```

z/OSMF creates the CA and the server certificate if you uncomment the following commands for creating certificates in the IZUSEC job:

```
//* Create the CA certificate for the z/OSMF server                 *
 RACDCERT CERTAUTH GENCERT +
   SUBJECTSDN(CN('z/OSMF CertAuth for Security Domain') +
   OU('IZUDFLT')) WITHLABEL('zOSMFCA')  +
   TRUST NOTAFTER(DATE(2023/05/17))
 RACDCERT ADDRING(IZUKeyring.IZUDFLT) ID(IZUSVR)

//* Create the server certificate for the z/OSMF server              *
 RACDCERT ID( IZUSVR ) GENCERT SUBJECTSDN(CN('PEV051.POK.IBM.COM') +
   O('IBM') OU('IZUDFLT')) WITHLABEL('DefaultzOSMFCert.IZUDFLT') , +
   SIGNWITH(CERTAUTH LABEL('zOSMFCA')) NOTAFTER(DATE(2023/05/17))
 RACDCERT ALTER(LABEL('DefaultzOSMFCert.IZUDFLT')) ID(IZUSVR) TRUST
 RACDCERT ID( IZUSVR ) CONNECT (LABEL('DefaultzOSMFCert.IZUDFLT') +
   RING(IZUKeyring.IZUDFLT) DEFAULT)
 RACDCERT ID( IZUSVR ) CONNECT (LABEL('zOSMFCA') +
   RING(IZUKeyring.IZUDFLT) CERTAUTH)
```

Planning for secure communication between instances

In the sections that follow, the z/OSMF instance that initiates communication is considered to be the *primary* instance. It serves as the repository for the data that is generated by the z/OSMF instances running in your installation. When planning to enable communication between instances of z/OSMF, first determine which of the instances is to be the primary.

The primary instance communicates with other z/OSMF instances through Secure Sockets Layer (SSL) connections. Each SSL connection requires an exchange of digital certificates, which are used to authenticate the z/OSMF server identities. For the SSL connection to be successful, the primary instance must be configured to trust the server certificates from the secondary instances.

For signing the server certificates, each instance uses a certificate authority (CA) certificate. Establishing a trust relationship between instances will require knowing which CA certificate is used to sign each secondary instance server certificate.

Another consideration is whether the instances share the same security database or use separate security databases. Using a shared database can simplify the process of enabling secure communications if the same CA certificate is used by all participating systems. Sharing a RACF database is not feasible for every installation, however. If your installation uses separate security databases, you must ensure that the appropriate certificates are shared by the participating z/OSMF instances.

For more information about digital certificates, see *z/OS Security Server RACF Security Administrator's Guide*.

Strategies for sharing CA certificates

This topic describes two scenarios for sharing CA certificates between multiple instances: You might choose to use one common CA certificate for all of the instances, or a different CA certificate for each instance. A third situation is also described, wherein the existence of identically named CA certificates can complicate certificate sharing.

If you have not yet created any secondary instances of z/OSMF, you might find it easier to create one CA certificate and use it to sign all of the server certificates in the primary and secondary instances. Using this approach, you export the CA certificate from the primary system and add it to each of the secondary system security databases. Then, you configure the additional instances of z/OSMF on each secondary system. Here, you should not run the IZUSEC job certificate commands on the secondary systems, as mentioned in "Each z/OSMF instance includes a server runtime and digital certificates" on page 74. Instead, use the certificate that you have from the primary system. As a result, the same CA certificate is used to sign the server certificate for each instance. This approach is shown in "Scenario 1: SSL connections using the same CA certificate" on page 76.

If you have already created one or more secondary instances of z/OSMF, and you want to enable them for communication with the primary, determine whether the secondary systems were configured to use identically-named CA certificates or uniquely-named CA certificates. If you created each of the secondary instances with unique SAF prefix values, each secondary instance uses a uniquely named CA certificate. To allow SSL connections in this case, you can make available the secondary system CA certificates on the primary system key ring (that is, export, add, and connect them). As a result, the primary system will trust the secondary system server certificates, and be able to establish SSL connections with those systems. This approach is shown in "Scenario 2: SSL connections using different CA certificates" on page 76.

A third possibility exists. If you created the secondary instances using the default z/OSMF security execs, it is likely that you have identically named CA certificates on each secondary system— and a problem. The CA certificates have identical names (that is, label name and distinguished name), but different key ring material. The reason is that the default z/OSMF commands for creating the CA certificates all specify the same label name and distinguished name, but the resulting CA certificates contain system-specific key ring material.

The differences in key ring material prevent the primary system from trusting the server certificates from the secondary systems, unless the corresponding CA certificates can be added to the primary system key ring. However, you cannot add the secondary system CA certificates to the primary system key ring, because of naming conflicts; those different CA certificates are not "unique" enough to be added to the same database. Attempting to add a certificate into a database that already has a same-named certificate will result in an error and a message such as: `IRRD109I The certificate cannot be added... already defined.`

This potential problem can be avoided if the same CA certificate (from the primary system) is used by all of the instances (primary and multiple secondaries). Or, if the secondary instances are created with unique cell names, thus ensuring that each system's CA certificate can be added to the same security database.

Scenario 1: SSL connections using the same CA certificate

In this scenario, you use the primary system CA to generate a common CA certificate, and distribute this CA certificate to the secondary systems. This approach is recommended if the secondary instances do not already exist.

For example, in Figure 25, both the primary z/OSMF and the secondary instances are identified by server certificates that were created using the same CA (Jupiter).

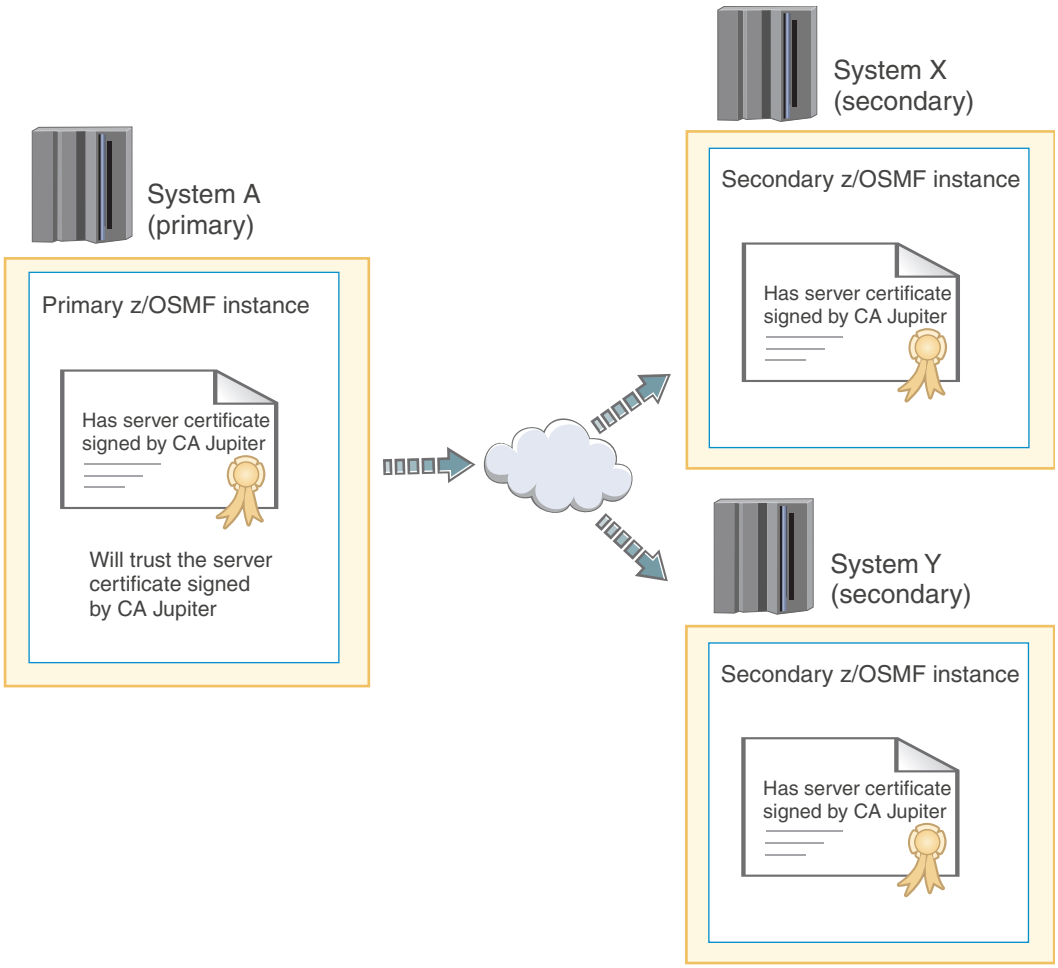


Figure 25. Trust relationship when server certificates are signed by the same CA certificate

Using the same CA to sign the server certificate for each system eliminates the need to import CA certificates from the secondary systems into the primary system security database.

Scenario 2: SSL connections using different CA certificates

In this scenario, each secondary instance of z/OSMF uses its own certificate authority and CA certificate to sign its server certificates. To enable SSL connections in this scenario, you must add each secondary system CA certificate to the primary system security database. This approach is recommended if the secondary instances already exist, and were created to use uniquely named CA certificates.

For example, in Figure 26, the primary z/OSMF:

- Is identified by a server certificate created by the Jupiter CA
- Holds (in its security database) the CA certificates from CA Saturn and CA Mars, for the secondary instances, System X and System Y, respectively.

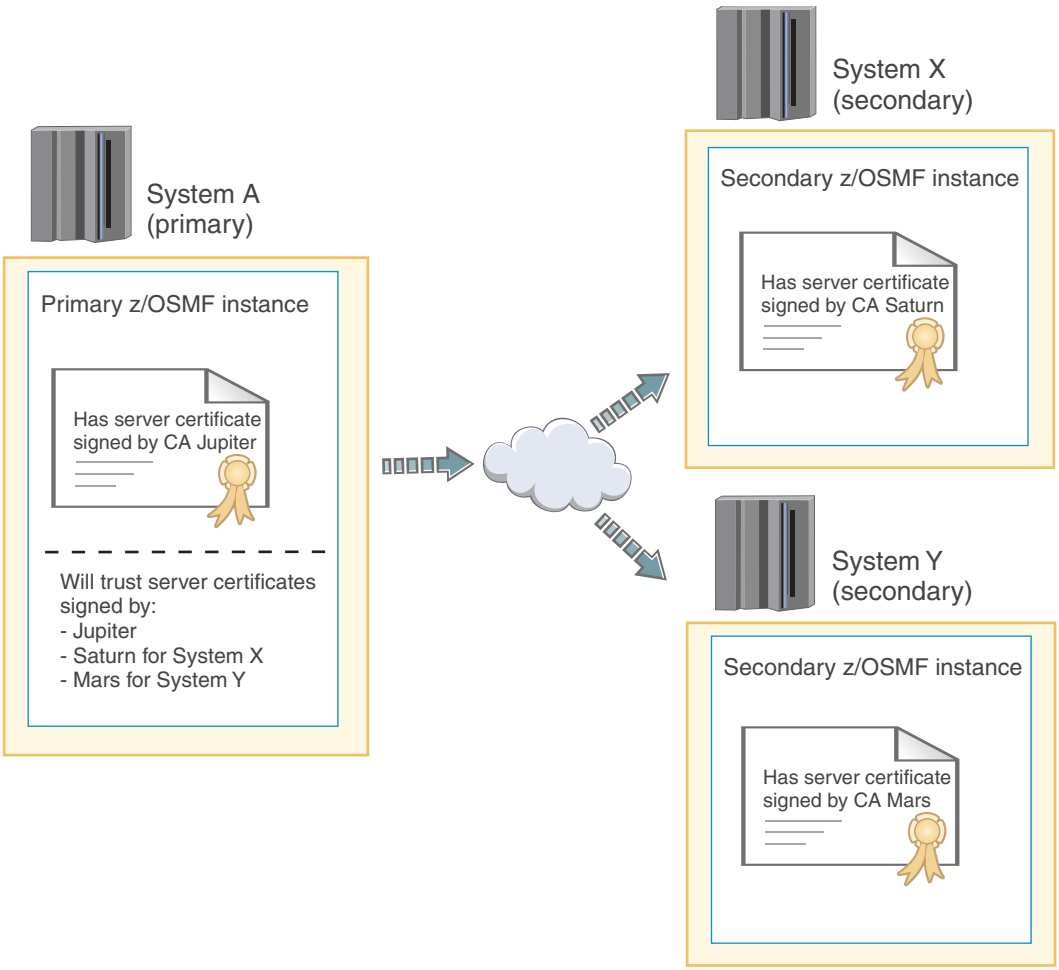


Figure 26. Trust relationship when the server certificates are signed by different CA certificates

To enable SSL connections between instances in this scenario, you would do the following:

1. Export the CA certificate from each secondary system
2. Import the CA certificates into the primary system security database
3. Connect the CA certificates to the primary system.

Enabling single sign-on between z/OSMF instances

Single sign-on (SSO) enables users to log into one z/OSMF instance and to access other z/OSMF instances without getting prompted to log in again. z/OSMF uses the Lightweight Third Party Authentication (LTPA) security protocol to enable a secure single sign-on environment among z/OSMF instances.

The LTPA protocol uses an LTPA token to authenticate a user with the z/OSMF servers that are enabled for single sign-on. The LTPA token contains information about the user and is encrypted using a cryptographic key. The z/OSMF servers pass the LTPA token to other z/OSMF servers through cookies for web resources. If the receiving server uses the same key as the *primary z/OSMF server* -- the server

that generated the key to be used for SSO, the receiving server decrypts the token to obtain the user information, verifies that the token has not expired, and confirms that the user ID exists in its user registry. After the receiving server validates the LTPA token, the server authenticates the user with that z/OSMF instance, and allows the user to access any resource to which the user is authorized.

To establish a single sign-on environment for z/OSMF, the following requirements must be satisfied:

- The z/OSMF servers participating in the single sign-on environment must reside in the same LTPA domain as the primary z/OSMF server. The LTPA domain name is the parent portion of the fully qualified hostname of the z/OSMF servers. For example, if the fully-qualified hostname is *server.yourco.com*, the LTPA domain is *yourco.com*. Due to browser restrictions, the hostname must be qualified with at least three levels (for example *server.yourco.com*). The domain name must have at least two levels (for example, *yourco.com*).
- The servers must share the same LTPA key. For z/OSMF, this is accomplished by invoking the **Enable Single Sign-on** action to synchronize the LTPA key on the primary and secondary z/OSMF servers. For instructions, see the z/OSMF online help.
- The user ID of the user must exist and be the same in all System Authorization Facility (SAF) user registries. It is recommended that you use the same user registry settings for all z/OSMF servers so that users and groups are the same, regardless of the server.
- The value specified for the SAF prefix during the z/OSMF configuration process must be the same for each z/OSMF server you want to enable for single sign-on. By default, the z/OSMF SAF prefix is IZUDFLT.

z/OSMF generates an LTPA keys file when you start the primary z/OSMF sever if an LTPA keys file does not exist. The file is encrypted with a randomly generated key, and a default password of *WebAS* is initially used to protect the file. When establishing a single sign-on environment, it is recommended that administrators change the default password on the primary z/OSMF server, restart the server to generate a new LTPA keys file, and then proceed with enabling single sign-on between one or more z/OSMF instances. For more information about changing the LTPA key password and enabling single sign-on, see the z/OSMF online help.

Part 3. Post-configuration

You can optionally perform additional tasks to enhance your z/OSMF configuration. z/OSMF administrators are the most likely IT personnel to participate in this activity.

Post-configuration in z/OSMF includes the following topics:

- Chapter 9, “Customizing the Welcome page for guest users,” on page 81
- Chapter 10, “Linking z/OSMF tasks and external applications,” on page 83
- Chapter 11, “Configuring your system for asynchronous job notifications,” on page 85
- Chapter 12, “Adding links to z/OSMF,” on page 95
- Chapter 13, “Deleting incidents and diagnostic data,” on page 99
- Chapter 14, “Troubleshooting problems,” on page 103
- Chapter 15, “Configuration messages,” on page 129.

© Copyright IBM Corp. 2009, 2016

Chapter 9. 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 at the beginning of the main work area

Footer area
: Horizontal area at the end of the main work area

Image area
: Small area at the end of the footer.

Figure 27 shows the areas of the z/OSMF Welcome page that can be customized.

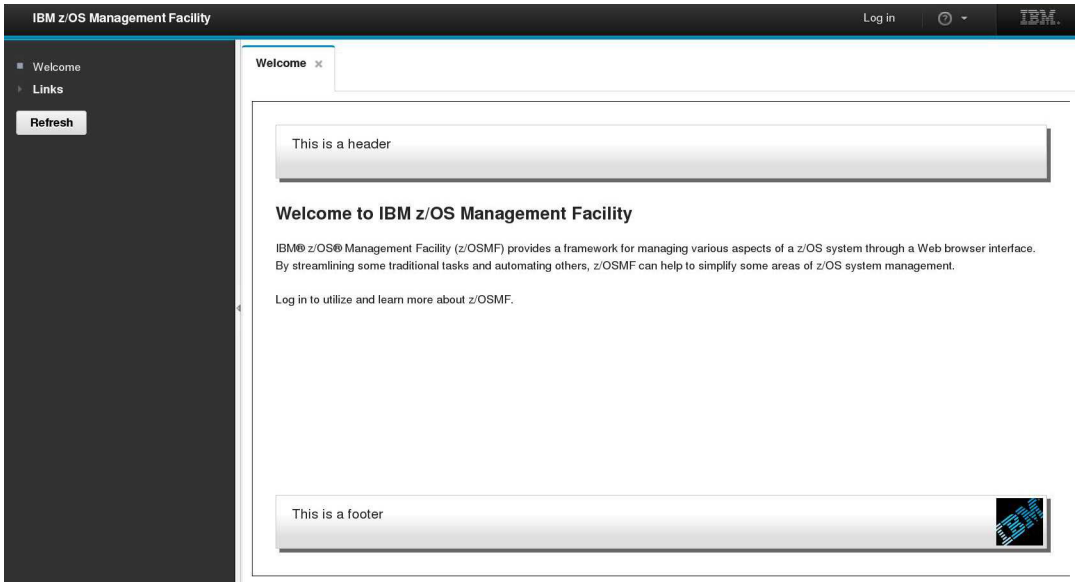


Figure 27. Customizable areas of the z/OSMF Welcome page

As shown in Figure 27, 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 end of the footer area. In Figure 27, 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:

`<product_dir>/samples/customWelcome.properties`

where `<product-dir>` is the z/OSMF product directory. By default, this is `/usr/lpp/zosmf`.

© Copyright IBM Corp. 2009, 2016

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 user file system directory. By default, the directory is `/var/zosmf/data`.

   It is recommended that you copy the file using the z/OSMF installer user ID that you created earlier; see "Selecting a user ID for configuration" on page 28. Doing so ensures that the files are stored with the correct ownership and permissions. Note that 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, adding your text.** As shown in Figure 28, the Welcome properties file contains the following input fields for the customizable areas:

```
header=
footer=
```

Figure 28. 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 256 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 256 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 (\u*xxxx*) is treated as one character.

   As an example, Figure 29 shows the Welcome page properties file that was used to customize the Welcome page in Figure 27 on page 81.

```
header=This is a header
footer=This is a footer
```

Figure 29. Example of the 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 user 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.

Chapter 10. Linking z/OSMF tasks and external applications

To perform traditional system management tasks in z/OS, you might interact with several different interfaces, such as the TSO command line, graphical user interfaces, and web-style interfaces. In z/OSMF, it is possible to link or connect some of these tasks and external applications together for a smoother user experience. To help manage these connections, 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 30 depicts the relationship of these components in the application linking process.

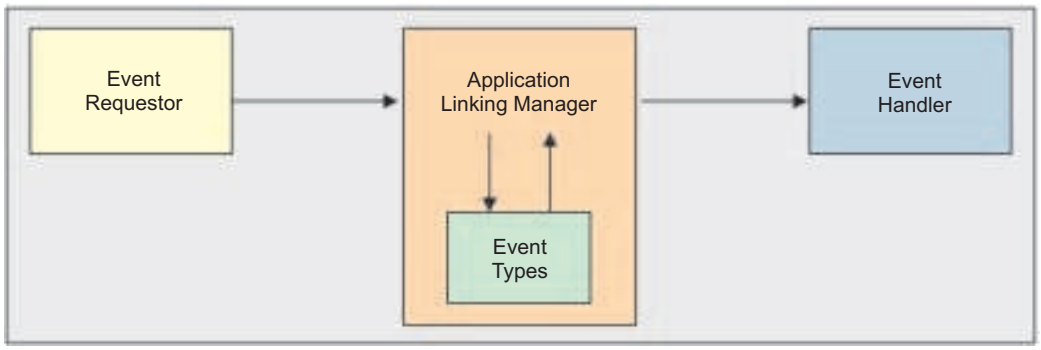


Figure 30. Key components in the application linking process

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.

z/OSMF includes a number of predefined event types, requestors, and handlers. For a list, see the topic about the event types, requestors, and handlers that are shipped with z/OSMF in *IBM z/OS Management Facility Programming Guide*.

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.

© Copyright IBM Corp. 2009, 2016

- Define new handlers; view, enable, disable, and delete existing handlers; and make a handler the default handler.

For assistance with the Application Linking Manager task, see the online help.

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 *IBM z/OS Management Facility Programming Guide*.

Chapter 11. Configuring your system for asynchronous job notifications

To allow HTTP client applications on your z/OS system to receive asynchronous job notifications, your system must be configured as described in this topic.

The z/OS jobs REST interface provides a set of REST services that allow a client application to perform operations with batch jobs on a z/OS system. Through the z/OS jobs REST interface services, an application can:

- 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
- Delete a job (cancel a job and purge its output).

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, either z/OS or non-z/OS. The z/OS jobs REST interface services are described in the document *IBM z/OS Management Facility Programming Guide*.

You can use the asynchronous job notifications function of z/OSMF to allow your programs to be notified when submitted jobs complete. With this function, the program that submits the job through the z/OS jobs REST interface services PUT method specifies a URL when submitting the job. When the job ends, z/OSMF returns an HTTP message to the URL location, indicating the job completion status. The data returned is in the form of a JSON document.

The asynchronous job notifications function is available for the JES2 subsystem only; it is not available for the JES3 subsystem.

The key requirement is that you must create a subscription to the Common Information Model (CIM) jobs indication provider for your system. Also, if the job notifications will require a secure network connection, you must enable an SSL connection between the client application and the server, including the sharing of digital certificates.

This topic is organized as follows:

- "Creating the CIM indication provider subscription"
- "Enabling secure job completion notifications for your programs" on page 91.

For extensive information on CIM indications and their use in a z/OS system (a *CIM managed system*), see *z/OS Common Information Model User's Guide*.

Creating the CIM indication provider subscription

To use the asynchronous job notification function that is provided with z/OS jobs REST interface, your system requires a subscription to the CIM jobs indication provider. You can create the subscription from the z/OSMF installer user ID, through a series of CIM command-line utilities. The subscription must be created on the local system, that is, the system on which z/OSMF is running. This topic provides instructions and considerations for creating the subscription.

© Copyright IBM Corp. 2009, 2016

As described in *z/OS Common Information Model User's Guide*, an indication provider is a CIM provider that recognizes when a particular type of event occurs on the managed system. To use the asynchronous job notification function that is provided with z/OSMF, your system requires a subscription to the CIM jobs indication provider. This indication provider is included with the z/OS operating system, and is defined as the CIM class IBMzOS_JobsIndicationProvider.

With the subscription created, the HTTP applications on your system can submit work to run on z/OS and be notified of the job completion status. On the submit request (an HTTP PUT method), the application specifies a location for receiving the job completion notification, such as a servlet that you have designed to take action in response to job completions.

Summary of the steps for creating a subscription:

- Select a user ID with sufficient access to CIM resources, such as the z/OSMF installer user ID; see "Selecting the appropriate user ID "
- Ensure that the user profile has the correct environment variable settings for entering CIM line commands; see "Customizing the administrator profile for running CIM commands" on page 87
- From this user ID, create the subscription to the CIM Jobs Indication Provider through a series of CIM line commands; see "Procedure for creating a subscription" on page 87.

Selecting the appropriate user ID

Choose an appropriate user ID for creating the subscription, one with sufficient access to CIM server resources to create CIM instances. Consider using the same user ID that you used earlier to install z/OSMF, as described in Chapter 3, "Configuring z/OSMF for the first time," on page 13. This user ID is likely to have the correct authorizations already, which it received during the configuration process. In effect, this user ID can serve as a CIM administrator, too. For more information, see "Ensure that the administrator role is authorized to the CIM server" on page 201.

CIM includes the CFZSEC job to help you authorize user IDs to CIM resources. See the topic on CIM server quick setup and verification in *z/OS Common Information Model User's Guide*. After the job is run, ask your security administrator to connect the user ID to the CFZADMGP group.

To perform these authorizations manually, do the following:

- Grant the user CONTROL access to the CIMSERV profile in the WBEM class. This access can be granted through an explicit PERMIT command, or, if the CIM administrator group is already permitted with CONTROL access, you can connect the user to the group. If necessary, refresh the WBEM class.
- Ensure that the user ID under which the CIM server is running has SURROGAT access for the new user ID. 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 user and authorize it. If necessary, refresh the SURROGAT class.
- Ensure that the user ID under which the CIM server is running has UPDATE access to the following profiles in the SERVAUTH class:
  - CEA.*
  - CEA.CONNECT
  - CEA.SUBSCRIBE.*
  - CEA.SUBSCRIBE.ENF_078*

  Figure 31 on page 87 shows sample RACF commands that a security administrator can use to provide these CEA profile authorizations for the default CIM server user ID:

```
PERMIT CEA.* CLASS(SERVAUTH) ID(CFZSRV) ACCESS(UPDATE)
PERMIT CEA.CONNECT CLASS(SERVAUTH) ID(CFZSRV) ACCESS(UPDATE)
PERMIT CEA.SUBSCRIBE.* CLASS(SERVAUTH) ID(CFZSRV) ACCESS(UPDATE)
PERMIT CEA.SUBSCRIBE.ENF_0078* CLASS(SERVAUTH) ID(CFZSRV) ACCESS(UPDATE)
```

Figure 31. Sample RACF commands for creating CIM authorizations

If necessary, refresh the SERVAUTH class.

Customizing the administrator profile for running CIM commands

The CIM server commands are UNIX style programs running in a UNIX shell. To ensure that the z/OSMF administrator can use the CIM commands, verify that the administrator profile is properly set up, as described in "Customizing the administrator role for running CIM commands" on page 202.

Alternatively, you can use the following command to temporarily include the CIM profile settings for the duration of a shell session:

```
. /usr/lpp/wbem/install/profile.add
```

If so, you must enter this command whenever the z/OSMF administrator logs into the z/OS UNIX shell to run CIM command-line utilities.

Procedure for creating a subscription

This topic describes the steps for creating a subscription to the CIM jobs indication provider.

Before you begin

Ensure that the CIM server is running on your system. To do so, you can enter the following command from the operator console to display information about your active jobs and started tasks:

```
D A,CFZCIM
```

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

Check the command output for the CIM server started task. If the CIM server is not already started, follow the steps described in *z/OS Common Information Model User's Guide* to start it. 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*.

Determine whether the CIM jobs indication provider subscription already exists. To view the existing subscriptions for your system, enter the following command from the z/OS UNIX shell command line:

```
cimsub -ls -v -n root/PG_InterOp
```

If the command output includes an entry like the one shown in Figure 32, the subscription for asynchronous job notification is already in place.

```
Handler:           root/PG_InterOp:IBMzOS_Job_Completed_ListenerDestination.<Name>
Query:             "SELECT * FROM IBMzOS_Job_Completed"
SubscriptionState: Enabled
```

Figure 32. Subscription values for asynchronous job notification

In Figure 32, `<Name>` is the name that was specified when the handler instance was created. If the subscription was created using the examples in this topic, for example, `<NAME>` would be `IZU_Job_Completed_Handler`.

If the command output is only a partial match with Figure 32 on page 87, observe the following considerations:

- If the handler value is correct, but the query value is not, a subscription was created using a filter other than the value that should be used with the listener destination. You can proceed with creating another subscription with the correct filter, but be aware that multiple notifications for the same completed job might result.
- If both the handler and query values are correct, but the SubscriptionState value is set to disabled, you can enter the following command to enable the subscription: **cimsub -e**

Otherwise, if the handler value is not present or correct, you must create the subscription to enable asynchronous job notification. Follow the procedure described in this topic.

About this task

A subscription requires the creation of three CIM instances:
- Filter instance
- Handler instance
- Subscription instance.

The examples in the section show the commands as they would be entered from a shell script.

If a command fails with the following message, verify that the CIM server is running:

```
Pegasus Exception: PGS08000: CIM HTTP or HTTPS connector cannot connect
to local CIM server. Connection failed.
```

Procedure

1. **Obtain the system name.** To obtain the system name, enter the following command from the z/OS UNIX shell command line:

   ```
   cimcli ei IBMzOS_ComputerSystem -niq -pl Name
   ```

   The results should look like the following example, where `MY.TEST.SYSTEM.COM` is the system name.

   ```
   Command:

   SYSTEMNAME=`cimcli ei IBMzOS_ComputerSystem -niq -pl Name |
     grep -e "^Name =" |
     sed  -e "s/Name = //g" |
     sed  -e "s/\"//g" |
     sed  -e "s/;//g"`

   echo $SYSTEMNAME

   Result:

   MY.TEST.SYSTEM.COM
   ```

   Record the result. You will use this value in subsequent steps.

2. **Create a filter instance.** To create the filter instance, enter the following command from the z/OS UNIX shell command line:

   ```
   cimcli ci CIM_IndicationFilter \
     SystemCreationClassName=CIM_ComputerSystem \
     SystemName=$SYSTEMNAME \
     CreationClassName=CIM_IndicationFilter \
     Name=IZU_Job_Completed_Filter \
   ```

```
  Query="SELECT * FROM IBMzOS_Job_Completed" \
  QueryLanguage="CIM:CQL" \
  SourceNamespace="root/cimv2" \
  -n root/PG_InterOp
```

where the value for *$SYSTEMNAME* is the value that was returned in Step 1 on page 88. The results should look like the following example:

```
Command:

SYSTEMNAME=`cimcli ei IBMzOS_ComputerSystem -niq -pl Name |
  grep -e "^Name =" |
  sed  -e "s/Name = //g" |
  sed  -e "s/\"//g" |
  sed  -e "s/;//g"`

FILTER_REFERENCE=`cimcli ci CIM_IndicationFilter \
  SystemCreationClassName=CIM_ComputerSystem \
  SystemName=$SYSTEMNAME \
  CreationClassName=CIM_IndicationFilter \
  Name=IZU_Job_Completed_Filter \
  Query="SELECT * FROM IBMzOS_Job_Completed" \
  QueryLanguage="CIM:CQL" \
  SourceNamespace="root/cimv2" \
  -n root/PG_InterOp |
  sed -e "s/Returned Path  //"`

echo $FILTER_REFERENCE

Result:

CIM_IndicationFilter.CreationClassName="CIM_IndicationFilter",
Name="CMPI_Indication_Jobs_Filter_0000",
SystemCreationClassName="CIM_ComputerSystem",
SystemName="MY.TEST.SYSTEM.COM"
```

Record the result. You will use this value in a subsequent step.

3. **Create a handler instance.** To create the handler instance, enter the following command from the z/OS UNIX shell command line:

```
cimcli ci IBMzOS_Job_Completed_ListenerDestination \
  SystemCreationClassName=CIM_ComputerSystem \
  SystemName=$SYSTEMNAME \
  CreationClassName=IBMzOS_Job_Completed_ListenerDestination \
  Name=IZU_Job_Completed_Handler \
  -n root/PG_InterOp
```

where the value for *$SYSTEMNAME* is the value that was returned in Step 1 on page 88.

The results should look like the following example:

```
Command:

SYSTEMNAME=`cimcli ei IBMzOS_ComputerSystem -niq -pl Name |
  grep -e "^Name =" |
  sed  -e "s/Name = //g" |
  sed  -e "s/\"//g" |
  sed  -e "s/;//g"`

HANDLER_REFERENCE=`cimcli ci IBMzOS_Job_Completed_ListenerDestination \
  SystemCreationClassName=CIM_ComputerSystem \
  SystemName=$SYSTEMNAME \
  CreationClassName=IBMzOS_Job_Completed_ListenerDestination \
  Name=IZU_Job_Completed_Handler \
  -n root/PG_InterOp |
  sed -e "s/Returned Path  //"`

echo $HANDLER_REFERENCE

Result:

IBMzOS_Job_Completed_ListenerDestination.CreationClassName=
"IBMzOS_Job_Completed_ListenerDestination",
Name="IZU_Job_Completed_Handler",
SystemCreationClassName="CIM_ComputerSystem",
SystemName="MY.TEST.SYSTEM.COM"
```

Record the result. You will use this value in a subsequent step.

4. **Create the subscription instance.** This step uses the filter and handler references that you collected in the previous steps. To create and enable a subscription instance, enter the following command from the z/OS UNIX shell command line:

   ```
   cimcli ci CIM_IndicationSubscription \
     Filter="root/PG_InterOp:"$FILTER_REFERENCE \
     Handler="root/PG_InterOp:"$HANDLER_REFERENCE \
     SubscriptionState=2 \
     -n root/PG_InterOp
   ```

   where $FILTER_REFERENCE and $HANDLER_REFERENCE are the values you collected previously.

   The results should look like the following example:

```
Command:

<filter and handler commands omitted for this example>

SUBSCRIPTION=`cimcli ci CIM_IndicationSubscription \
  Filter="root/PG_InterOp:"$FILTER_REFERENCE \
  Handler="root/PG_InterOp:"$HANDLER_REFERENCE \
  SubscriptionState=2 \
  -n root/PG_InterOp |
  sed -e "s/Returned Path  //"`

echo $SUBSCRIPTION

Result:

CIM_IndicationSubscription.Filter="root/PG_InterOp:CIM_IndicationFilter.CreationClassName=\
"CIM_IndicationFilter\",Name=\"IZU_Job_Completed_Filter\",SystemCreationClassName=\
"CIM_ComputerSystem\",SystemName=\"MY.TEST.SYSTEM.COM\
"",Handler="root/PG_InterOp:IBMzOS_Job_Completed_ListenerDestination.CreationClassName=\
"IBMzOS_Job_Completed_ListenerDestination\",Name=\"IZU_Job_Completed_Handler\
",SystemCreationClassName=\"CIM_ComputerSystem\",SystemName=\"MY.TEST.SYSTEM.COM\""
```

What to do next

Verify that the subscription was created. To do so, you can enter the following command from the z/OS UNIX shell command line: **cimsub -ls -v**.

If necessary, you can remove the subscription and its related structures, as follows:

- To remove the subscription, filter, and handler instances with one command invocation:

```
cimsub -ra -n root/PG_InterOp -F IZU_Job_Completed_Filter
-H IZU_Job_Completed_Handler
```

- To remove the subscription only:

```
cimsub -rs -n root/PG_InterOp -F IZU_Job_Completed_Filter
-H IZU_Job_Completed_Handler
```

- To remove the handler only:

```
cimsub -rh -n root/PG_InterOp
-H IBMzOS_Job_Completed_ListenerDestination.IZU_Job_Completed_Handler
```

- To remove the filter only:

```
cimsub -rf -n root/PG_InterOp -F IZU_Job_Completed_Filter
```

Enabling secure job completion notifications for your programs

Depending on your installation security requirements, you might need to enable secure connections for program that will receive asynchronous job notifications. The communication between the client (your program) and the CIM server can be secured through encryption (SSL). Additionally the CIM server can be authenticated through the use of a certificate. This topic describes the setup required for ensuring that your program can receive job completion notifications through secure SSL connections.

Configuring the CIM server for SSL connections

If your installation uses a program (such as a servlet) to receive job completion notifications from jobs submitted through z/OS jobs REST interface services, you might require that such connections be secured through SSL. If so, you must ensure that the CIM server on the z/OSMF system is configured to use the AT-TLS feature of z/OS for sending HTTPS transmissions.

For information about how to configure the CIM server HTTPS connection using AT-TLS, see *z/OS Common Information Model User's Guide*.

SSL connections can use either one-way or two-way authentication of server certificates. You must determine which type of SSL security is needed for communicating job completion notifications in your enterprise. The job notifications contain job names and other details that your installation might regard as confidential information.

Consider the following:

- If the servlet runs in the same security domain as the z/OSMF (that is, within the same system, keyring, or realm), you might not need to secure the notifications between the CIM server and the servlet. Here, you could specify NO-AUTH security for your SSL connections.
- If the servlet is required to authenticate the job completion notifications it receives, but the CIM server can trust the target servlet, you can use BASIC AUTH security for the SSL connections.
- If two-way authentication is required—that is, the servlet must be able to determine if an incoming request was from an authenticated server—you must use CLIENT CERT security. Here, each connection results in an exchange of certificates between the client (the servlet) and the server (the CIM server).

The remainder of this topic describes the steps needed to set up secure SSL connections for your job completion notifications. The instructions that follow cover both BASIC AUTH and CLIENT-CERT forms

of SSL security setup. In the latter case, the key requirement is to export certificates and to enable the sharing of the certificates between the CIM server and the user-supplied servlet to which the notifications are being sent.

This information assumes the use of RACF. If you use another security product, contact the vendor for more information.

Enabling BASIC AUTH connections for your servlet

This section describes a procedure for enabling the CIM server to send job completion notifications through the HTTPS protocol. This procedure involves using a SAF keyring as the certificate trust store, and configuring the Communication Server Policy Agent, as described in *z/OS Common Information Model User's Guide*.

When Transparent Transport Layer Security (TTLS) is enabled, Policy Agent (PAGENT) must be started before TCP/IP can join the network. Transparent Transport Layer Security (TTLS) is also referred to as *Application Transparent - Transport Layer Security (AT-TLS)*.

Follow these steps:

1. Create a SAF keyring to be used by TCP/IP for the CIM server outbound SSL connections.
2. Add the signer certificate that is used by the servlet for receiving secure job completion notifications. That is, add the signer certificate of the target server's SSL digital certificate to the SAF keyring that is identified for use by CIM in the Policy Agent TLS policy definition. For example, the default configuration for z/OSMF uses a signer certificate labelled zOSMFCA. Thus, you must add the zOSMFCA certificate (or an alternative, if you used a non-default certificate) to the CIM server keyring that is identified in the Policy Agent TLS policy.
3. Configure the Communication Server Policy Agent. Consider using the z/OSMF Configuration Assistant task to perform this step. For the TLS policy, do the following:
   a. Create the `/etc/pagent.conf` file, as described in the *z/OS Common Information Model User's Guide*. For more information, see the Communication Server Configuration Guide and Reference publications.
   b. Create the `/etc/tlsPolicy` file, following the instructions in *z/OS Common Information Model User's Guide* for securing CIM indications. Use the name of the SAF keyring created in Step 1.
   c. Create the `/etc/stackPagent` file, specifying the job name that is used by TCP/IP.
   d. Add the `TCPCONFIG TTLS` statement to the TCPIP PROFILE.
4. Restart TCP/IP and wait for the following message to be displayed on the system console:
   ```
   EZZ4248E TCPIP WAITING FOR PAGENT TTLS POLICY
   ```
5. Start the policy agent (PAGENT). On successful start-up, messages similar to the following are written to the console. If you are not using hardware cryptography, you can ignore the last message regarding ICSF:
   ```
   $HASP373 PAGENT   STARTED
   EZZ8431I PAGENT STARTING
   EZZ8432I PAGENT INITIALIZATION COMPLETE
   EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPIP : TTLS
   EZD1586I PAGENT HAS INSTALLED ALL LOCAL POLICIES FOR TCPIP
   EZZ4250I AT-TLS SERVICES ARE AVAILABLE FOR TCPIP
   EZD1576I PAGENT IS READY FOR SERVICES CONNECTION REQUESTS
   EZD1290I TCPIP ICSF SERVICES ARE CURRENTLY UNAVAILABLE FOR AT-TLS GROUP
   group_TLSenable
   ```

If TCP/IP and the Policy Agent are not configured properly, any attempts by the CIM server to connect through the HTTPS protocol are intercepted by TCP/IP, and an HTTP connection is created instead. No errors are logged by TCP/IP or the CIM server, other than possible SSL errors at the target server to which CIM attempted to connect.

Enabling CLIENT CERT connections for your servlet

There is little difference between the setups for the CIM server to send job completion notifications through normal SSL and SSL with client certificate authentication. The only difference with using client certificate authentication is that you must ensure that the CIM server keyring has a default personal certificate (and the signer certificate used to create the default personal certificate) and that the CIM server signer certificate is added to the SAF keyring. By default, the keyring is called IZUKeyring.IZUDFLT.

Follow these steps:

1. Create a SAF keyring to be used by TCP/IP for the CIM server outbound SSL connections. Add the z/OSMF CA certificate to this keyring. The default name of this CA certificate in a standard z/OSMF installation is "zOSMFCA" and is associated with the IZUSVR1 userid.

   You can use the following commands to accomplish this setup. Note that IZUSVR1 is the user ID associated with the CIM server.

   ```
   RACDCERT ADDRING(CIMServerKeyring.SY1) ID(IZUSVR1)

   RACDCERT ID(IZUSVR1) CONNECT(CERTAUTH LABEL('zOSMFCA')
         RING(CIMServerKeyring.SY1) USAGE(CERTAUTH) )
   ```

2. Configure the Communication Server Policy Agent to send CIM indications over SSL per the instructions in the CIM Users Guide. This includes the step of adding TCPCONFIG TTLS to the TCPIP PROFILE to enable AT-TLS in the TCP/IP stack. Doing so causes TCP/IP to pause initialization until the Policy Agent has been started.
3. Add the signer certificate used by the servlet for receiving secure job completion notifications.
4. Configure the Communication Server Policy Agent. Consider using the Configuration Assistant task to perform this step. In the policy, specify the following:
   a. Create the /etc/pagent.conf file, as described in the CIM User's Guide. You will probably also need to refer to the Communication Server Configuration Guide and Reference manuals.
   b. Create the /etc/tlsPolicy file, following the instructions in the CIM User's Guide for securing CIM indications. Use the name of the SAF keyring created in Step 1.
   c. Create the /etc/stackPagent file, specifying the jobname used by TCP/IP
   d. Add the following statement to the TCPIP PROFILE: `TCPCONFIG TTLS`
5. Restart TCP/IP and wait for the following message to be displayed on the system console:

   ```
   EZZ4248E TCPIP WAITING FOR PAGENT TTLS POLICY
   ```

6. Start the policy agent (PAGENT). On successful start-up, a set of message similar to these are written to the console. You can ignore the last message regarding ICSF if you are not using hardware cryptography:

   ```
   $HASP373 PAGENT   STARTED
   EZZ8431I PAGENT STARTING
   EZZ8432I PAGENT INITIALIZATION COMPLETE
   EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPIP : TTLS
   EZD1586I PAGENT HAS INSTALLED ALL LOCAL POLICIES FOR TCPIP
   EZZ4250I AT-TLS SERVICES ARE AVAILABLE FOR TCPIP
   EZD1576I PAGENT IS READY FOR SERVICES CONNECTION REQUESTS
   EZD1290I TCPIP ICSF SERVICES ARE CURRENTLY UNAVAILABLE FOR AT-TLS GROUP
   group_TLSenable
   ```

Coding considerations for your servlet

To ensure that a servlet that is the target for a notification (that is, specified as the URL for a job completion notification) is secure and only accepts requests from authorized clients, do the following:

1. The servlet's web descriptor must specify SSL with client certificate authentication in the application's web descriptor. For example:

```
<security-constraint>
     <display-name>SecuredConstraint</display-name>
     <web-resource-collection>

        <web-resource-name>Test</web-resource-name>
        <url-pattern>/*</url-pattern>
        <http-method>GET</http-method>
        <http-method>HEAD</http-method>
        <http-method>POST</http-method>
        <http-method>PUT</http-method>
        <http-method>DELETE</http-method>
     </web-resource-collection>

     <user-data-constraint>
        <transport-guarantee>CONFIDENTIAL</transport-guarantee>
     </user-data-constraint>
</security-constraint>

<login-config>
     <auth-method>CLIENT-CERT</auth-method>
</login-config>
```

2. The servlet POST method processing must check the values of HttpServletRequest AuthType and RemoteUser. These values can be through the HttpServletRequest getAuthType and getRemoteUser methods, respectively. The AuthType value must be "CLIENT-CERT" and the remote user value cannot be null for the servlet to process the request. If the request was sent through normal server authentication SSL (that is, without requiring authentication based on client certificate), or the client certificate was unavailable, the AuthType and RemoteUser values would be null and the servlet should not process the request.

   For example, your servlet could use code such as the following to perform this check:

```
public void checkUserAuthorized(HttpServletRequest request,
   IRestResourceHandler handlerForRequest)
   throws AuthorizationException, DataException {

  String authType = request.getAuthType();
  String user = request.getRemoteUser();

  if (authType==null || user==null || !authType.equals("CLIENT_CERT")) {
   System.out.println("\nRejecting request from an unauthenticated user.\n");

   Exception ex = new Exception("Rejecting request from an unauthenticated user.");
   throw new AuthorizationException(Level.WARNING, null, null, ex);
  }
 }
```

Considerations for receiving job notifications

SSL connections can use either one-way or two-way authentication of server certificates. To allow for secure communications between your program and z/OSMF, see the instructions that follow.

Do the following:

1. You must provide an HTTP server, such as a TomCat server, for receiving the notifications. z/OSMF does not include an HTTP server.
2. Generate a server certificate for your server.
3. Ensure that the CIM server running on the local z/OSMF system is configured to use AT-TLS for sending HTTPS transmissions.
4. Import the target server's CA certificate into the CIM server keyring

Chapter 12. Adding links to z/OSMF

Generally, when you want to add a link to the z/OSMF navigation area, you can do so through the Links task of z/OSMF. In some situations, however, you might be asked at the direction of a vendor to add a link to z/OSMF through the link properties file. If so, you can follow the steps in this section.

After a link is added to the z/OSMF navigation area, you can modify or remove the link through the Links task, as described in the online help.

Steps for adding a link to z/OSMF

A sample link properties file is supplied with z/OSMF:

`<product_dir>/samples/sampleLink.properties`

where `<product_dir>` is the z/OSMF product directory. By default, this is `/usr/lpp/zosmf`.

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 33, the link properties file contains the following input fields for a link:

```
LinkName=
LinkURL=
LinkNavigationCategory=
LinkAuthorizedRoles=
LinkSafSuffix=
LinkLaunchWorkArea=
```

Figure 33. 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 (\u*xxxx*) 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`

© Copyright IBM Corp. 2009, 2016

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 where the link is to appear in the navigation area. You can assign the link to any valid category, or you can have the link appear outside of the categories. If assigned to a category, the link is sorted alphabetically with the other links and tasks in the category. If added outside of the categories, the link is placed after the Welcome task in the navigation area, sorted alphabetically with any other uncategorized links.

To indicate the placement of the link, 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.
10 z/OSMF Settings.
11 No category. The link is placed outside of the categories, after the Welcome task.

Specify one value 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/OS Security Administrator
- 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 link is added 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 z/OSMF SAF profile prefix (by default, IZUDFLT), followed by ZOSMF.LINK. Specify a unique resource name suffix, for example:
`IZUDFLT.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.

You must provide a unique SAF resource name suffix for each link. 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 34 shows an example of a completed link definition.

```
LinkName=IBM
LinkURL=http://www.ibm.com
LinkNavigationCategory=3
LinkAuthorizedRoles=z/OSMF Guest, z/OSMF User
LinkSafSuffix=IBM_COM
LinkLaunchWorkArea=false
```

Figure 34. Example of a link definition

3. **Restart the z/OSMF server to make your changes effective**. The new link does not appear in the z/OSMF navigation area until after z/OSMF is started.

   To start z/OSMF, enter the appropriate START command.

Managing security for links in z/OSMF

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

Managing a link in z/OSMF involves the following steps:
- Defining the link to z/OSMF through the Links task
- Controlling access to the link through the ZMFAPLA resource class profile.

The z/OSMF configuration process defines a generic resource profile for links and permits groups to it. Specifically, links in z/OSMF are protected under the generic resource profile: <*SAF-prefix*>.ZOSMF.LINK.** where <*SAF-prefix*> is the SAF profile prefix that was defined for your configuration (IZUDFLT by default). 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. z/OSMF does not, by default, permit the z/OS security administrator role to the ZOSMF.LINK** profile.

For more information about the Links task, see the online help.

Defining a link as a protected resource

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 SAF resource name, 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 35 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.

```
RDEFINE ZMFAPLA (IZUDFLT.ZOSMF.LINK.Z_OS_BASICS_INFORMATION_CENTER) UACC(NONE)
PERMIT IZUDFLT.ZOSMF.LINK.Z_OS_BASICS_INFORMATION_CENTER CLASS(ZMFAPLA) ID(IZUUSER) ACC(READ)
```

Figure 35. Example: Defining a link resource name and permitting a group to it

If you change a link SAF resource name through the Links task, ensure that the new link resource name is adequately protected through a ZMFAPLA resource profile definition. You might need to create a new profile to properly secure the link.

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

Chapter 13. Deleting incidents and diagnostic data

For installations that use the Incident Log task, the **ceatool** program provides a command line interface for deleting the incidents that you no longer want to retain.

When an incident occurs, the system typically creates an SVC dump and collects diagnostic log snapshots of the operations log, error log, and error log summary. This data can consume a large amount of system resources, such as DASD space and logstream slots, if incidents are not periodically deleted. To delete incidents, you can use the delete option provided in the **ceatool** command-line interface.

Tip: You can also use the **Delete Incident** action provided in the Incident Log task. For instructions, see the topic about *Deleting incidents* in the z/OSMF online help.

Overview

The **ceatool** command-line interface is a utility that you can use to send requests to the z/OS common event adapter (CEA) component. With this utility, you can manage the incidents that were created for the z/OSMF Incident Log task. Specifically, you can use a z/OS UNIX System Services shell, a JCL job, or a cron job to delete incidents and the associated diagnostic data. The diagnostic data to be deleted includes:

- Error log
- Error log summary
- Operations log
- Entry for the dump in the sysplex dump directory
- SVC dump (optional)

Note: The utility deletes only incidents that are not associated with a problem number or tracking ID. These incidents are referred to as *inactive incidents*. The utility ignores all active incidents. To delete active incidents, use the **Delete Incident** action provided in the Incident Log task.

Before invoking the utility

Before invoking the utility, complete the following steps:

1. Ensure that the common event adapter (CEA) component and the System REXX (SYSREXX) component are active on your z/OS system. For instructions, see "Ensure that common event adapter (CEA) is configured and active" on page 219 and "Ensuring that System REXX is set up and active" on page 221.
2. Ensure that the user ID you are using to invoke the utility is authorized to access SAF resource CEA.CEAPDWB.CEADELETEINCIDENT, which is defined in the SERVAUTH class.
3. Ensure that the PATH environment variable is set to the directory in which the utility is installed. By default, the utility is installed in the `/bin` directory.
4. Ensure that the NLSPATH environment variable contains `/usr/lib/nls/msg/%L/%N`, which is, by default, the directory in which the CEA message catalog, called *ceamsg.cat*, is installed.

If these requirements are not satisfied, errors will occur when you invoke the utility.

When you configure the Incident Log plug-in for z/OSMF, you specify a high-level qualifier to use for naming log snapshot data sets. By default, this value is `CEA`. z/OS V2R1 increased the allowable length of this high-level qualifier from four- to eight-characters through the new HLQLONG statement in member CEAPRMxx. If your installation uses systems with a mix of shorter and longer high-level qualifiers, be sure to run the **ceatool** program from a system in your sysplex that specifies the HLQLONG value. Doing so ensures allows the **ceatool** program to locate all dump data sets, regardless of which style of high-level qualifier is used.

© Copyright IBM Corp. 2009, 2016

Invoking the utility

The **ceatool** command-line interface must be invoked from the z/OS UNIX System Services shell or a BPXBATCH environment. Figure 36 shows the format of the **ceatool** command, which invokes the utility.

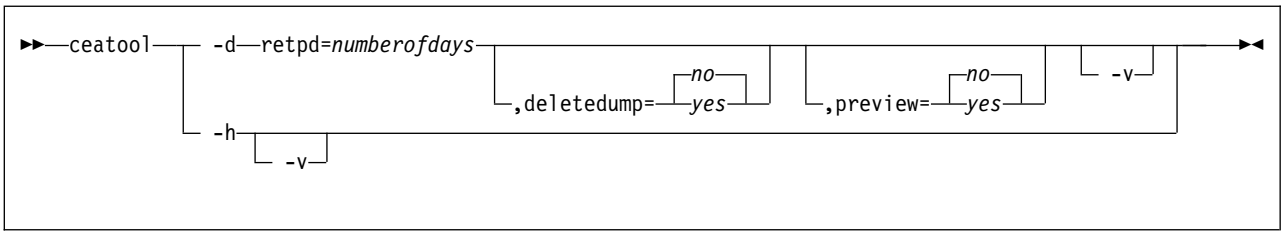


Figure 36. Format of the **ceatool** *command.*

This figure shows the valid syntax options for the ceatool command.

Where:

-d Deletes incidents that satisfy the specified criteria. Use the following options to identify the incidents to be deleted:

retpd=*numberofdays*
This is a required parameter that indicates the number of days an incident must be kept before it can be deleted. All inactive incidents that are older than the retention period will be deleted. The value for *numberofdays* can be any whole number in the range of 0 - 9999.

The retention period is derived from the current time. For example, if the retention period is one (retpd=1) and the current time is 10:00 am, all incidents that occurred at or before 10:00 am yesterday will be deleted.

To delete all inactive incidents, use a retention period of zero (retpd=0).

deletedump
This is an optional parameter that indicates whether the SVC dumps associated with an incident will be deleted. The value can be:

yes All diagnostic data associated with an incident, including the SVC dumps, will be deleted when the incident is deleted.

no All diagnostic data associated with an incident, except the SVC dumps, will be deleted when the incident is deleted. This is the default.

Specify this value if your installation has procedures or policies for managing dump data sets. Doing so instructs the utility to ignore the dump data sets during delete processing.

preview
This is an optional parameter that indicates whether to activate preview mode. The value can be:

yes Preview mode is enabled. In this case, the incidents that match the filter criteria will *not* be deleted. Instead, the tool will provide the number of incidents that are candidates for deletion.

no Preview mode is disabled. In this case, the incidents that match the filter criteria will be deleted. This is the default.

-v Activates verbose mode, which issues additional diagnostic messages while the **ceatool** command is processing.

-h Displays usage help for the **ceatool** command.

You can use a JCL or cron job to invoke the utility, or you can enter the commands directly in the z/OS UNIX shell. To invoke the utility using a batch job, see sample job CEATOOL, which is supplied by IBM in SYS1.SAMPLIB(CEATOOL).

Important: Do not submit multiple, concurrent requests to delete incidents using the **ceatool** utility. Otherwise, errors might occur.

Examples

Table 10 provides sample commands to invoke the **ceatool** utility and describes the expected result for each command.

Table 10. Sample **ceatool** *commands*

Sample Command	Results
`ceatool -d retpd=7,deletedump=no`	Deletes inactive incidents and the corresponding diagnostic data, excluding SVC dumps, that are older than seven days.
`ceatool -d retpd=7,deletedump=yes`	Deletes inactive incidents and the corresponding diagnostic data, including SVC dumps, that are older than seven days.
`ceatool -d retpd=7,deletedump=yes -v`	Deletes inactive incidents and the corresponding diagnostic data, including SVC dumps, that are older than seven days. Because verbose mode is requested, additional diagnostic messages are displayed during processing.
`ceatool -d retpd=0`	Deletes all inactive incidents and the corresponding diagnostic data, excluding SVC dumps.
`ceatool -d retpd=7,preview=yes`	Displays the number of inactive incidents that are older than seven days. The incidents that satisfy the filter criteria are not deleted.
`ceatool -h`	Displays help for the **ceatool** command.
`ceatool -hv`	Displays help for the **ceatool** command, plus an additional message with the build date.

Verifying that the incidents were deleted

To verify that the incidents were deleted, complete one of the following steps:

- Display the list of incidents in the z/OSMF Incident Log task, and verify that the incidents in the specified retention period are not listed.
- Check the contents of the sysplex dump directory, and verify that the incidents in the specified retention period are not listed.

Note: If the utility encounters an error during delete processing, the processing will stop and any incidents that were *not* deleted before the error occurred will still be listed in the incident log and the sysplex dump directory.

Chapter 14. Troubleshooting problems

This chapter provides tips and techniques for troubleshooting 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 topics, as follows:

- "Resources for troubleshooting"
- "Tools and techniques for troubleshooting" on page 104
- "Common problems and scenarios" on page 117.

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 11 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 11. Summary of tools and information for troubleshooting problems with z/OSMF

Component or task	Tools to assist with troubleshooting	Where described	Associated messages
Workstation and web browser	Environment checker tool	"Verifying your workstation with the environment checker" on page 104.	N/A
z/OSMF core functions and system management tasks	• The About page • z/OSMF log files and tracing.	• "Finding information about z/OSMF" on page 113 • "Working with z/OSMF runtime log files" on page 114. • "Problems when using Configuration Assistant" on page 124.	Messages encountered while configuring z/OSMF; see Chapter 15, "Configuration messages," on page 129. z/OSMF messages. For assistance, click on the message help link. For Configuration Assistant, messages and pop-ups are supplied with the task.
z/OSMF server	z/OSMF log files and tracing.	"Optionally creating a IZUPRMxx parmlib member" on page 22.	• Chapter 15, "Configuration messages," on page 129 • z/OSMF messages. For assistance, click on the message help link.
WebSphere Liberty profile	Troubleshooting information is provided in the WebSphere Application Server for z/OS information center.	See the topics at: http://www.ibm.com/software/webservers/appserv/was/library/v85/was-zos/index.html.	Messages prefixed by `CW`.
CIM server and CIM providers	• CIM server logging • CIM server trace • CIM provider trace.	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*.	*z/OS Common Information Model User's Guide*.
Common event adapter (CEA)	System commands: • MODIFY CEA • MODIFY AXR • TRACE CT.	z/OS MVS System Commands.	*z/OS MVS System Messages* for information about: • WTO messages • CTRACE • Reason codes.

© Copyright IBM Corp. 2009, 2016

Tools and techniques for troubleshooting

This section describes the tools and techniques available for troubleshooting problems with 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 16.

Ensure that your browser is enabled for JavaScript. For instructions, see Table 13 on page 107 or Table 14 on page 110, 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 z/OSMF server job log, as described in "Step 3: Start the z/OSMF server" on page 31.
2. Follow the instructions for your particular browser in the online help for the tool.

Understanding the results of the tool

Table 12 describes the layout of the environment checker report.

Table 12. Columns in the environment checker tool results page

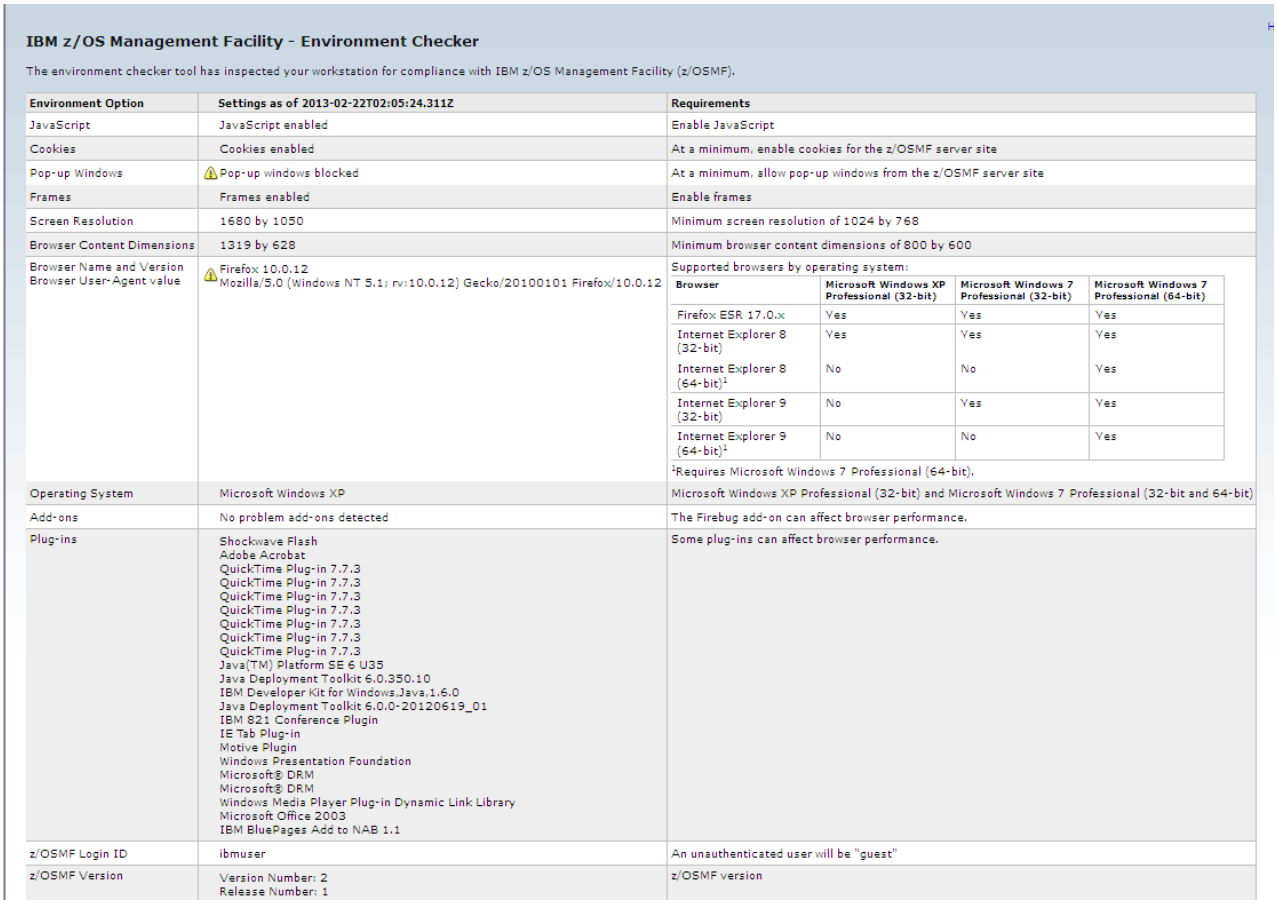
Column	Description
Environment Option	Browser setting that was examined by the environment checker tool.

Table 12. Columns in the environment checker tool results page (continued)

Column	Description
Settings as of *date-time*	Findings from the most recent invocation of the tool. This column indicates potential problems with your browser. 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.
Requirements	Recommended setting for your environment.

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.

Figure 37 on page 106 shows an example of the output from the environment checker tool.



IBM z/OS Management Facility - Environment Checker

The environment checker tool has inspected your workstation for compliance with IBM z/OS Management Facility (z/OSMF).

Environment Option	Settings as of 2013-02-22T02:05:24.311Z	Requirements
JavaScript	JavaScript enabled	Enable JavaScript
Cookies	Cookies enabled	At a minimum, enable cookies for the z/OSMF server site
Pop-up Windows	⚠ Pop-up windows blocked	At a minimum, allow pop-up windows from the z/OSMF server site
Frames	Frames enabled	Enable frames
Screen Resolution	1680 by 1050	Minimum screen resolution of 1024 by 768
Browser Content Dimensions	1319 by 628	Minimum browser content dimensions of 800 by 600
Browser Name and Version Browser User-Agent value	⚠ Firefox 10.0.12 Mozilla/5.0 (Windows NT 5.1; rv:10.0.12) Gecko/20100101 Firefox/10.0.12	Supported browsers by operating system:
Operating System	Microsoft Windows XP	Microsoft Windows XP Professional (32-bit) and Microsoft Windows 7 Professional (32-bit and 64-bit)
Add-ons	No problem add-ons detected	The Firebug add-on can affect browser performance.
Plug-ins	Shockwave Flash Adobe Acrobat QuickTime Plug-in 7.7.3 QuickTime Plug-in 7.7.3 QuickTime Plug-in 7.7.3 QuickTime Plug-in 7.7.3 QuickTime Plug-in 7.7.3 QuickTime Plug-in 7.7.3 QuickTime Plug-in 7.7.3 Java(TM) Platform SE 6 U35 Java Deployment Toolkit 6.0.350.10 IBM Developer Kit for Windows,Java.1.6.0 Java Deployment Toolkit 6.0.0-20120619_01 IBM 821 Conference Plugin IE Tab Plug-in Motive Plugin Windows Presentation Foundation Microsoft® DRM Microsoft® DRM Windows Media Player Plug-in Dynamic Link Library Microsoft Office 2003 IBM BluePages Add to NAB 1.1	Some plug-ins can affect browser performance.
z/OSMF Login ID	ibmuser	An unauthenticated user will be "guest"
z/OSMF Version	Version Number: 2 Release Number: 1	z/OSMF version

Browser	Microsoft Windows XP Professional (32-bit)	Microsoft Windows 7 Professional (32-bit)	Microsoft Windows 7 Professional (64-bit)
Firefox ESR 17.0.x	Yes	Yes	Yes
Internet Explorer 8 (32-bit)	Yes	Yes	Yes
Internet Explorer 8 (64-bit)[1]	No	No	Yes
Internet Explorer 9 (32-bit)	No	Yes	Yes
Internet Explorer 9 (64-bit)[1]	No	No	Yes

[1]Requires Microsoft Windows 7 Professional (64-bit).

Figure 37. Example output from the environment checker tool

If you are using the Internet Explorer browser:

- When working 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 112.
- When working with Resource Monitoring task, users who plan to export the data collected in a dashboard to a CSV file should ensure that automatic prompting for file downloads is enabled. See "Enabling automatic prompting for file downloads" on page 112.
- Do not use the browser with the Compatibility View feature enabled, which allows web sites to appear as they do when viewed with Internet Explorer Version 7. Some z/OSMF functions might not work correctly because Internet Explorer 7 is not supported.

When using the Internet Explorer 8 browser, you might experience:

- Browser memory issues, if you open multiple tabs. If so, close some unneeded tabs to use less memory.
- Slow responsiveness for certain data-intensive operations. If so, consider using another supported browser.

If you are using Internet Explorer 9 on a Windows 7 system, note that this browser uses Compatibility View mode by default. Here, it is recommended that you switch to Internet Explorer 9 mode, as follows:

1. From the *Tools* menu, click **F12 developer Tools** > **Browser Mode: IE9** tab.
2. Click **Internet Explorer 9**.

Recommended settings for the Mozilla Firefox browser

Table 13 shows the recommended settings for the Mozilla Firefox browser.

Table 13. Recommended settings for Firefox

Environment Option	Response
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 **Enable** > **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. By default, the Firefox browser is enabled for frames. If you need 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 13. Recommended settings for Firefox (continued)

Environment Option	Response
Screen Resolution	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** > **Settings** tab. 2. Move the slider to select a screen resolution of at least 1024 by 768 pixels. 3. Click **OK**.
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 13. Recommended settings for Firefox (continued)

Environment Option	Response
Plug-ins	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** > **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.

Recommended settings for the Windows Internet Explorer browser

Table 14 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 112.

Table 14. Recommended settings for Internet Explorer

Environment Option	Response
JavaScript	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** > **Security** tab. 2. Click **Custom Level**. 3. Scroll down to *Scripting*, then *Active Scripting*. 4. Click **Enable**. 5. Click **OK** > **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 **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**.

Table 14. Recommended settings for Internet Explorer (continued)

Environment Option	Response
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**.
Screen Resolution	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** > **Settings** tab. 2. Move the slider to select a screen resolution of at least 1024 by 768 pixels. 3. Click **OK**.
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, 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, it is recommended that you include only required add-ons with your browser. To disable an add-on, 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.

Table 14. Recommended settings for Internet Explorer (continued)

Environment Option	Response
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 or RMF exported data, 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 one of the procedures described in this section, depending on the version of the Internet Explorer browser.

Microsoft Internet Explorer Version 8:
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**.

Microsoft Internet Explorer Version 9:
Procedure

1. From the *Tools* menu, click **Internet Options** > **Security** tab.
2. Under *Select a zone*, click **Local intranet**.
3. Click **Sites**.
4. Click **Advanced**.
5. 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**.
6. Click **Close**.
7. Click **OK**.
8. 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 in the *Welcome* page. Details about the product build level, and the SMP/E-installed plug-ins and their versions (FMIDs), are displayed in a new browser window. If no plug-ins are installed, this area is empty.

Working with z/OSMF messages

z/OSMF records messages from the product interface, from tasks performed by z/OSMF users, and from programs running on the z/OS host system. Because of the various layers of functions involved in typical z/OSMF operations, locating a particular message might require you to check more than one location.

The following information provides an overview of the z/OSMF messages and where to find them:

Operator console messages

z/OSMF writes some messages to the operator console, with timestamps that are assigned by the console. z/OSMF also records these messages in the z/OSMF server joblog, with timestamps that are assigned by the JES subsystem. For example:

```
16.52.31 STC00049  IZUG400I: The z/OSMF Web application services are initialized.
```

Runtime data messages

z/OSMF collects its runtime data (log and trace messages) in the product logs directory. By default, the product logs directory is located in `/var/zosmf/data/logs`. The product logs directory contains one or more log files with the name IZUG*n*.log, where *n* is a numeral from 0 to 9.

In a runtime log file, a message might appear, as follows:

```
[tx0000000000000008:*izubootstrap*]
   2013-09-06T20:52:31.937Z|0000001F|com.ibm.zoszmf.navigation.listener.Boo
   tstrap|contextInitialized(ServletContextEvent)
   INFO:IZUG400I: The z/OSMF Web application services are initialized.
```

More information about these messages is provided in "Working with z/OSMF runtime log files" on page 114.

Messages from tasks

Messages issued by z/OSMF tasks are written to SYSOUT and the joblog. In addition, some z/OSMF tasks might write messages to the standard UNIX streams (STDOUT and STDERR) or to z/OS data sets. Typically, messages written to the UNIX streams do not have timestamps, for example:

```
.AUDIT   . CWWKZ0001I: Application IzuManagementFacilityWorkload....
```

Regardless of the message origin, z/OSMF records all of its messages and traces in the z/OSMF server logs directory. By default, the server logs directory is located in `/var/zosmf/data/logs/zosmfServer/logs/`. The server logs directory contains the following logs:

- `trace.log` data set contains z/OSMF related trace messages
- `messages.log` data set contains z/OSMF server messages. These messages have timestamps. For example:

```
[9/6/13 20:52:21:569 GMT] 0000001f
   com.ibm.ws.app.manager.internal.statemachine.StartAction A CWWKZ0001I:
   Application IzuManagementFacilityWorkloadManagement started in 4.121
   seconds.
```

In summary, by checking the operator console messages, the IZUGx.log file, and the messages.log file, you can locate any of the messages written by z/OSMF.

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 IZUG*n*.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 a user ID with z/OSMF administrator authority (that is, a user ID defined to the z/OSMF administrator group). Changing the level of logging and activating trace are performed through the IZUPRMxx parmlib member. For information, see “Optionally creating a IZUPRMxx parmlib member” on page 22.

For examples of z/OSMF runtime log data, and a description of the log file format, see “Examples of working with z/OSMF runtime logs” on page 115.

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 the z/OSMF server ends abnormally, however, the lock files might remain. If so, the log file handler appends 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 the IZUG0.log file cannot be accessed

If the current IZUG0.log file becomes unavailable, z/OSMF writes its runtime data to the z/OSMF server logs directory until the problem is resolved. Specifically, z/OSMF writes log and trace data to the following locations:

- Messages are written to the message.log file, which is located in `/var/zosmf/data/logs/zosmfServer/logs/messages.log`
- Trace data is written to the trace.log file, which is located in `/var/zosmf/data/logs/zosmfServer/logs/trace.log`

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.

Other log files in z/OSMF

Do not confuse the z/OSMF runtime log file with the job log files that are created during the configuration process. In contrast to runtime data, configuration log data is written to a file in the z/OSMF user file system, which is, by default `/var/zosmf`. If a problem occurs with the configuration log file, the log data is written instead to the directory specified by the `/tmp` parmlib statement.

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 38 shows portions of an example of z/OSMF server side log data.

```
2009-04-29T18:38:51.285Z|00000012|com.ibm.zoszmf.util.eis.cim.ccp.CimClientPool|getWBEMClient(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:145)
   com.ibm.zoszmf.util.eis.EisException.diagnoseAndThrow(EisException.java:221)
   com.ibm.zoszmf.util.eis.cim.ccp.CimClientPool.getWBEMClient(CimClientPool.java:279)

          o
          o
          o

+-> javax.wbem.WBEMException: JNI Exception type CannotConnectException:
   Cannot connect to local CIM server. Connection failed.
   org.sblim.cimclient.internal.jni.pegasus.CimReturnBuffer.getWBEMException(CimReturnBuffer.java:1244)
   org.sblim.cimclient.internal.jni.pegasus.NativeCimClient.verifyResult(NativeCimClient.java:1834)

          o
          o
          o

[tx0000000000000017:pegadm@IBM-FF0E8EC4FCB.xxx.yyy.com (GET) /zosmf/pdw/PdwServiceServlet/
Incidents?filters=IncidentTime(FROM1240704000000)&dojo.preventCache=1241030163470]
```

Figure 38. Portion of z/OSMF server side log data

As shown in Figure 38, 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.

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 final line in every log record is contained in 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 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 final 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 39.

```
[tx0000000000000ED5:debug2@9.10.83.13 (POST) /zosmf/IzuUICommon/UILoggerServlet?preventCache=1243956783360]
2009-06-02T15:37:51.933Z|0000001A|com.ibm.zoszmf.util.log.servlet.UILoggerServlet|UILoggerServlet::doPost()
SEVERE: [2009-06-02T15:36:47.047Z] IZUG802E: An error occurred. Error: "makeTree error: Error: timeout exceeded"
[tx0000000000000ED8:debug2@9.10.83.13 (POST) /zosmf/IzuUICommon/UILoggerServlet?preventCache=1243956783360]
2009-06-02T15:37:52.020Z|0000001A|com.ibm.zoszmf.util.log.servlet.UILoggerServlet|UILoggerServlet::doPost()
SEVERE: [2009-06-02T15:36:47.203Z] IZUG802E: An error occurred. Error: "makeTree error: Error: timeout exceeded"
[tx0000000000000ED9:debug2@9.10.83.13 (POST) /zosmf/IzuUICommon/UILoggerServlet?preventCache=1243956783360]
```

Figure 39. Example of z/OSMF client side log data

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 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.

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 base 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"
- "Problems when accessing the user interface" on page 118
- "Problems when using Configuration Assistant" on page 124
- "Problems when using the Incident Log task" on page 126
- "Problems when using the ISPF task" on page 125
- "Problems when attempting to send data" on page 127.

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:

- "IZUSEC job fails with an authorization failure for the issuer"
- "A z/OSMF script fails because no z/OS UNIX processes are available"
- "You receive message EDC5134I: Function not implemented" on page 118
- "RACDCERT or another RACF command abends during configuration" on page 118.

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 C, "Common event adapter (CEA) reason codes," on page 239.

IZUSEC job fails with an authorization failure for the issuer

Symptom: The job IZUSEC fails with an authorization failure message for the z/OSMF issuer's user ID.

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 installer user ID. For example:

```
ADDSD 'CEA.*' UACC(NONE)
PERMIT 'CEA.*' ID(CEA) ACCESS(ALTER)
PERMIT 'CEA.*' ID(USER-ID) ACCESS(ALTER)
```

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 exceeds 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. For example:

```
ALTUSER USER-ID 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 your security administrator.

You receive message EDC5134I: Function not implemented

Symptom: You receive the following message and error code:

```
atoe_getcwd error: EDC5134I Function not implemented. (errno2=0x052C04DC)
```

Possible Cause: The error code indicates that the system root directory is not mounted. However, this message is also issued if the OMVS home settings for a user ID include a root directory (/) specification, but the user ID does not have access to the root directory.

Corrective Action: Verify that the system root directory is mounted and that the user ID OMVS home settings are correct.

RACDCERT or another RACF command abends during configuration

Symptom: A RACF command abends with code `S684` or code `047` during the configuration process. On checking the script log, you find a message such as the following:

```
Script izutsoz.rexx returned with reason code -1668
```

Possible Cause: The RACF command is not defined in AUTHCMD section of your active IKJTSOxx parmlib member.

Corrective Action: Verify that the IKJTSOxx member defines the required RACF commands. See the list of IKJTSOxx parmlib updates in the *z/OS Program Directory*. The AUTHCMD section of member IKJTSOxx should list RACDCERT and a number of other RACF commands. You can update the IKJTSOxx member dynamically through the TSO command: `PARMLIB UPDATE(xx)` where *xx* is the correct suffix.

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" on page 119
- "Missing initialization message or JSP processing error when attempting to use z/OSMF" on page 119
- "Certificate error in the Mozilla Firefox browser" on page 120
- "Cannot log into z/OSMF" on page 122
- "Re-authenticating in z/OSMF" on page 122

- "Message or help information is not available" on page 123
- "Action or link that was previously provided is not available" on page 123
- "A script takes too long to run or is not responding" on page 124.

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 z/OSMF instance is running. If your network connectivity is functioning properly, there might be an issue with the digital certificates used for SSL connections.

Try the following network diagnostic techniques:
- Entering the command NSLOOKUP to verify that the host name is resolvable
- Pinging the host system for a response
- Running the TRACEROUTE command.

For more information about working with certificates, see "Configuring a primary z/OSMF for communicating with secondary instances" on page 74.

Missing initialization message or JSP processing error when attempting to use z/OSMF

Symptoms: The following symptoms occur in this sequence:

1. You start z/OSMF, but see no message in 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 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 z/OSMF. No .lck file exists either, which suggests that the logs are not active.
4. You examine the z/OSMF 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/lib/izugjni.jar.
   ```

Possible Cause: A failure of the JSP to compile typically means that one or more 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 the following:
- Shared libraries class path entries are incorrect.
- Class path entries point to missing JAR files.

In this situation, the message shows which paths were not found.

Investigation: Use the following procedure to determine the cause of the error.

1. Examine the contents of the directory where the JARs are supposed to exist:

   ```
   # ls /usr/lpp/zosmf/lib
   ls: FSUM6785 File or directory "/usr/lpp/zosmf/lib" is not found
   ```
2. The directory does not exist, so determine which file systems are mounted.

Corrective Action: Mount the necessary file system in the correct location and restart z/OSMF.

Certificate error in the Mozilla Firefox browser

When logging into z/OSMF for the first time, you might notice that the Mozilla Firefox browser displays the error message: `Secure Connection Failed`.

If the error message indicates that the browser does not recognize the Certificate Authority (CA) certificate that is configured for z/OSMF, you can resolve the error by adding the certificate to the browser security exception list, or importing the certificate into the browser. For information, see the following sections:

- "Adding the CA certificate to the security exceptions list"
- "Importing the CA certificate into the browser."

If the error message indicates that the certificate contains the same serial number as another certificate issued by the CA, it is possible that your browser contains a CA certificate from a previous installation of z/OSMF. If so, you can remove the older certificate from the browser, as described in "Removing the CA certificate from the browser" on page 121. Then, try again to access the z/OSMF Welcome page again and allow the new certificate to be stored in the browser.

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.

   Examine the *Issued To* fields. Verify that the information identifies 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, z/OSMF uses the certificate authority *zOSMFCA*.

   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 open to the z/OSMF interface.

Importing the CA certificate into the browser

You can import the CA certificate into your browser. Doing so involves exporting the z/OSMF certificate from RACF, transferring the CA certificate to your workstation, and importing the CA certificate into your browser.

The CA certificate is determined by your configuration setting for the variable IZU_DEFAULT_CERTAUTH. If this variable is set to Y, z/OSMF creates the CA during the configuration process. Otherwise, no CA is created, and z/OSMF uses CERTAUTH LABEL('zOSMFCA') to sign the certificate. z/OSMF uses the SAF key ring name `IZUKeyring.IZU_SAF_PROFILE_PREFIX`.

To import the CA certificate into your browser, do the following:

1. List the key rings for the z/OSMF server user ID, using the RACDCERT command, for example:

```
RACDCERT ID(IZUSVR1) LISTRING(*)
```

Figure 40 shows an example of the output from the RACDCERT command.

```
Digital ring information for user IZUSVR1:

  Ring:
       >IZUKeyring.IZUDFLT<
  Certificate Label Name              Cert Owner     USAGE      DEFAULT
  --------------------------------    ------------   --------   -------
  zOSMFCA                             CERTAUTH       CERTAUTH     NO
  Verisign Class 3 Primary CA         CERTAUTH       CERTAUTH     NO
  Verisign Class 1 Primary CA         CERTAUTH       CERTAUTH     NO
  Thawte Server CA                    CERTAUTH       CERTAUTH     NO
  Thawte Premium Server CA            CERTAUTH       CERTAUTH     NO
  Thawte Personal Basic CA            CERTAUTH       CERTAUTH     NO
  Thawte Personal Freemail CA         CERTAUTH       CERTAUTH     NO
  Thawte Personal Premium CA          CERTAUTH       CERTAUTH     NO
```

Figure 40. Digital ring information for the z/OSMF server user ID

Verify that the configured SAF key ring is shown for the z/OSMF server user ID. Note the key ring name and the certificate label (zOSMFCA, in this case).

2. Export the CA certificate using the RACDCERT command, for example:

```
RACDCERT EXPORT(LABEL(' zOSMFCA')) CERTAUTH
DSN('??????.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.

Removing the CA certificate from the browser

You can remove an older CA certificate from the browser to allow the CA certificate for the new release of z/OSMF to be added.

Do the following:

1. From the *Tools* menu, click **Options** > **Advanced** tab.
2. Click the **Encryption** tab.
3. Click *View Certificates*.
4. Click the **Servers** tab.
5. In the *Certificate Name* column, locate the *z/OSMF CertAuth* section.
6. Select the certificate files under z/OSMF and click **Delete**.
7. Click **OK**.

Try to access the z/OSMF Welcome page again. If prompted, allow the CA certificate to be stored in the browser. Your browser will now open to the z/OSMF interface.

Cannot log into z/OSMF

If a user receives an error while attempting to log into z/OSMF, try troubleshooting with the following steps.

Procedure

1. Verify that the user ID is correct and try logging in. If the user is still not able to log in, continue to the next step.
2. Ensure that the password associated with the user ID is correct. If the user is still not able to log in, continue to the next step.
3. It is possible that the password for the user ID has expired. To check, try logging in to TSO through an emulator.
4. If the user is 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, you must restart the z/OSMF server.

What to do next

If none of these steps resolve the problem, contact your system programmer for assistance. The system programmer should check the z/OSMF log files for messages indicating that the user ID is not authorized.

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.

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 495 minutes from the time you log into z/OSMF. Your installation can choose to modify this setting (SESSION_EXPIRE) using the IZUPRMxx parmlib member. z/OSMF. For details, see “Optionally creating a IZUPRMxx parmlib member” on page 22.

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.

Message or help information is not available

The help information for user interface (UI) pages or messages is not available.

Symptom

The user clicks on the help link to open a new window with help information for a UI page or message, but the help is not displayed. Instead, the error message `file not found` is displayed in the user's web browser.

Possible cause

The help files are missing or are not readable. Or, new help files were installed and z/OSMF was not restarted. By default, the z/OSMF help files must reside at the location `/var/zosmf/helps/eclipse/plugins`.

System programmer response

Use the following procedure to resolve this error:

1. Verify that symlinks exist in the `/var/zosmf/helps/eclipse/plugins` subdirectory. The symlinks should refer to the z/OSMF product directory, which, by default, is `/usr/lpp/zosmf`).
2. Verify that the EJBROLE resource class is defined properly; it is case sensitive.
3. Restart the z/OSMF server, for example, through the MVS **START** command.

User response

No action is required.

Action or link that was previously provided is not available

Symptom: An action or link that was previously provided in the user interface is disabled, not listed, or no longer provided.

Possible Cause:

- No items have been selected against which to perform the action.
- Too many items have been selected.
- The action or link is not applicable for the selected items.
- The event type is not registered or no handlers are available to process the request.

Administrator Action:

1. Determine if the user-interface control invokes an event type. For IBM-supplied event requestors, see the topic about the event types, requestors, and handlers that are shipped with z/OSMF in *IBM z/OS Management Facility Programming Guide*.
2. If the user-interface control invokes an event type, do the following:
   a. Verify that the event type is registered in the Application Linking Manager task.
   b. If the event type is not registered, ensure that the plug-in that registers the event type is configured in z/OSMF.
   c. If the plug-in is configured, you can use the Application Linking Manager task or the API to register the event type, or you can recycle the z/OSMF server to register it automatically. For IBM-supplied event types, to register them manually, specify the information included in the topic about the event types, requestors, and handlers that are shipped with z/OSMF in *IBM z/OS Management Facility Programming Guide*.
   d. Verify that a handler is registered for the event type and that the user is authorized to access the handler.

User Action: Ensure that items are selected and that the correct number and type of items are selected.

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.

Internet Explorer

- See the following Microsoft web site for information you might find useful: 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"
- "Log-on through the ISPF task takes too long, even though the system is enabled for reconnectable user sessions" on page 126.

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*.

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*. 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*. 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"
- "User encounters message ICH408I"
- "CEA address space is blocking the use of the sysplex dump directory" on page 127
- "CEA cannot allocate a data set for dump prepare or snapshot" on page 127
- "Diagnostic log streams and other incident data for deleted incidents are not being deleted over time" on page 127
- "Problems when attempting to send data" on page 127.

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 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: Determine whether the user should be allowed to update the master catalog. If so, you can authorize the user to create entries in the master catalog through the appropriate security commands.

To authorize a user to create entries in a user catalog, use the following command:

```
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 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 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. Typically, this is done by using z/OS System Display and Search Facility (SDSF) to examine the spooled output from the job.

FTP job status codes and other information

The Incident Log task 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.

Chapter 15. Configuration messages

This chapter describes the z/OSMF messages that you might encounter during the configuration process. These messages have a message ID between IZUG000-IZUG399.

For each configuration message, this document provides a detailed explanation of the message; describes the reason codes (if any) listed in each message; and, suggests actions that you can take to resolve the issue. The messages are organized by message ID.

Information about other messages you might encounter while configuring z/OSMF is provided in the following documents:

- Messages for the common event adapter (CEA) component of z/OS are prefixed by `CEA`. See *z/OS MVS System Messages*, which is available online in the IBM z/OS Internet Library.
- Messages for the WebSphere Liberty profile are prefixed by `CW`. For descriptions of the WebSphere messages, see the Messages topic: http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/topic/com.ibm.websphere.wlp.zseries.doc/ae/rwlp_messages.html.
- z/OS-specific messages for the CIM server are prefixed by `CFZ`. For information about CIM server logging and messages, see *z/OS Common Information Model User's Guide*.

All other messages for z/OSMF are documented in the z/OSMF node of the IBM Knowledge Center, which is available at https://www.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zosmfmessages.help.doc/izuG00hpMessages.html.

Because of the various layers of function involved in typical z/OSMF operations, locating a particular message might require you to check more than one location. For more information, see "Working with z/OSMF messages" on page 113.

IZUG000-IZUG399

This topic describes the z/OSMF messages that have a message ID between IZUG000-IZUG399.

IZUG011I *action* **z/OSMF** *procedure-name* **procedure on** *timestamp***.**

Explanation: The specified action was taken on the specified procedure. The timestamp indicates the time the action was taken on the procedure.

In the message text:

action The action being performed on the procedure. This can be the start or completion of the procedure.

procedure-name
Name of the procedure.

timestamp
The timestamp for the procedure being performed.

System programmer response: No action is required.

User response: No action is required.

IZUG012W **The user ID executing this procedure is** *actual-userid***. The expected user ID** *expected-userid* **should be used instead.**

Explanation: An unexpected user ID was found to be executing the procedure. The specified expected user ID should be used instead.

In the message text:

actual-userid
User ID executing the procedure.

expected-userid
The user id expected to be executing the procedure.

System programmer response: The expected user id should be used to execute the procedure.

User response: No action is required.

IZUG013E **The** *branch-country-name* **code must be** *branch-country-range* **alphanumeric characters (A-Z, 0-9).**

© Copyright IBM Corp. 2009, 2016

Explanation: The value specified for the branch or country code does not conform to guidelines.

In the message text:

branch-country-name
Name of the branch or country

branch-country-range
Range for the branch or country attribute.

System programmer response: Specify the correct value.

User response: No action is required.

IZUG014E **No roles match the value** *the-value* **specified with the -role option.**

Explanation: There were no matches found for the specified value.

In the message text:

the-value
No roles were found matching the specified value.

System programmer response: Ensure that the role file or alias exists and retry the operation.

User response: No action is required.

IZUG015I **The following aliases (and role files) can be specified when authorizing users.**

Explanation: Specifies that a list of role files will follow based on the request.

System programmer response: No action is required.

User response: No action is required.

IZUG016I **Specify** *the-alias* **or** *the-role-file* **to authorize the user id to this role.**

Explanation: The specified alias value is set in the specified role file.

In the message text:

the-alias The alias value in the role file.

the-role-file
The role file.

System programmer response: No action is required.

User response: No action is required.

IZUG017W **Unable to access file** *the-target-file***. The file** *the-default-file* **will be used.**

Explanation: The specified file is not accessible. The specified default file will be used.

In the message text:

the-target-file
The target file to be used.

the-default-file
The default file to be used.

System programmer response: Check the specified target file to ensure that the file is accessible and retry the operation.

User response: No action is required.

IZUG018W **The property** *the-property* **is set to** *the-value***. The value is incorrect. The default value of** *the-default* **will be used.**

Explanation: The specified timeout value is incorrect. The specified default value will be used.

In the message text:

the-property
The property that is set.

the-timeout
The value for the property.

the-default
The default value for the property.

System programmer response: No action is required.

User response: No action is required.

IZUG019I **The** *the-procedure* **timeout value is set to** *the-timeout***.**

Explanation: The specified timeout value will be used for the specified procedure.

In the message text:

the-procedure
The procedure being performed.

the-timeout
The timeout value for the procedure being performed.

System programmer response: No action is required.

User response: No action is required.

IZUG020W **The value** *prop-value* **was found for property** *prop-name1* **in file** *file-name1***. The role file** *file-name2* **will not be processed.**

Explanation: The indicated property was found in the specified file containing the indicated value. At least one valid group name or user id is required in order to process the specified file.

In the message text:

prop-value
The value of the property.

prop-name1
The name of the property.

file-name1
The name of the file.

file-name2
The name of the file.

System programmer response: Specify a valid group name or user id and retry the operation.

User response: No action is required.

IZUG021E The argument *the-argument* is required.

Explanation: The specified argument is required and must be supplied.

In the message text:

the-argument
The name of the required argument.

System programmer response: Retry the operation and provide the specified argument.

User response: No action is required.

IZUG022W Argument *the-argument* is ignored.

Explanation: The specified argument will be ignored.

In the message text:

the-argument
Name of the argument that will be ignored.

System programmer response: No action is required.

User response: No action is required.

IZUG023W An unexpected error has occurred while attempting to *the-procedure*.

Explanation: An error was encountered while attempting to run the specified procedure.

In the message text:

the-procedure
The procedure where the error occured.

System programmer response: Review the log file for additional information and retry the operation.

User response: No action is required.

IZUG024W Te value *prop-value* was found for properties *prop-name1* and *prop-name2* in file *file-name1*. The role file *file-name2* will not be processed.

Explanation: The indicated properties was found in the specified file containing the indicated value. At least one valid group name or user id is required in order to process the specified file.

In the message text:

prop-value
The value of the property.

prop-name1
The name of the property.

prop-name2
The name of the property.

file-name1
The name of the file.

file-name2
The name of the file.

System programmer response: Specify a valid group name or user id and retry the operation.

User response: No action is required.

IZUG025I The value *prop-value* for property *prop-name* was found in file *file-name*.

Explanation: The indicated property was found in the specified file containing the indicated value.

In the message text:

prop-value
The value of the property.

prop-name
The name of the property.

file-name
The name of the file.

System programmer response: No action is required.

User response: No action is required.

IZUG026I The *file-type* file *file-name* is being processed.

Explanation: The specified file of the specfied type is being processed.

In the message text:

file-type The type of file being processed.

file-name
The name of the file being processed.

System programmer response: No action is required.

User response: No action is required.

IZUG027E Multiple selection of plug-ins in *value* are not allowed.

Explanation: One or more duplicate entries were found in the value. The specified value is incorrect for the property.

In the message text:

value The value containing duplicate entries

System programmer response: Correct the error and retry. Ensure the value for the specified property is valid.

User response: No action is required.

IZUG028I **Completed** *procedure-name* **for** *plugin-name***.**

Explanation: The specified procedure has completed for the specified plug-in.

In the message text:

procedure-name
Name of the procedure.

plugin-name
Name of the plugin.

System programmer response: No action is required.

User response: No action is required.

IZUG029I **Starting** *procedure-name* **for** *plugin-name***.**

Explanation: The specified procedure is being processed for the specified plug-in.

In the message text:

procedure-name
Name of the procedure.

plugin-name
Name of the plugin.

System programmer response: No action is required.

User response: No action is required.

IZUG030E **Script** *script-name* **requires the following input options:** *input-options***.**

Explanation: The valid script options are displayed. For information about the script options, see *IBM z/OS Management Facility Configuration Guide*.

In the message text:

script-name
Name of the script

input-options
Options required by the script.

System programmer response: Correct the error and retry the operation.

User response: No action is required.

IZUG031I **The** *file-name* **file will be used from the following location:** *file-name-location*

Explanation: The specified file will be used from the specified location.

In the message text:

file-name
Name of the file.

file-name-location
Name of the file location.

System programmer response: No action is required.

User response: No action is required.

IZUG032W **The property** *var-name* **could not be found in** *file-name***. Defaulting value to:** *value-name*

Explanation: The specified variable could not be found in the specified file. The variable will default to the specified value. The value is obtained from the shipped default file.

In the message text:

var-name
Name of the variable.

file-name
Name of the file.

value-name
Value for the variable.

System programmer response: No action is required.

User response: No action is required.

IZUG033I **Examine each of the output execs and determine which exec is appropriate for your environment. Run one exec only. The output execs are:** *rexx-exec-name1*, *rexx-exec-name2*

Explanation: The z/OSMF configuration process creates sample security execs to assist your security administrator in creating security authorizations for z/OSMF. The execs are tailored, based on the selections you made when running the script izusetup.sh -config, or specified in your override file.

z/OSMF creates several execs to accommodate a number of possible configuration paths, however, your installation should run only one of the execs. Your choice of which exec to run depends on whether:

- You are creating a new z/OSMF configuration or migrating from an earlier release of z/OSMF.
- The configuration process detected a change in the authorization mode for your installation.
- One or more of your selected plug-ins require additional security authorizations on your z/OS system.

In the message text:

rexx-exec-name1
Name of the first generated RACF exec.

rexx-exec-name2
Name of the second generated RACF exec.

Have your security administrator review the execs, and run the exec that is appropriate for your environment. Most likely, one of the following descriptions fits your environment.

- The exec named *configfilename*.cfg.rexx is the appropriate choice for new or first-time z/OSMF configurations. This exec contains the superset of required RACF commands, tailored for the plug-in selections you specified when running the script izusetup.sh -config, or specified in your override file.
- The exec named *configfilename*.cfg.convertFromSAFtoREP.rexx is the appropriate choice if your installation is migrating from an earlier release of z/OSMF for the new configuration. This exec contains the subset of RACF commands that are needed to update an existing security setup to SAF based security.

z/OSMF creates the execs for any izusetup.sh invocation that updates your configuration file, even if you are just adding a plug-in to an existing configuration (izusetup.sh -add). If the plug-ins to be added require no additional security setup, the created execs are "empty" and need not be run. It is recommended that your security administrator review each of the output execs to determine whether they require changes and should be run for your installation.

System programmer response: Have your security administrator review the execs and determine which exec to run, based on the guidance information in this message. For more information about the security execs, see *IBM z/OS Management Facility Configuration Guide*.

User response: No action is required.

IZUG034I **The z/OSMF configuration process has created a set of sample security execs for your reference in directory** *directory-name***.**

Explanation: The z/OSMF configuration process creates sample security execs to assist your security administrator in creating security authorizations for z/OSMF. The execs are tailored, based on the selections you made when running the script izusetup.sh -config, or specified in your override file. The execs are stored in the indicated directory.

In the message text:

directory-name
Directory in which the generated sample security execs reside.

System programmer response: See the accompanying message for the names of the sample security execs.

User response: No action is required.

IZUG035W **The default value** *file-name* **will be used because a fully-qualified path name was not provided for the file.**

Explanation: A fully-qualified path name was not provided for the file. The default value specified in the property IZU_CONFIG_DIR will be used.

In the message text:

file-name
Name of the file.

System programmer response: No action is required.

User response: No action is required.

IZUG036W **The variable** *var-name* **could not be found in the configuration file** *file-name***. Defaulting value to:** *value-name*

Explanation: The specified variable could not be found in the specified configuration file. The variable will default to the specified value.

In the message text:

var-name
Name of the variable.

file-name
Name of the configuration file.

value-name
Value for the variable.

System programmer response: No action is required.

User response: No action is required.

IZUG037E **The value** *value* **in file** *file* **is incorrect for property** *property***.**

Explanation: The specified value is incorrect for the property.

In the message text:

value The value for the property

file File containing the value.

property
Property containing the value.

System programmer response: Correct the error and retry. Ensure the value for the specified property is valid.

User response: No action is required.

IZUG038E **The file** *file-name* **does not conform to the expected format:** *release-level***. Migrate the file to the correct format and retry the operation.**

Explanation: The file is not at the correct release level.

In the message text:

file-name
Name of the file.

release-level
Level of the release.

System programmer response: Migrate the file to the correct release level and retry the request.

User response: No action is required.

IZUG039I **The override file** *config-file* **has been migrated to the format:** *release-level***.**

Explanation: The specified configuration file has been migrated to the specified release level.

In the message text:

config-file
Name of the configuration file.

release-level
Level of the release.

System programmer response: No action is required.

User response: No action is required.

IZUG040W **The variable** *var-name* **could not be found in the override file** *file-name***. Defaulting value to:** *value-name*

Explanation: The specified variable could not be found in the specified override file. The variable will default to the specified value.

In the message text:

var-name
Name of the variable.

file-name
Name of the override file.

value-name
Value for the variable.

System programmer response: No action is required.

User response: No action is required.

IZUG041E **The variables specified in override file** *file-name* **could not be exported.**

Explanation: The variables included in the specified override file were not exported because an error occurred.

In the message text:

file-name
Name of the override file.

System programmer response: For more information, review the log file that was created for the error.

User response: No action is required.

IZUG042I **The override file** *file-name* **conforms to the expected format:** *release-level***. No migration will be performed.**

Explanation: No migration is needed since the specified override file is at the correct version level.

In the message text:

file-name
Name of the override file.

release-level
Level of the release.

System programmer response: No action is required.

User response: No action is required.

IZUG043E **Unable to update override file** *file-name***.**

Explanation: The specified override file could not be updated.

In the message text:

file-name
Name of the override file.

System programmer response: Ensure that the caller is authorized to update the override file. For more information, review the log file that was created for the error.

User response: No action is required.

IZUG044I **The input override file** *over-file* **was saved to a backup file** *back-up-override-file***.**

Explanation: The data of the source override file has been saved to the specified override file.

In the message text:

over-file Name of the override file.

back-up-override-file
Name of the backup override file.

System programmer response: No action is required.

User response: No action is required.

IZUG045E **Unable to back up override file data.**

Explanation: The data of the source override file could not be saved. Ensure that the permission settings are correct for the file and directory.

System programmer response: Ensure that the permission settings are correct for the file and directory.

User response: No action is required.

IZUG046I **Enter the existing** *group-name* **group name that is used to authorize users to the** *plug-in-name* **resources. Enter** *keyword-name* **if no group exists.**

Explanation: The message prompts for the plug-in group name. These group are expected to already exist. If a group does not exist or if the group has not yet been created enter the specified keyword. The RACF exec generated will have the required commands commented out. Once the group has been created, update and uncomment the commands in the RACF exec.

In the message text:

group-name
Name of the group

plug-in-name
Name of the plug-in

keyword-name
Name of the keyword

System programmer response: Enter the information or enter the specified keyword if no group exists.

User response: No action is required.

IZUG047I **Enter the existing** *group-name* **group name that is used to authorize users to the** *plug-in-name* **resources. Press Enter to accept the default** *default-value***, or enter** *keyword-name* **if no group exists.**

Explanation: The message prompts for the plug-in group name. These groups are expected to already exist. If a group does not exist or if the group has not yet been created enter the specified keyword. The RACF exec generated will have the required commands commented out. Once the group has been created, update and uncomment the commands in the RACF exec.

In the message text:

group-name
Name of the group

plug-in-name
Name of the plug-in

default-value
The default value

keyword-name
Name of the keyword

System programmer response: Enter the information, press Enter to accept the default, or enter the keyword if no group exists.

User response: No action is required.

IZUG048W **Group** *group-name* **does not exist.**

Explanation: The specified group does not exist.

In the message text:

group-name
Name of the group.

System programmer response: Ensure that the specified group exists. If not create it and retry.

User response: No action is required.

IZUG049I **z/OSMF configuration has detected a** *current-auth-mode* **to** *new-auth-mode* **authorization mode switch.**

Explanation: The current authorization mode will be changed to the new authorization mode specified.

In the message text:

current-auth-mode
The current authorization mode.

new-auth-mode
The new authorization mode.

System programmer response: No action is required.

User response: No action is required.

IZUG050I **z/OSMF configuration has detected a** *current-auth-mode* **to** *new-auth-mode* **authorization mode switch. The data file system** *file-system* **must be mounted.**

Explanation: The authorization mode switch indicated requires the data file system specified be mounted.

In the message text:

current-auth-mode
The current authorization mode.

new-auth-mode
The new authorization mode.

file-system
The data file system.

System programmer response: No action is required.

User response: No action is required.

IZUG051W **The permissions assigned to directory** *directory-name* **will be changed to** *permissions***.**

Explanation: The current assigned permissions for the specified directory will be changed to the new permissions specified.

In the message text:

directory-name
The directory being checked.

permissions
The new permissions that will be assigned to the specified directory.

System programmer response: No action is required.

User response: No action is required.

IZUG052W **The group assigned to directory** *directory-name* **will be changed to** *group-name***.**

Explanation: The current assigned group of the specified directory will be changed to the new group specified.

In the message text:

directory-name
The directory being checked.

group-name
The new group that will be assigned to the specified directory.

System programmer response: No action is required.

User response: No action is required.

IZUG053W **The owner assigned to directory** *directory-name* **will be changed to** *new-owner***.**

Explanation: The current owner of the specified directory will be changed to the new owner specified.

In the message text:

directory-name
Directory being checked.

new-owner
User id of the new owner to be assigned to the specified directory.

System programmer response: No action is required.

User response: No action is required.

IZUG054I **To obtain the results of the** *verification-type* **verification, review report** *report-name***.**

Explanation: Review the specified report file to obtain the results of the verification.

In the message text:

verification-type
The type of verification being performed.

report-name
Name of the verification report.

System programmer response: Review the specified report.

User response: No action is required.

IZUG055E **Group** *group-name* **not permitted to RACF class** *class-name***.**

Explanation: The specified group name is not permitted to the specified RACF class.

In the message text:

group-name
Name of the group being evailuated.

class-name
Name of the RACF class.

System programmer response: For more information, review the log file created for the error and the RACF report.

User response: No action is required.

IZUG056I **The file** *target-file* **was saved to a backup file** *back-up-file***.**

Explanation: The data of the source file has been saved to the specified file.

System programmer response: No action is required.

User response: No action is required.

IZUG057E **File** *file-name* **does not exist or is not accessible.**

Explanation: The specified file does not exist or is not accessible.

In the message text:

file-name
Name of the file.

System programmer response: Ensure that the specified file exists and is accessible. Retry your request.

User response: No action is required.

IZUG058E **File** *file-name* **is incomplete. The property** *configuration-property* **is missing.**

Explanation: This message indicates that the specified configuration property was not found. The script exits in error.

In the message text:

file-name
The configuration file.

configuration-property
The configuration property.

System programmer response: Ensure that the specified property exists in the specified configuration file.

User response: No action is required.

IZUG059I **Specify the CEA high level qualifier (HLQ) to use for log snapshot data sets. The HLQ can be 1-4 characters.**

Explanation: The message prompts for the high level qualifier to use.

System programmer response: Enter the high level qualifier value to use.

User response: No action is required.

IZUG060I **Specify the CEA high level qualifier (HLQ) to use for log snapshot data sets. The HLQ can be 1-4 characters. Or press Enter to accept the default** *default-HLQ-mode***:**

Explanation: The message prompts for the high level qualifier to use.

System programmer response: Enter the high level qualifier value to use or press Enter to use the specified default value.

User response: No action is required.

IZUG061I **What security mode do you want to use? To use SAF mode, enter S. To use Repository mode, enter R. Or press Enter to accept the current setting** *current-mode***:**

Explanation: The message prompts for the security mode to use.

In the message text:

current-mode
Current security mode for the z/OSMF configuration.

System programmer response: Enter S to use SAF security mode or R to use Repository mode or press Enter to use the current setting for security mode.

User response: No action is required.

IZUG062I **What security mode do you want to use? To use SAF mode, enter S. To use Repository mode, enter R:**

Explanation: The message prompts for the security mode to use.

System programmer response: Enter S to use SAF security mode or R to use Repository mode.

User response: No action is required.

IZUG063E **File** *file-name* **could not be found in** *dataset-name***. This file is required for the configuration of Common Event Adapter (CEA) for Incident Log.**

Explanation: The specified file does not exist in specified data set. This file is used by the Incident Log verification to verify the Inicdent Log configuration. As part of the configuration of CEA for Incident Log, this file is copied to the specified target dataset where it will be used to create a test dump for the verification of Incident Log.

In the message text:

file-name
File name.

dataset-name
Data set name.

System programmer response: Ensure that the specified file exists in the specified data set. Retry your request.

User response: No action is required.

IZUG064I **Enter the name of the target data set to be used for saving the updated** *member-name* **parmlib member. Specify the fully qualified data set name, or press Enter to accept the default:** *default-member-name***:**

Explanation: The message prompts you for the name of the data set to be used for saving the updated parmlib members, IEADMCnn and CEAPRMnn, which are used for Incident Log task processing. A fully qualified data set name is expected.

In the message text:

member-name
User-specified parmlib member

default-member-name
Default data set name.

System programmer response: Specify the fully qualified data set name, or press Enter to accept the supplied default if it is correct for your environment. If you specify the data set name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response: No action is required.

IZUG065I **Enter the name of the target data set to be used for saving the updated** *member-name* **parmlib member. Specify the fully qualified data set name, or press Enter to use SYS1.PARMLIB:**

Explanation: The message prompts you for the name of the data set to be used for saving the updated

parmlib members, IEADMCnn and CEAPRMnn, which are used for Incident Log task processing. A fully qualified data set name is expected.

In the message text:

member-name
User-specified PARMLIB member.

System programmer response: Specify the fully qualified data set name, or press Enter to save the updated member in SYS1.PARMLIB. If you specify the data set name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response: No action is required.

IZUG066I **Enter the name of the source data set for the IEADMCZM parmlib member. Specify the fully qualified data set name, or press Enter to accept the default** *data-set-name***:**

Explanation: The message prompts you for the name of the data set that contains the IEADMCZM parmlib member. This is shipped by default in SYS1.SAMPLIB. A fully qualified data set name is expected.

In the message text:

data-set-name
Default data set name.

System programmer response: Specify the fully qualified data set name, or press Enter to accept the supplied default if it is correct for your environment. If you specify the data set name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response: No action is required.

IZUG067I **Enter the name of the source data set for the IEADMCZM parmlib member. Specify the fully qualified data set name, or press Enter to use SYS1.SAMPLIB:**

Explanation: The message prompts you for the name of the data set that contains the IEADMCZM parmlib member. This is shipped by default in SYS1.SAMPLIB. A fully qualified data set name is expected.

System programmer response: Specify the fully qualified data set name, or press Enter to use SYS1.SAMPLIB as the source for the IEADMCZM member. If you specify the data set name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response: No action is required.

IZUG068W **The configuration property** *cfg-prop* **was found in file** *cfg-ovr-file***. This property will be ignored.**

Explanation: The indicated configuration property was found in either the configuration or override file. The indicated property will be ignored since the property can only be set by manually exporting it or through the use of the environment file specified by environment variable IZU_ENV_FILE.

In the message text:

cfg-prop Name of the property.

cfg-ovr-file
The configuration or override file.

System programmer response: If the intent was to set the specified property, either update the file specified by IZU_ENV_FILE with the property and then export IZU_ENV_FILE OR manually export the property prior to calling the script. Otherwise, no action is required.

User response: No action is required.

IZUG069I **The configuration property** *cfg-prop* **is set to the value** *cfg-val***.**

Explanation: The indicated configuration property is set to the indicated value.

In the message text:

cfg-prop Name of the property.

cfg-val Value of the property.

System programmer response: No action is required.

User response: No action is required.

IZUG070I **If you have AUTOGID enabled, RACF can assign unused GIDs for your group ids. Do you want RACF to automatically assign GIDs to groups created by z/OSMF? For yes, enter Y. For no, enter N:**

Explanation: RACF can automatically assign unused GIDs to your group ids if AUTOGID is enabled. If selected, all GID properties in the configuration file will be set to AUTOGID. This can also reduce the number of prompts for UIDs.

System programmer response: Enter Y to have RACF automatically assign unused GIDs for your z/OSMF created group ids or enter N to assign your own.

User response: No action is required.

IZUG071I **If you have AUTOGID enabled, RACF can assign unused GIDs for your group ids. Do you want RACF to automatically assign GIDs to groups created by z/OSMF? For yes, enter Y. For no, enter N. Or press Enter to accept the default** *default-value***:**

Explanation: RACF can automatically assign unused GIDs to your group ids if AUTOGID is enabled. If selected, all GID properties in the configuration file will be set to AUTOGID. This can also reduce the number of prompts for UIDs.

In the message text:

default-value
The default value to use.

System programmer response: Enter Y to have RACF automatically assign unused GIDs for your z/OSMF created group ids or enter N to assign your own.

User response: No action is required.

IZUG072I **If you have AUTOUID enabled, RACF can assign unused UIDs for your user ids. Do you want RACF to automatically assign UIDs to user ids created by z/OSMF? For yes, enter Y. For no, enter N:**

Explanation: RACF can automatically assign unused UIDs to your user ids if AUTOUID is enabled. If selected, all UID properties in the configuration file will be set to AUTOUID. This can also reduce the number of prompts for UIDs.

System programmer response: Enter Y to have RACF automatically assign unused UIDs for your z/OSMF created user ids or enter N to assign your own.

User response: No action is required.

IZUG073I **If you have AUTOUID enabled, RACF can assign unused UIDs for your user ids. Do you want RACF to automatically assign UIDs to user ids created by z/OSMF? For yes, enter Y. For no, enter N. Or press Enter to accept the default** *default-value***:**

Explanation: RACF can automatically assign unused UIDs to your user ids if AUTOUID is enabled. If selected, all UID properties in the configuration file will be set to AUTOUID. This can also reduce the number of prompts for UIDs.

In the message text:

default-value
The default value to use.

System programmer response: Enter Y to have RACF automatically assign unused UIDs for your z/OSMF created user ids or enter N to assign your own.

User response: No action is required.

IZUG074I **Clearing cached content for z/OSMF online help at location:** *help-dir***.**

Explanation: While processing your request, z/OSMF deployed or redeployed one or more plug-ins. This activity includes the deletion of the contents of the z/OSMF online help directory. This processing is normal.

In the message text:

help-dir Name of the directory to be processed.

System programmer response: No action is required.

User response: No action is required.

IZUG075I **Environment file** *env-file* **has been sourced.**

Explanation: The indicated environment file has been sourced.

In the message text:

env-file Name of the environment file.

System programmer response: No action is required.

User response: No action is required.

IZUG076E **An unexpected error occurred.**

Explanation: An error occurred, but the cause could not be determined.

System programmer response: Check the job log for any other messages that might indicate a reason for this error. If the log messages do not explain the cause of the problem, contact IBM Support for assistance.

User response: No action is required.

IZUG077E **The value specified for** *attribute* **is not valid. The value must start with an alpha character (A-Z, a-z) or a special character (# $ @) and must contain** *number* **characters.**

Explanation: The value specified for the variable is not valid.

In the message text:

attribute
Attribute for the prompt.

number Minimum and maximum number of characters the variable can contain.

System programmer response: Enter a value that starts with an alpha character (A-Z, a-z) or a special character (# $ @) and contains between the minimum and maximum number of characters specified.

User response: No action is required.

IZUG078E **File *file-name* does not exist. This file is required for the configuration of Common Event Adapter (CEA) for Incident Log.**

Explanation: The specified file does not exist. This file is required for the configuration of the Incident Log plug-in.

In the message text:

file-name
File name.

System programmer response: Ensure that the specified file exists. Retry your request.

User response: No action is required.

IZUG079E **File *file-name* could not be found in SYS1.SAMPLIB. This file is required for the configuration of Common Event Adapter (CEA) for Incident Log.**

Explanation: The specified file does not exist in SYS1.SAMPLIB. This file is used by the Incident Log verification to verify the Inicdent Log configuration. As part of the configuration of CEA for Incident Log, this file is copied to the specified target dataset where it will be used to create a test dump for the verification of Incident Log.

In the message text:

file-name
File name.

System programmer response: Ensure that the specified file exists in SYS1.SAMPLIB. Retry your request.

User response: No action is required.

IZUG080I **All of the available z/OSMF plug-ins have been configured already.**

Explanation: All of the plug-ins that were shipped with z/OSMF have been configured with the product already. No other plug-ins remain to be configured.

System programmer response: No action is required.

User response: No action is required.

IZUG081E **The plug-in -add request cannot be performed because the specified configuration file *file-name* was not found. This file is required for adding plug-ins.**

Explanation: The request to add one or more plug-ins could not be completed because the specified input configuration file was not found. This file is required for configuring plug-ins on your system.

In the message text:

file-name
Name of the configuration file.

System programmer response: Ensure that the specified configuration file exists. If not, recreate the configuration file with the values for your existing z/OSMF configuration. Retry your request.

User response: No action is required.

IZUG082E **File system *file-system-name* at mount point *file-system-mount-point* must be a ZFS or HFS file system and must be mounted in read-write mode.**

Explanation: The specified file system at the specified mount point must be of type ZFS or HFS and must be mounted in read-write mode. This can be done by specifying rdwr for the mode when mounting the filesystem.

In the message text:

file-system-name
Name of the file system.

file-system-mount-point
The mount point of the file system.

System programmer response: Ensure the file system is a ZFS or HFS. Also, ensure that the file system is mounted in read-write mode.

User response: No action is required.

IZUG083I **The verification of *verify-type* has completed successfully.**

Explanation: The verification request completed.

In the message text:

verify-type
Type of verification that was requested.

System programmer response: No action is required.

User response: No action is required.

IZUG084W **The IZU_DATA_DIR variable, which identifies the mount point of the z/OSMF data file system, has been reset to the default value *mount-point*.**

Explanation: The z/OSMF configuration process has updated the IZU_DATA_DIR variable in your configuration file to the default value of /var/zosmf/data. In the previous release of z/OSMF, the z/OSMF data file system was mounted at /var/zosmf by default.

In the message text:

mount-point
Default mount point for the z/OSMF data file system.

System programmer response: Determine whether the z/OSMF data file system on your system is currently mounted at the previous default location /var/zosmf. If so, unmount it. You can remount the data file system manually at the new location /var/zosmf/data or you can allow z/OSMF processing to mount it at this location during the processing of the izusetup.sh -config script.

User response: No action is required.

IZUG085I The IZU_IL_CONFIGURE variable must be set to Y before completing action *action***.**

Explanation: The IZU_IL_CONFIGURE variable in the configuration file must be set to Y before the specified action can be completed.

In the message text:

action The Incident Log action to be completed.

System programmer response: Enter the `izusetup.sh -config [ filename.cfg ]` command, specifying as input the configuration file that you used previously for setting up z/OSMF. If you omit this file name, the IBM-supplied configuration file (izudflt.cfg) is used. Then, when prompted to configure the Incident Log, enter `Y`.

User response: No action is required.

IZUG086E The Incident Log configuration request failed. The IZU_IL_CEA_CONFIGURE variable in the configuration file must be set to Y before the request can be processed.

Explanation: The Incident Log configuration request failed because the IZU_IL_CEA_CONFIGURE variable is not set to Y.

System programmer response: Enter the `izusetup.sh -config [ filename.cfg ]` command. The configuration file name is optional. If you omit this file name, the IBM-supplied configuration file (izudflt.cfg) is used. Then, when prompted to configure the Incident Log, enter `Y`.

User response: No action is required.

IZUG087I The IZU_IL_CEA_CONFIGURE variable must be set to Y before completing action *action***.**

Explanation: The IZU_IL_CEA_CONFIGURE environment variable in the configuration file must be set to Y before the specified action can be completed.

In the message text:

action The Incident Log action to be completed.

System programmer response: Enter the `izusetup.sh -config [ filename.cfg ]` command. Use the configuration file that you used previously for setting up z/OSMF. If you omit this file name, the IBM-supplied configuration file (izudflt.cfg) is used. Then, when prompted to configure the Incident Log, enter `Y`.

User response: No action is required.

IZUG088E The required environment variable *env-var* **is not set.**

Explanation: For script processing, z/OSMF requires that the indicated environment variable be set to a valid value. However, no value was found for the variable.

In the message text:

env-var Name of the variable that was not set.

System programmer response: A serious error has occured. Contact IBM Support.

User response: No action is required.

IZUG089E Directory *directory-name* **must be writable.**

Explanation: Processing of the script has stopped. For processing to continue, the indicated directory must be writable.

In the message text:

directory-name
Name of the directory.

System programmer response: Ensure that the user running the script has permission to write to the directory. After correcting the error, have the user run the script again.

User response: No action is required.

IZUG090I Environment variable *env-var* **has been set to the default value** *env-value***.**

Explanation: The indicated environment variable has been set to the specified default value.

In the message text:

env-var Name of the variable.

env-value
Value of the variable.

System programmer response: No action is required.

User response: No action is required.

IZUG091I **Environment variable *env-var* is set to the value *env-value*.**

Explanation: The indicated environment variable is set to the indicated value.

In the message text:

env-var Name of the variable.

env-value
Value of the variable.

System programmer response: No action is required.

User response: No action is required.

IZUG092E **Path /usr/lib was not found in LIBPATH variable in file *file-name*.**

Explanation: The path /usr/lib was not found in the LIBPATH variable in the specified file.

In the message text:

file-name
Name of the file that was processed.

System programmer response: Ensure that the path /usr/lib in LIBPATH environment variable is set in the specified file.

User response: No action is required.

IZUG093I **The directory *tmpdir-value* will be used for storing temporary files.**

Explanation: z/OSMF processing will use the indicated directory for storing temporary files.

In the message text:

tmpdir-value
Temporary directory value.

System programmer response: No action is required.

User response: No action is required.

IZUG094I **In the previous configuration of z/OSMF, you allowed z/OSMF to configure the Common Information Model (CIM) server. In the current release of z/OSMF, the CIM configuration procedure is modified.**

Explanation: The procedure for configuring the CIM server has been modified in the current release of z/OSMF.

System programmer response: No action is required.

User response: No action is required.

IZUG095I **The Common Information Model (CIM) server must be configured and started before proceeding with configuration.**

Explanation: After reviewing the RACF instructions for the CIM server, and running the exec, your installation must configure and start the CIM server before proceeding with the configuration of z/OSMF.

System programmer response: Review the contents of the RACF exec that was created by the z/OSMF configuration process and run the exec, if appropriate. Then, configure and start the CIM server. For information about configuring the CIM server, see *z/OS Common Information Model User's Guide*, SC33-7998, which is available on-line in the IBM z/OS Internet Library.

User response: No action is required.

IZUG096I **Do you need assistance in setting up security for the Common Information Model (CIM) server? To have z/OSMF create an exec with sample RACF commands, enter Y. Otherwise, enter N.**

Explanation: The z/OSMF configuration process includes the option of creating a REXX exec with sample RACF commands. Your security administrator can use these commands for authorizing z/OSMF users to the CIM server.

System programmer response: To allow z/OSMF to create this exec, enter Y in response to this prompt. Otherwise, enter N.

User response: No action is required.

IZUG097I **Do you need assistance in setting up security for the Common Information Model (CIM) server? To have z/OSMF create an exec with sample RACF commands, enter Y. For no, enter N. Press Enter to accept the default *value*:**

Explanation: The z/OSMF configuration process includes the option of creating a REXX exec with sample RACF commands. Your security administrator can use these commands for authorizing z/OSMF users to the CIM server.

In the message text:

value Default for whether to set up RACF security for the CIM server.

System programmer response: Enter Y or N, or accept the default value.

User response: No action is required.

IZUG098E Unable to remove file *file-name*.

Explanation: z/OSMF processing of the izusetup.sh -finish request was unable to remove the indicated file. Possibly, the file is marked read-only or has permissions that do not allow for write access.

In the message text:

file-name
File that could not be removed.

System programmer response: Ensure that the specified file exists. Ensure that the file and the file directory have permissions that allow for write access. Also, verify that the user ID for the request has update access to the file and its directory. Then, retry your request.

User response: No action is required.

IZUG099W File *file-name* does not exist.

Explanation: In processing a izusetup.sh -config request, z/OSMF did not find the indicated file. If the file is needed, z/OSMF processing will create it using IBM defaults.

In the message text:

file-name
File that does not exist.

System programmer response: No action is required.

User response: If you are running the izusetup.sh script in interactive mode, the script will prompt you for a number of installation-specific values needed for configuration. In response to each prompt, you must either press Enter to use the default value, or type your installation specific value. Ensure that these values are appropriate for your setup. If you are running the script in fastpath mode, check the override file to ensure that the appropriate values have been specified for your installation.

IZUG100E Unable to register provider *name*.

Explanation: The specified provider could not be registered. Typically, this error occurs when the user is not authorized to write to the Common Information Model (CIM) server repository or when the providers are missing.

In the message text:

name Name of the provider.

System programmer response: Verify that the user is authorized to write to the Common Information Model (CIM) server repository. Ensure that the providers are available.

User response: No action is required.

IZUG101W The file or parmlib member was not overwritten.

Explanation: The specified file or parmlib member was not overwritten.

System programmer response: No action is required.

User response: No action is required.

IZUG102E The request to start the Common Information Model (CIM) server failed because the server is already running.

Explanation: The Common Information Model (CIM) server could not be started because it is already running.

System programmer response: Shutdown the CIM server by entering the `cimserver -s` command. Then, re-run the script.

User response: No action is required.

IZUG104I Provider *name* module has already been registered with the Common Information Model (CIM) server.

Explanation: The specified provider module is already registered with the Common Information Model (CIM) server.

In the message text:

name Name of the provider.

System programmer response: No action is required.

User response: No action is required.

IZUG105W Provider *name* module is not registered with the Common Information Model (CIM) server.

Explanation: The specified provider module is not registered with the Common Information Model (CIM) server. The script will register it.

In the message text:

name Name of the provider.

System programmer response: No action is required.

User response: No action is required.

IZUG106I The provider *name* module is being registered with the Common Information Model (CIM) server.

Explanation: The provider module is not registered with the Common Information Model (CIM) server; therefore, the script is registering it.

In the message text:

name Name of the provider.

System programmer response: No action is required.

User response: No action is required.

IZUG107E **Unable to register provider** *name* **module.**

Explanation: The specified provider module could not be registered. Typically, this error occurs when the user is not authorized to write to the Common Information Model (CIM) server repository or when the providers are missing.

In the message text:

name Name of the provider.

System programmer response: Verify that the z/OSMF administrator is authorized to write to the Common Information Model (CIM) server repository. Ensure that the providers are available.

User response: No action is required.

IZUG108W **The temporary directory** *directory-name* **specified for environment variable TMPDIR does not exist or cannot be accessed. The directory /tmp will be used.**

Explanation: The specified temporary directory either could not be found or is not writable. Thus, the directory /tmp will be used.

In the message text:

directory-name
Name of the directory specified for the TMPDIR environment variable.

System programmer response: Verify that the directory exists. Ensure that the user running the script has permission to write to the directory.

User response: No action is required.

IZUG109E **Temporary directory** *directory-name* **must exist and be writable: exiting script.**

Explanation: For script processing, the named temporary directory must exist and be writable. If these requirements are not satisfied, processing of the script stops.

In the message text:

directory-name
Name of the temporary directory.

System programmer response: Verify that the directory exists. Ensure that the user running the script has permission to write to the directory. After correcting the error, run the script again.

User response: No action is required.

IZUG110I **The IZU_INCIDENT_LOG environment variable must be set to Y before completing action** *action***.**

Explanation: The IZU_INCIDENT_LOG environment variable in the configuration file must be set to Y before the specified action can be completed.

In the message text:

action The Incident Log action to be completed.

System programmer response: Enter the `izusetup.sh -config [ filename.cfg ]` command. Use the configuration file that you used for setup. If the file name is omitted, the default configuration file is used. When prompted to configure the Incident Log, enter `Y`.

User response: No action is required.

IZUG111E **The value specified for variable** *variable-name* **is not valid. The variable must start with an alphanumeric character (A-Z, a-z, and 0-9) or a special character (# $ @) and must contain** *number* **characters.**

Explanation: The value specified for the variable is not valid.

In the message text:

variable-name
Name of the input variable.

number Minimum and maximum number of characters the variable can contain.

System programmer response: Enter a value that starts with an alphanumeric character (A-Z, a-z, and 0-9) or a special character (# $ @) and contains between the minimum and maximum number of characters specified.

User response: No action is required.

IZUG112I **Script** *script-name* **returned with reason code** *code***.**

Explanation: The specified script returned with the specified reason code.

In the message text:

script-name
Name of the script.

code Reason code.

System programmer response: If the reason code is not 0, check the log for errors.

User response: No action is required.

IZUG113I The output of the command that was passed to script *script-name* is *output*.

Explanation: The output of the command that was passed to the specified script is displayed.

In the message text:

script-name
Name of the script.

output The output of the command.

System programmer response: No action is required.

User response: No action is required.

IZUG114I Command *command-name* was passed to script *script-name*.

Explanation: The specified command was passed to the specified script.

In the message text:

command-name
The command to execute.

script-name
Name of the script.

System programmer response: No action is required.

User response: No action is required.

IZUG115I The RACF REXX executable was generated and saved in file *file-name*. Review and execute the script before proceeding.

Explanation: The RACF REXX executable has been created and saved in the specified file. The script sets up the RACF security for z/OSMF.

In the message text:

file-name
Name of the file in which the RACF REXX executable is stored.

System programmer response: Review and execute the script. If you do not set up the security, you cannot proceed.

User response: No action is required.

IZUG116E User *user-name* does not exist.

Explanation: The specified user does not exist.

In the message text:

user-name
User ID of the user.

System programmer response: Provide a valid user name and try your request again.

User response: No action is required.

IZUG117I A *action* of the test incident for the Incident Log has occurred.

Explanation: To verify that the Incident Log is configured properly, a test incident is created. Then, a series of tests are run against the incident. After verification is complete, the test incident is deleted. This message indicates that the test incident is either being created or that it is being deleted.

In the message text:

action The action being performed as part of Incident Log verification.

System programmer response: No action is required.

User response: No action is required.

IZUG118I Checking Incident Log dependencies.

Explanation: The PDW_IVP is being called to determine the status of Incident Log dependencies on the system.

System programmer response: No action is required.

User response: No action is required.

IZUG119I Obtaining data for dependency *dependency-name*.

Explanation: Dependency data is being collected for either the SysplexDumpDirectory provider or PDWLogstream provider.

In the message text:

dependency-name
Name of the Incident Log dependency.

System programmer response: No action is required.

User response: No action is required.

IZUG120I Creating Incident Log report *report-name*.

Explanation: The specified Incident Log report is being created.

In the message text:

report-name
Name of the Incident Log report.

System programmer response: No action is required.

User response: No action is required.

IZUG121I To obtain the results of the Incident Log verification, review report *report-name*.

Explanation: Review the Incident Log report to obtain the results of the verification.

In the message text:

report-name
Name of the Incident Log report.

System programmer response: Review the specified report.

User response: No action is required.

IZUG122E Verification failed for *item-name***.**

Explanation: Verification failed because an error occurred while the specified item was being verified.

In the message text:

item-name
The item being verified.

System programmer response: For more information, review the log file created for the error.

User response: No action is required.

IZUG123E An error occurred. The Common Event Adapter (CEA) parmlib member was not activated.

Explanation: The CEA parmlib member was not activated because an error occurred.

System programmer response: For more information, review the log file created for the error.

User response: No action is required.

IZUG124I The Common Event Adapter (CEA) parmlib member *member-name* **is being activated.**

Explanation: The specified CEA parmlib member is being activated on the system.

In the message text:

member-name
Name of the CEA parmlib member.

System programmer response: No action is required.

User response: No action is required.

IZUG126E An error occurred. Variable *variable-name* **is set to value** *actual-value***. The expected value is** *expected value***.**

Explanation: The specified variable is set to the specified value. The variable must be set to the expected value.

In the message text:

variable-name
Name of the variable.

actual-value
Actual value specified for the variable.

expected value
Value to which z/OSMF expects the variable to be set.

System programmer response: For more information, review the log file created for the error and the RACF report.

User response: No action is required.

IZUG127E User *user-name* **not connected to group** *group-name***.**

Explanation: The specified user is not connected to the specified group.

In the message text:

user-name
User ID of the user.

group-name
Name of the group.

System programmer response: For more information, review the log file created for the error and the RACF report.

User response: No action is required.

IZUG128E User *user-name* **not permitted to RACF class** *class-name***.**

Explanation: The specified user or group name is not permitted to the specified RACF class.

In the message text:

user-name
User ID of the user.

class-name
Name of the RACF class.

System programmer response: For more information, review the log file created for the error and the RACF report.

User response: No action is required.

IZUG129E Unable to allocate the sysplex dump directory.

Explanation: The sysplex dump directory could not be allocated.

System programmer response: For more information, review the log file created for the error.

User response: No action is required.

IZUG130I Allocating sysplex dump directory on volume *volume-name***.**

Explanation: The sysplex dump directory is being allocated on the specified volume.

In the message text:

volume-name
Name of the volume.

System programmer response: No action is required.

User response: No action is required.

IZUG131I Activating sysplex dump directory.

Explanation: The sysplex dump directory is being activated.

System programmer response: No action is required.

User response: No action is required.

IZUG132E Unable to activate sysplex dump directory.

Explanation: The sysplex dump directory could not be activated.

System programmer response: For more information, review the log file created for the error.

User response: No action is required.

IZUG133I Enter the cluster transition name (case sensitive) for the server:

Explanation: Indicate the cluster transition name to be used. The name is case sensitive.

System programmer response: Enter the cluster transition name.

User response: No action is required.

IZUG134I Enter the cluster transition name (case sensitive) for the server, or press Enter to accept the default *cluster-name***:**

Explanation: Indicate the cluster transition name to be used.

In the message text:

cluster-name
The default cluster transition name.

System programmer response: To use the default cluster transition name, press Enter without entering a value. Otherwise, enter the name of the cluster transition.

User response: No action is required.

IZUG135W File *file-name* **already exists. Ensure that the environment variables specified in the file have the same value as the corresponding variables in the configuration file.**

Explanation: The specified file already exists.

In the message text:

file-name
Name of the file.

System programmer response: Ensure that the environment variables specified in the file have the same values as the corresponding variables in the configuration file. After you compare the variables and make any corrections, you can continue.

User response: No action is required.

IZUG136I The *item-type file-name* **was created.**

Explanation: The specified file or directory has been created.

In the message text:

item-type
Type of item being created: file or directory.

file-name
Name of the file or directory.

System programmer response: No action is required.

User response: No action is required.

IZUG137E File *file-name* **already exists. The value specified in the file for the PEGASUS_HOME environment variable does not match the value specified in the configuration file for the IZU_WBEM_ROOT variable.**

Explanation: The specified file already exists. An error occurred because the PEGASUS_HOME variable specified in the file does not have the same value as the IZU_WBEM_ROOT variable specified in the configuration file. The values for these two variables must be the same.

In the message text:

file-name
Name of the file.

System programmer response: Update the specified file so that the PEGASUS_HOME variable has the same value as the IZU_WBEM_ROOT variable in the configuration file.

User response: No action is required.

IZUG138E Unable to read file *file-name***.**

Explanation: The permissions specified for the file does not allow read access.

In the message text:

file-name
Name of the file.

System programmer response: Enable read access for the file.

User response: No action is required.

IZUG139I Has the Common Information Model (CIM) server been setup? [Y|N]:

Explanation: The message prompts to determine if the Common Information Model (CIM) server has been set up.

System programmer response: Enter Y or N.

User response: No action is required.

IZUG140I Has the Common Information Model (CIM) server been setup? [Y/N]. Or press Enter to accept the default *value*:

Explanation: The message prompts to determine if the Common Information Model (CIM) server has been setup. A default value is provided.

In the message text:

value The default response value for the CIM setup option.

System programmer response: Enter Y or N, or accept the default. Default is NO

User response: No action is required.

IZUG141W No data directory specified. Using *directory-name* as the data directory.

Explanation: The message indicates that no data directory was specified and that the default data directory will be used.

In the message text:

directory-name
The default data directory.

System programmer response: Ensure the default data directory use is correct to the configuration.

User response: No action is required.

IZUG142I Enter the name of the target data set to be used for saving the updated parmlib members *ceaprm-parmlib-member* and *ieadmc-parmlib-member*. Specify the fully qualified data set name, or press Enter to accept the default: *parmlib-name*:

Explanation: The message prompts you for the name of the data set to be used for saving the updated parmlib members, IEADMCnn and CEAPRMnn, which are used for Incident Log task processing. A fully qualified data set name is expected.

In the message text:

ceaprm-parmlib-member
User-specified CEAPRMxx member

ieadmc-parmlib-member
The user-specified IEADMCxx member

parmlib-name
Default data set name.

System programmer response: Specify the fully qualified data set name, or press Enter to accept the supplied default if it is correct for your environment. If you specify the data set name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response: No action is required.

IZUG143I Enter the name of the target data set to be used for saving the updated parmlib members *ceaprm-parmlib-member* and *ieadmc-parmlib-member*. Specify the fully qualified data set name, or press Enter to use SYS1.PARMLIB:

Explanation: The message prompts you for the name of the data set to be used for saving the updated parmlib members, IEADMCnn and CEAPRMnn, which are used for Incident Log task processing. A fully qualified data set name is expected.

In the message text:

ceaprm-parmlib-member
User-specified CEAPRMxx member.

ieadmc-parmlib-member
User-specified IEADMCxx member.

System programmer response: Specify the fully qualified data set name, or press Enter to save the updated members in SYS1.PARMLIB. If you specify the data set name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response: No action is required.

IZUG144I Enter the mount point for the z/OSMF data file system:

Explanation: The message prompts for the mount point for where the z/OSMF data file system is to be mounted.

System programmer response: Enter the mount point for where the z/OSMF data file system is to be mounted.

User response: No action is required.

IZUG145I Enter the mount point for the z/OSMF data file system, or press Enter to accept the default *mount-point*:

Explanation: The message prompts for the mount point for where the z/OSMF data file system is to be mounted.

In the message text:

mount-point
The default mount point for the z/OSMF data file system.

System programmer response: Enter the mount point for where the z/OSMF data file system is to be mounted.

User response: No action is required.

IZUG146I Invoking script *script-name-options*.

Explanation: The message displays the script name and options that are being invoked.

In the message text:

script-name-options
The script name and options that are being invoked.

System programmer response: No action is required.

User response: No action is required.

IZUG147W Path /usr/lib not found in LIBPATH variable.

Explanation: The message indicates the path /usr/lib was not found in the LIBPATH environment variable.

System programmer response: Set the path /usr/lib in LIBPATH environment variable.

User response: No action is required.

IZUG148I Stopping Common Information Model (CIM) server.

Explanation: The message indicates that the CIM server is being stopped.

System programmer response: No action is required.

User response: No action is required.

IZUG149W Path /usr/lib not found in LIBPATH variable in file *file-name*.

Explanation: The message indicates the path /usr/lib was not found in the LIBPATH variable in the specified file.

In the message text:

file-name
The name of the file being checked.

System programmer response: Ensure the path /usr/lib in LIBPATH environment variable is set in the specified file.

User response: No action is required.

IZUG150E Mount point *mount-point* must be a fully-qualified path name.

Explanation: The message indicates the mount point provided is not a fully-qualified path.

In the message text:

mount-point
The mount point for the file system.

System programmer response: Provide a fully-qualified path.

User response: No action is required.

IZUG151I z/OSMF data file system will be created using SMS managed storage.

Explanation: This message confirms your selection to use the z/OS storage management subsystem (SMS) to manage the storage of the z/OSMF data file system.

System programmer response: No action is required.

User response: No action is required.

IZUG157I Enter the z/OSMF data file system type for the file system: *file-system-name*, or press Enter to accept the default *file-system-type*:

Explanation: This message prompts for the type (zfs or hfs) of the specified file system. A default value is provided.

In the message text:

file-system-name
Name of the file system

file-system-type
Default file system type.

System programmer response: No action is required.

User response: No action is required.

IZUG158I Enter the name of the volume to use for creating the z/OSMF data file system, enter an asterisk (*) to use SMS managed storage, or press Enter to accept the default *volume-name*:

Explanation: The message prompts you for the name of the volume to create the z/OSMF data file system. To have the z/OS storage management subsystem (SMS) manage the storage, enter an asterisk (*). A default value is provided.

In the message text:

volume-name
Default volume name.

System programmer response: Perform the requested action. If you specify a volume, the volume must be

on-line. If you specify SMS managed storage, ensure that you have an automatic class selection (ACS) routine in place to assign the appropriate SMS construct, based on the name of the data set to be used for the z/OSMF file system.

User response: No action is required.

IZUG159I **Enter the size (in cylinders) to allocate for the data file system, or press Enter to accept the default** *file-system-size***:**

Explanation: Enter the initial space allocation, in cylinders, for the z/OSMF data file system. z/OSMF uses 90 percent of this value for the primary allocation and 10 percent for the secondary allocation. The minimum suggested size is 100 cylinders, which causes the script to use 90 cylinders for the primary allocation and 10 cylinders for the secondary allocation. A default value is provided.

In the message text:

file-system-size
Default size for the file system.

System programmer response: Perform the requested action.

User response: No action is required.

IZUG160E **The file extension specified for the override file is incorrect. The file must have a .ovr extension.**

Explanation: An error occurred because the specified override file does not have a .ovr extension.

System programmer response: Modify the override file name so that it has the .ovr extension.

User response: No action is required.

IZUG161E **Directory** *directory-name* **must be a fully-qualified path name.**

Explanation: The message indicates that the directory provided is not a fully-qualified path.

In the message text:

directory-name
Name of the directory.

System programmer response: Provide a fully-qualified path.

User response: No action is required.

IZUG162I **Select the plug-ins to be configured. Multiple plug-ins can be selected by separating plug-ins with a comma.**

Explanation: The message indicates that multiple plug-ins may be selected by separating plug-in ids with a comma.

System programmer response: No action is required.

User response: No action is required.

IZUG163I **Select** *plug-in-id* **to configure** *plug-in-name***.**

Explanation: The message indicates the plug-in ID and plug-in name for selection.

In the message text:

plug-in-id
Identifier of the plug-in

plug-in-name
Name of the plug-in.

System programmer response: No action is required.

User response: No action is required.

IZUG164I **Which plug-ins do you want to configure?**

Explanation: Enter the plug-in IDs for selection. For multiple selections, separate plug-in IDs with a comma.

System programmer response: Select the plug-in ids for configuration.

User response: No action is required.

IZUG165I **You have selected to configure** *plug-in-name***.**

Explanation: The message indicates the specified plug-in was selected for configuration.

In the message text:

plug-in-name
Name of the plug-in.

System programmer response: No action is required.

User response: No action is required.

IZUG166I **No configuration prompts are required for the plug-in** *plug-in-name***.**

Explanation: The message indicates there are no prompts to be displayed for the selected plug-in.

In the message text:

plug-in-name
Name of the plug-in.

System programmer response: No action is required.

User response: No action is required.

IZUG167E **Value *plug-in-id* is ignored. Plug-in was already selected.**

Explanation: The plug-in ID is ignored because the plug-in has already been selected for configuration.

In the message text:

plug-in-id
Plug-in ID.

System programmer response: No action is required.

User response: No action is required.

IZUG168E **Expecting *number* arguments.**

Explanation: The message indicates the value that represents the number of plug-ins is incorrect.

In the message text:

number Number of plug-ins.

System programmer response: No action is required.

User response: No action is required.

IZUG169E **Configuration file variable *variable-name* is not valid.**

Explanation: The message indicates the configuration file variable is not valid.

In the message text:

variable-name
The configuration file variable.

System programmer response: No action is required.

User response: No action is required.

IZUG170E **Log file variable *variable-name* is not valid.**

Explanation: The message indicates the log file is not valid.

In the message text:

variable-name
Log file variable.

System programmer response: No action is required.

User response: No action is required.

IZUG171I **Do you want to configure the Common Information Model (CIM) server as part of z/OSMF customization? If so, enter Y. To skip this step, enter N:**

Explanation: Specify whether the z/OS Common Information Model (CIM) server is to be configured as part of the z/OSMF configuration process. z/OSMF requires that the CIM server be operational on your system. To have z/OSMF configure the CIM server for you, enter Y. Otherwise, if you have already configured the CIM server or plan to do this step yourself, specify N.

System programmer response: Enter Y or N.

User response: No action is required.

IZUG172I **Do you want to configure the Common Information Model (CIM) server as part of z/OSMF customization? If so, enter Y. To skip this step, enter N. To accept the default, press Enter: *value*:**

Explanation: Specify whether the z/OS Common Information Model (CIM) server is to be configured as part of the z/OSMF configuration process. z/OSMF requires that the CIM server be operational on your system. To have z/OSMF configure the CIM server for you, enter Y. Otherwise, if you have already configured the CIM server or plan to do this step manually, specify N. To accept the default value displayed in the message, press Enter.

In the message text:

value Default selection for setting up the CIM server.

System programmer response: Enter Y or N, or accept the default value.

User response: No action is required.

IZUG173I **Enter "N" to select none of these plug-ins.**

Explanation: The value N indicates that no plug-ins are selected.

System programmer response: No action is required.

User response: No action is required.

IZUG174E **The value *value* is incorrect for *property*.**

Explanation: The specified value is incorrect for the indicated property. During the configuration process, the izusetup.sh script collects installation-specific data that is used in the configuration of the product. The script starts with the variable settings that are contained in the configuration file (izudflt.cfg), and substitutes any installation-specific changes that you supply (through interactive prompting or an optional override file) to tailor the configuration for your environment.

In the message text:

value Value that was specified for the property

property
Property containing the value.

System programmer response: Specify a valid value for the indicated property and retry the operation. Depending on how you choose to configure z/OSMF,

you might need to respecify this value interactively or as a setting in the optional override file. Some values are case sensitive. For more information, see *IBM z/OS Management Facility Configuration Guide*. Do not edit the izudflt.cfg file directly.

User response: No action is required.

IZUG175I **The configuration file** *config-file* **will be migrated to the format:** *release-level***. Enter the** *release-level* **z/OSMF product file system mount point, or press Enter to accept the default path** *default-code-root***:**

Explanation: The specified configuration file will be migrated to the specified release level. This message prompts for the default code root directory.

System programmer response: Enter the root code directory path or press Enter to accept the default.

User response: No action is required.

IZUG176I **The configuration file** *config-file* **conforms to the expected format:** *release-level***. No migration will be performed.**

Explanation: No migration is needed since the specified configuration file is at the correct version level.

System programmer response: No action is required.

User response: No action is required.

IZUG177I **The configuration file** *config-file* **has been migrated to the format:** *release-level***.**

Explanation: The specified configuration file has been migrated to the specified release level.

System programmer response: No action is required.

User response: No action is required.

IZUG178I **The input configuration file** *config-file* **was saved to a backup file** *back-up-config-file***.**

Explanation: The data of the source configuration file has been saved to the specified configuration file.

System programmer response: No action is required.

User response: No action is required.

IZUG179E **Unable to back up configuration data.**

Explanation: The data of the source configuration file could not be saved. Ensure that the permission settings are correct for the file and directory.

System programmer response: Ensure that the permission settings are correct for the file and directory.

User response: No action is required.

IZUG180E **The configuration file** *config-file* **does not conform to the expected format:** *release-level***. Migrate the configuration file to the correct format and retry the operation.**

Explanation: The configuration file is not at the correct release level.

System programmer response: Migrate the configuration file to the correct release level and retry the request.

User response: No action is required.

IZUG181E **The value for the property** *plugin-property* **is set inconsistently in the configuration file and the override file. In the configuration file,** *plugin-property* **is set to** *plugin-property-value***. In the override file,** *plugin-property* **is set to** *plugin-property-value***.**

Explanation: In processing a izusetup.sh -add request, z/OSMF detected that the indicated property is specified inconsistently in the configuration file and the override file.

In the message text:

plugin-property
: The property name

plugin-property
: The property for the plug-in.

plugin-property-value
: The value for the property for the plug-in.

plugin-property
: The property for the plug-in.

plugin-property-value
: The value for the property for the plug-in.

System programmer response: Update the property with the correct value in the configuration file and in the override file. Then, retry the request.

User response: No action is required.

IZUG182I **The property** *plugin-property* **is set inconsistently in the configuration file and the override file. The property** *plugin-property* **will be set to** *plugin-property-value***.**

Explanation: In processing a izusetup.sh -add request, z/OSMF detected that the indicated property is specified inconsistently in the configuration file and the override file. Z/OSMF processing will set the property as indicated in the resulting configuration file.

In the message text:

plugin-property
Property for the plug-in

plugin-property
Property for the plug-in

plugin-property-value
The value for the property for the plug-in.

System programmer response: No action is required.

User response:

IZUG183I **The property** *plugin-property* **in the override file contains the value** *plugin-property-value***. The value for the property** *plugin-property* **will be set to** *plugin-property-value***.**

Explanation: The indicated property was set incorrectly in the override file. z/OSMF processing uses a reset value as indicated and ignores the value specified in the override file.

In the message text:

plugin-property
Property for the plug-in

plugin-property-value
Value of the property

plugin-property
The property for the plug-in

plugin-property-value
The new value for the property

System programmer response: No action is required.

User response: No action is required.

IZUG184E **The property** *plugin-property* **in the specified configuration file is set to an incorrect value** *plugin-property-value***.**

Explanation: In processing the izusetup.sh -add request, z/OSMF processing detected that the indicated variable was set incorrectly in the specified configuration file.

In the message text:

plugin-property
Property for the plug-in

plugin-property-value
Value that is incorrect

System programmer response: Check the override file for errors. Some variables are initially set to the following value, which is not a valid setting: NO.DEFAULT.VALUE. Correct the errors and try the request again.

User response: No action is required.

IZUG185I **Enter the value for the Common Information Model (CIM) server attribute** *server-attribute***, or press Enter to accept the default** *server-attribute-value***:**

Explanation: The message prompts for CIM server attribute values.

System programmer response: Provide the value for the server attribute.

User response: No action is required.

IZUG186I **You have selected to add the following plug-ins.**

Explanation: This message precedes the list of one or more plug-ins that have been selected for configuration.

System programmer response: No action is required.

User response: No action is required.

IZUG187I **Plug-in:** *plug-in-name***.**

Explanation: The specified plug-in has been selected for configuration.

In the message text:

plug-in-name
Name of the plug-in to be added.

System programmer response: No action is required.

User response: No action is required.

IZUG188I **To accept these plug-in selections, press Enter. To edit these selections, enter E.**

Explanation: The message prompts you to confirm your selection of which plug-ins are to be configured. You can change your selection.

System programmer response: Enter E to modify the selection. Press enter with no value to accept the current selection.

User response: No action is required.

IZUG189I **No plug-ins were selected for configuration.**

Explanation: The izusetup.sh -add request identified no plug-ins to be added to the z/OSMF configuration.

System programmer response: No action is required.

User response: No action is required.

IZUG190I **The plug-in** *plug-in-name* **is set to the value** *plug-in-value***, this indicates that it is already configured. The request to add this plug-in is ignored.**

Explanation: The plug-in is already configured. Your request is ignored.

In the message text:

plug-in-name
Name of the plug-in

plug-in-value
Value of the plug-in

System programmer response: No action is required.

User response: No action is required.

IZUG191I **No security setup procedure is required for the specified plug-ins.**

Explanation: The RACF setup procedure is not required for the specified plug-ins.

System programmer response: No action is required.

User response: No action is required.

IZUG192I **Enter the Common Information Model (CIM) Server attribute** *server-attribute***:**

Explanation: You requested that z/OSMF set this CIM server attribute, but no value was supplied for the attribute in the configuration file or override file. Therefore, the script prompts you for the value.

System programmer response: Enter the appropriate value for your installation.

User response: No action is required.

IZUG193E **Group** *group-name* **does not exist.**

Explanation: In processing the izusetup.sh -verify racf request, z/OSMF detected that the specified group is not defined.

In the message text:

group-name
Name of the group.

System programmer response: For more information, check the log file created for the error and the RACF report. Also, examine the generated RACF exec to ensure that the indicated group was created.

User response: No action is required.

IZUG194E **The value for variable** *property-name* **contains an incorrect character** *char-value***.**

Explanation: The specified value is incorrect because it contains an incorrect character.

In the message text:

property-name
The incorrect property.

char-value
The incorrect character within the input value.

System programmer response: Correct the value.

User response: No action is required.

IZUG195E **The value for variable** *property-name* **contains one or more spaces. Enter the value without spaces.**

Explanation: The value specified for the variable is not valid because it contains one or more spaces, which is not allowed.

In the message text:

property-name
Name of the incorrect property.

System programmer response: Specify a value that does not contain spaces.

User response: No action is required.

IZUG196E **The variable** *property-name* **contains an incorrect value** *property-value***.**

Explanation: The specified value is incorrect.

In the message text:

property-name
Name of the property.

property-value
Value of the property.

System programmer response: Correct the value.

User response: No action is required.

IZUG197E **The file system name** *file-system-name* **is incorrect. The maximum allowable length is 44 characters.**

Explanation: The specified value is incorrect.

In the message text:

file-system-name
The incorrect value.

System programmer response: Correct the value.

User response: No action is required.

IZUG198E **Parmlib data set** *parmlib-name* **does not exist.**

Explanation: The specified parmlib data set does not exist.

In the message text:

parmlib-name
Parmlib name.

System programmer response: Ensure that the

specified parmlib exists. Retry your request.

User response: No action is required.

IZUG199W File *file-name* already exists.

Explanation: The specified file already exists. Later during the configuration of CEAPRM parmlib member you will be given the option to overwrite the file.

In the message text:

file-name
File name.

System programmer response: No action is required.

User response: No action is required.

IZUG200E z/OSMF *process-name* process failed with return code *return-code*.

Explanation: The specified z/OSMF process failed with the specified return code.

In the message text:

process-name
Name of the z/OSMF process

return-code
Return code indicating the result of the process.

System programmer response: For more information, review the log file created for the error.

User response: No action is required.

IZUG201E User *user-id* could not be primed for z/OSMF. The action failed with return code *return-code*.

Explanation: The -prime request failed for the specified user ID. A return code is provided to indicate the cause of the error.

In the message text:

user-id User ID that could not be processed by the -prime request

return-code
Return code indicating the result of the process.

The following return codes are valid:

1 Usage error.

2 Problem with the log directory.

3 Error writing to the log file.

4 Script encountered an error when running a z/OS UNIX shell command, such as mkdir or cp.

5 A repository already exists.

6 Specified user ID is not defined to the z/OS system.

7 The data directory specified by IZU_DATA_DIR does not exist or is not accessible.

This message is accompanied by one or more related messages with more information about the error.

System programmer response: For more information, check for related messages. For return code 6, see the z/OSMF log file. After correcting the error, run the script again.

User response: No action is required.

IZUG202E z/OSMF could not make user *user-name* owner of *directory-file name*.

Explanation: z/OSMF could not make the specified user owner of the specified file or directory.

In the message text:

user-name
User name

directory-file
Indication of directory or file

name Name of the directory or file.

System programmer response: Ensure that the caller has permission to set ownership. For more information, review the log file created for the error.

User response: No action is required.

IZUG203E The request to set permissions for the files in directory *directory-name* failed.

Explanation: z/OSMF could not set permissions for the files in the specified directory.

In the message text:

directory-name
Name of the directory.

System programmer response: Ensure that the caller has permission to set ownership. For more information, review the log file created for the error.

User response: No action is required.

IZUG204E The request to set permissions for file *file-name* failed.

Explanation: z/OSMF could not set permissions for the specified file.

In the message text:

file-name
File name.

System programmer response: Ensure that the caller

has permission to set ownership. For more information, review the log file created for the error.

User response: No action is required.

IZUG205E **The file extension specified for the configuration file is incorrect. The file must have a .cfg extension.**

Explanation: An error occurred because the specified configuration file does not have a .cfg extension.

System programmer response: Modify the configuration file name so that it has the .cfg extension.

User response: No action is required.

IZUG206E **The variables specified in configuration file** *file-name* **could not be exported.**

Explanation: The variables included in the specified configuration file were not exported because an error occurred.

In the message text:

file-name
Name of the configuration file.

System programmer response: For more information, review the log file created for the error.

User response: No action is required.

IZUG207E **File** *file-name* **does not exist.**

Explanation: The specified file does not exist.

In the message text:

file-name
File name.

System programmer response: Ensure that the specified file exists. Retry your request.

User response: No action is required.

IZUG208E **The configuration file is incomplete. The value for variable** *variable-name* **is missing.**

Explanation: The request could not be completed because an error occurred. The configuration file is missing the specified information.

In the message text:

variable-name
Name of the variable that is missing from the configuration file.

System programmer response: Enter the `izusetup.sh -config [ filename.cfg ]` command. *filename.cfg* is the name of the configuration file that is missing the specified data. When prompted, provide a value for the specified variable.

User response: No action is required.

IZUG209I **Script** *script-name* **supports one or more of the following input options:** *input-options***.**

Explanation: The valid script options are displayed. For information about the script options, see *IBM z/OS Management Facility Configuration Guide*.

In the message text:

script-name
Name of the script

input-options
Options supported by the script.

System programmer response: No action is required.

User response: No action is required.

IZUG210I **The script** *script-name* **has completed.**

Explanation: The specified script completed.

In the message text:

script-name
Name of the script.

System programmer response: No action is required.

User response: No action is required.

IZUG211E **Script** *script-name* **encountered errors: exiting script.**

Explanation: Processing of the script stopped because one or more errors occurred.

In the message text:

script-name
Name of the script.

System programmer response: For more information, review the log file created for the error. Correct any errors and re-run the script.

User response: No action is required.

IZUG212E **Directory** *directory-name* **does not exist or is not accessible.**

Explanation: The specified directory does not exist or is not accessible.

In the message text:

directory-name
Name of the directory.

System programmer response: Ensure that the specified directory exists and is accessible. Retry your request.

User response: No action is required.

IZUG213I **Log information will be written to file** *file-name***.**

Explanation: Log information will be saved to the specified file.

In the message text:

file-name
Name of the file.

System programmer response: No action is required.

User response: No action is required.

IZUG214E **Failed to create** *directory-file directory-file-name***.**

Explanation: The specified file or directory could not be created.

In the message text:

directory-file
Directory or file

directory-file-name
Name of the directory or file.

System programmer response: Ensure that the caller is authorized to create files or directories. For more information, review the log file created for the error.

User response: No action is required.

IZUG215I **Starting z/OSMF** *procedure-name* **procedure.**

Explanation: The specified procedure is being processed.

In the message text:

procedure-name
Name of the procedure.

System programmer response: No action is required.

User response: No action is required.

IZUG216E **The command is missing one of the required arguments:** *argument-name***.**

Explanation: The command could not be completed because the specified argument was not found.

In the message text:

argument-name
Name of the argument.

System programmer response: Re-enter the command and include the missing argument.

User response: No action is required.

IZUG217E **The command could not be completed because it contains an incorrect argument.**

Explanation: An incorrect argument was provided with the command. Typically, this error occurs when an argument that is not supported by the command is used or when the argument is misspelled.

System programmer response: Verify that the correct argument is being used. Ensure that it is spelled correctly. Correct any errors and re-enter the command.

User response: No action is required.

IZUG218E **The command could not be completed because it contains an incorrect argument** *argument-name***.**

Explanation: An incorrect argument was provided with the command. The name of the incorrect argument is provided. Typically, this error occurs when an argument that is not supported by the command is used or when the argument is misspelled.

In the message text:

argument-name
Name of the incorrect argument.

System programmer response: Verify that the correct argument is being used. Ensure that it is spelled correctly. Correct any errors and enter the command again.

User response: No action is required.

IZUG220E **The Incident Log configuration request failed. The IZU_INCIDENT_LOG variable in the configuration file must be set to Y before the request can be processed.**

Explanation: The Incident Log configuration request failed because the IZU_INCIDENT_LOG variable is not set to Y.

System programmer response: Enter the `izusetup.sh -config [ filename.cfg ]` command. The configuration file name is optional. If the file name is omitted, the default configuration file is used. When prompted to configure the Incident Log, enter `Y`.

User response: No action is required.

IZUG221E **A value must be provided for argument** *argument-name***.**

Explanation: An error occurred because no value was found for the specified argument.

In the message text:

argument-name
Name of the required argument.

System programmer response: Correct the input to the request.

User response: No action is required.

IZUG222E Unable to update configuration file *file-name***.**

Explanation: The specified configuration file could not be updated.

In the message text:

file-name
Name of the configuration file.

System programmer response: Ensure that the caller is authorized to update the configuration file. For more information, review the log file created for the error.

User response: No action is required.

IZUG223I For more information, review log file *file-name***.**

Explanation: For more information, review the log file created for the error.

In the message text:

file-name
Name of the log file.

System programmer response: No action is required.

User response: No action is required.

IZUG224I The configuration data was saved in file *file-name***.**

Explanation: The configuration data was saved in the specified file.

In the message text:

file-name
Name of the configuration file.

System programmer response: No action is required.

User response: No action is required.

IZUG225E Unable to mount file system *file-system-name***.**

Explanation: The specified file system could not be mounted.

In the message text:

file-system-name
Name of the file system.

System programmer response: For more information, review the log file created for the error.

User response: No action is required.

IZUG226E Unable to allocate file system *file-system-name***.**

Explanation: The specified file system could not be allocated.

In the message text:

file-system-name
Name of the file system.

System programmer response: For more information, review the log file created for the error.

User response: No action is required.

IZUG227I Creating *directory-file directory-file-name***.**

Explanation: The specified file or directory is being created.

In the message text:

directory-file
Directory or file

directory-file-name
Name of the directory or file.

System programmer response: No action is required.

User response: No action is required.

IZUG228I Enter the fully qualified name of the z/OSMF *file-system-type* **file system:**

Explanation: The message prompts you for the name to be used for the z/OSMF data file system. A fully qualified name is expected.

In the message text:

file-system-type
File system type.

System programmer response: Specify the fully qualified name of the z/OSMF data file system. If you specify the file system name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response: No action is required.

IZUG229I Enter the fully qualified name of the z/OSMF *file-system-type* **file system, or press Enter to accept the default** *value* **file system name :**

Explanation: The message prompts you for the name to be used for the z/OSMF data file system. A fully qualified name is expected.

In the message text:

file-system-type
File system type.

value Default file system name.

System programmer response: Specify the fully qualified name of the z/OSMF data file system, or press Enter to accept the supplied default if it is correct for your environment. If you specify the file system name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response: No action is required.

IZUG230E **The value *value* is incorrect.**

Explanation: The specified value is incorrect.

In the message text:

value Name of the input field.

System programmer response: Correct the value.

User response: No action is required.

IZUG231W **A file system with the name *file-system-name* already exists. Do you want to use the existing file system as the z/OSMF *file-system-type* file system (Y|N)?**

Explanation: The specified file system already exists. Indicate whether you want to use the existing file system.

In the message text:

file-system-name
Name of the file system

file-system-type
File system type.

System programmer response: To use the existing file system, enter `Y`. Otherwise, enter `N`. Prior to mounting a new file system, you must unmount the existing file system.

User response: No action is required.

IZUG232I **The specified z/OSMF *file-system-type* file system with *name-type* *file-system-name-type* was accepted.**

Explanation: The value specified for the file system name or type was accepted.

In the message text:

file-system-type
File system type

name-type
The word name or type

file-system-name-type
File system name or file system type.

System programmer response: No action is required.

User response: No action is required.

IZUG233E **File system *file-system-name* could not be mounted. A file system with the same name is already mounted at *mount-point*.**

Explanation: The file system could not be mounted at the specified mount point because a file system with the same name is already mounted at another mount point.

In the message text:

file-system-name
Name of the file system

mount-point
Mount point of the file system.

System programmer response: To mount a new file system at that mount point, you must unmount the existing file system and then mount the new file system.

User response: No action is required.

IZUG234I **File system *file-system-name* is already mounted at mount point *mount-point*. Do you want to use the existing file system as the z/OSMF *file-system-type* file system (Y|N)?**

Explanation: The specified file system is already mounted at the mount point. Indicate whether you want to use the existing file system.

In the message text:

file-system-name
Name of the file system

mount-point
Mount point of the file system

file-system-type
File system type.

System programmer response: To use the existing file system, enter `Y`. Otherwise, enter `N`. Prior to mounting a new file system, you must unmount the existing file system.

User response: No action is required.

IZUG235E **The file system could not be mounted at mount point *mount-point*. File system *file-system-name* is already mounted at that mount point.**

Explanation: The file system could not be mounted at the specified mount point because another file system is already mounted at that mount point.

In the message text:

mount-point
Name of the mount point

file-system-name
Name of the file system.

System programmer response: To mount a new file system at that mount point, you must unmount the existing file system and then mount the new file system.

User response: No action is required.

IZUG236I **Enter zFS or HFS as the z/OSMF data file system type for the file system:** *file-system-name***:**

Explanation: This message prompts for the type (zfs or hfs) of the specified file system.

In the message text:

file-system-name
Name of the file system.

System programmer response: No action is required.

User response: No action is required.

IZUG237I **Enter the name of the file to save the configuration data (must be .cfg extension), or press Enter to save as file** *default-cfg-file***:**

Explanation: This message prompts the user to provide the name of the configuration file where the configuration data is to be saved. A default name is provided.

In the message text:

default-cfg-file
Configuration file name.

System programmer response: No action is required.

User response: No action is required.

IZUG238E **File name must be specified with the path.**

Explanation: A value was provided but did not contain a file name.

System programmer response: Provide a valid value and retry.

User response: No action is required.

IZUG239W **File name** *file-name* **already exists: Overwrite (Y|N)?**

Explanation: The specified file name already exists. The message prompts the user to overwrite it.

In the message text:

file-name
File name.

System programmer response: Try the action again.

User response: No action is required.

IZUG240E **Overwrite reply was not (Y). Try again.**

Explanation: A value of Y was not received to overwrite the file. The message prompts the caller to try again.

System programmer response: Try the action again.

User response: No action is required.

IZUG241E **File** *file-name* **cannot be saved to a read-only file system.**

Explanation: The file cannot be saved to a read-only file system.

In the message text:

file-name
File name.

System programmer response: Review the location of where to save the file and try again.

User response: No action is required.

IZUG242I **Do one of the following: Enter the system name, enter NONE not to set the name, or press Enter to accept the default** *system-name***:**

Explanation: The message prompts the caller for the system name value to use. A default value is provided. Enter a value of NONE if you do not want to set the system name.

In the message text:

system-name
Default system name.

System programmer response: No action is required.

User response: No action is required.

IZUG243I **Accepted input:** *input-value*

Explanation: The value for the input has been accepted.

In the message text:

input-value
Input value.

System programmer response: No action is required.

User response: No action is required.

IZUG244I **Enter the z/OSMF root code directory path:**

Explanation: The message prompts for the z/OSMF root code directory path.

System programmer response: No action is required.

User response: No action is required.

IZUG245I Enter the z/OSMF root code directory path or press Enter to accept the default path *path-name*:

Explanation: The message prompts for the root code directory for z/OSMF. A default value is provided.

In the message text:

path-name
Default root code directory path for z/OSMF.

System programmer response: No action is required.

User response: No action is required.

IZUG246I Enter the name of the volume to use for creating the z/OSMF data file system, or enter an asterisk (*) to use SMS managed storage:

Explanation: The message prompts you for the name of the volume to create the z/OSMF data file system. If you enter an asterisk (*), it indicates that you want the z/OS storage management subsystem (SMS) to manage the storage.

System programmer response: Perform the requested action. If you specify a volume, the volume must be on-line. If you specify SMS managed storage, ensure that you have an automatic class selection (ACS) routine in place to assign the appropriate SMS construct, based on the name of the data set to be used for the z/OSMF file system.

User response: No action is required.

IZUG247I z/OSMF data file system will be created on volume: *volume-name*

Explanation: The file system will be created on the specified volume.

In the message text:

volume-name
Name of the volume to create the file system.

System programmer response: No action is required.

User response: No action is required.

IZUG248I Enter the size (in cylinders) to allocate for the data file system:

Explanation: Enter the initial space allocation, in cylinders, for the z/OSMF data file system. z/OSMF uses 90 percent of this value for the primary allocation and 10 percent for the secondary allocation. The minimum suggested size is 100 cylinders, which causes the script to use 90 cylinders for the primary allocation and 10 cylinders for the secondary allocation.

System programmer response: Perform the requested action.

User response: No action is required.

IZUG249E Volume size must be greater than 10 cylinders.

Explanation: The specified volume is too small (less than 10 cylinders).

System programmer response: Specify a volume that is at least 10 cylinders in size.

User response: No action is required.

IZUG250I The z/OSMF data file system *file-system-name* has a *primary-secondary* allocation size of *cylinder-size* cylinders.

Explanation: The specified file system was allocated with the specified number of cylinders for the primary or secondary extent.

In the message text:

file-system-name
Name of the file system

primary-secondary
Primary or secondary allocation for the file system.

cylinder-size
Size in cylinders of the allocation.

System programmer response: No action is required.

User response: No action is required.

IZUG251I Allocating z/OSMF data file system *file-system-name*.

Explanation: The procedure to allocate the specified file system has started.

In the message text:

file-system-name
Name of the file system.

System programmer response: No action is required.

User response: No action is required.

IZUG252I Mounting *file-system-name* at *mount-point*.

Explanation: The procedure to mount the specified file system at the specified mount point has started.

In the message text:

file-system-name
Name of the file system

mount-point
Mount point of the file system.

System programmer response: No action is required.

User response: No action is required.

IZUG253I Enter the Common Information Model (CIM) administrator user ID, or press Enter to accept the default *default-value*:

Explanation: The message prompts for the Common Information Model (CIM) administrator user ID. A default attribute value is provided.

In the message text:

default-value
Default value for the CIM administrator user ID.

System programmer response: Perform the requested action, or accept the default.

User response: No action is required.

IZUG254E Unable to copy *source-file-name* to *target-file-name*.

Explanation: Attempt to copy the specified file failed.

In the message text:

file-name
Name of the file source

target-file-name
Name of the file target

System programmer response: Ensure that the caller is authorized to perform the copy.

User response: No action is required.

IZUG255I Enter the z/OSMF administrator *attribute-name*:

Explanation: The message prompts for the z/OSMF administrator attributes used to create the z/OSMF administrator.

In the message text:

attribute-name
Name of the attribute to create z/OSMF administrator.

System programmer response: No action is required.

User response: No action is required.

IZUG256I Enter the z/OSMF administrator *attribute-name-keyword*, or press Enter to accept the default *value*:

Explanation: The message is used to prompt for the z/OSMF administrator attributes. The message individually prompts for the following attributes:

- User ID
- Home directory
- Shell program name
- Logon Procedure Name
- Account number
- Region size

These attributes are used to create the z/OSMF administrator user ID. A default attribute value is provided.

In the message text:

attribute-name-keyword
Name of the attribute

value Default value of the attribute.

System programmer response: Enter the requested information, or accept the default.

User response: No action is required.

IZUG257W User *user-id* already exists.

Explanation: The user ID provided already exists.

In the message text:

user-id User name.

System programmer response: No action is required.

User response: No action is required.

IZUG258I Enter the Common Information Model (CIM) administrator user ID:

Explanation: The message prompts for the Common Information Model (CIM) administrator user ID.

System programmer response: No action is required.

User response: No action is required.

IZUG259I Enter the default RACF-defined group for the z/OSMF administrator:

Explanation: The message prompts for the default group for the z/OSMF administrator.

System programmer response: No action is required.

User response: No action is required.

IZUG260I Enter the default RACF-defined group for the z/OSMF administrator, or press Enter to accept the default *group-id*:

Explanation: The message prompts for the default group for the z/OSMF administrator. A default value is provided.

In the message text:

group-id
Name of the default group.

System programmer response: No action is required.

User response: No action is required.

IZUG261E **Attribute** *attribute-name* **must be** *attribute-size***.**

Explanation: The value provided for the attribute does not conform to the expected range or size in the number of characters.

In the message text:

attribute-name
Name of the attribute

attribute-size
Expected attribute size.

System programmer response: Specify the value within the correct range or size.

User response: No action is required.

IZUG262I **Enter the server attribute** *attribute-name***:**

Explanation: The message prompts for the name of the z/OSMF server attributes.

In the message text:

attribute-name
Name of the attribute for the server.

System programmer response: Enter the server attribute name.

User response: No action is required.

IZUG263I **Enter the server attribute** *attribute-name***, or press Enter to accept the default value** *value***:**

Explanation: The message prompts for the z/OSMF server attributes. A default value is provided.

In the message text:

attribute-name
Name of the attribute

value Name of the attribute to which the default applies.

System programmer response: Enter the requested information, or accept the default.

User response: No action is required.

IZUG264E **Value** *attribute-name* **must be alphanumeric and must be** *attribute-size* **characters.**

Explanation: The value provided for the z/OSMF server is incorrect or outside the expected range or size for that attribute.

In the message text:

attribute-name
Name of the attribute for the z/OSMF server.

attribute-size
Size or range for the attribute for the z/OSMF server.

System programmer response: Specify with the correct range or size.

User response: No action is required.

IZUG265I **Enter the root directory path of the z/OSMF server:**

Explanation: The message prompts for the root directory path for the z/OSMF server.

System programmer response: Enter the root directory path.

User response: No action is required.

IZUG266I **Enter the root directory path of the z/OSMF server, or press Enter to accept the default** *server-root-directory***:**

Explanation: The message prompts for the root directory path for the z/OSMF server. A default value is provided.

In the message text:

server-root-directory
Default root directory path of the z/OSMF server.

System programmer response: Enter the root directory path or accept the default.

User response: No action is required.

IZUG267I **Enter the SAF profile prefix (case sensitive) for z/OSMF resources:**

Explanation: The message prompts for the SAF profile prefix.

System programmer response: Enter the SAF profile prefix.

User response: No action is required.

IZUG268I **Enter the SAF profile prefix (case sensitive) for z/OSMF resources, or press Enter to accept the default** *saf-profile***:**

Explanation: The message prompts for the SAF profile prefix. A default value is provided.

In the message text:

saf-profile
Default SAF profile prefix.

System programmer response: Enter the SAF profile

prefix, or accept the default.

User response: No action is required.

IZUG271I **Do you want to enable the common event adapter (CEA) component and update related parmlib options for using the Incident Log task? For yes, enter Y. For no, enter N:**

Explanation: The message prompts you to determine whether the Incident Log task is to be configured. When you select to configure the Incident Log task, z/OSMF verifies that the Common Information Model (CIM) server and the common event adapter (CEA) are properly configured. If you have already configured CIM and have set up the CEA parmlib, you still must enter Y. z/OSMF provides additional prompts allowing you to indicate whether the CIM server and the CEA parmlib need to be configured.

If you do not configure the Incident Log task, you cannot complete any other Incident Log set up steps, such as setting up RACF permissions for the Incident Log. In this case, the Incident Log task stills displays in the navigation area in z/OSMF; however, it will not be functional. To remove it from the navigation area, do not authorize any roles to access the Incident Log task.

System programmer response: Enter Y or N.

User response: No action is required.

IZUG272I **Do you want to enable the common event adapter (CEA) component and update related parmlib options for using the Incident Log task? For yes, enter Y. For no, enter N. Or press Enter to accept the default** *value***:**

Explanation: The message prompts you to determine whether the Incident Log task should be configured. When you select to configure the Incident Log task, the Common Information Model (CIM) server and the common event adapter (CEA) are configured so that they can support the Incident Log task. If you have already configured CIM and have set up the CEA parmlib, you still need to enter Y. When you are asked whether CIM needs to be configured, you can say no. In this case, confirming that you want to set up the Incident Log task gives z/OSMF permission to verify that all of the settings are correct.

If you do not configure the Incident Log task, you cannot complete any other Incident Log set up steps, such as setting up RACF permissions for the Incident Log. The Incident Log task still displays the navigation area in z/OSMF; however, it will not be functional. To remove the Incident Log task from the navigation area, do not authorize any roles to access this task.

In the message text:

value Default value to specify setup of the Incident Log task.

System programmer response: Enter Y or N, or accept the default, which is Y.

User response: No action is required.

IZUG273I **Enter the** *dependency-name dependency-attribute***:**

Explanation: The message prompts for the Common Information Model (CIM) or common event adapter (CEA) attributes. The *attribute-name-keyword* can be a group user ID or the keyword AUTOGID, the user ID, or the keyword AUTOUID, or the group name. The *attribute-name* can be a group user ID, user ID, or group name.

In the message text:

dependency-name
Name of the Incident Log dependency

dependency-attribute
Name of the Incident Log attribute.

System programmer response: Enter the incident dependency name and log attribute names.

User response: No action is required.

IZUG274I **Enter the** *component-name attribute-name-keyword***, or press Enter to accept** *value***:**

Explanation: The message prompts for the Common Information Model (CIM) or common event adapter (CEA) attributes. The *attribute-name-keyword* can be a group user ID or the keyword AUTOGID, the user ID, or the keyword AUTOUID, or the group name. The *attribute-name* can be a group user ID, user ID, or group name. A default value is provided.

In the message text:

component-name
Name of the component

attribute-name-keyword
Name of the attribute keyword

value Default value.

System programmer response: Enter the information, or accept the default.

User response: No action is required.

IZUG275I **Enter the member name suffix to use for the** *parmlib-member-name* **parmlib member, or press Enter to accept the default** *suffix-value***:**

Explanation: The message prompts for the suffix to use for IEADMC and CEAPRM members. A default value is provided.

In the message text:

parmlib-member-name
Name of the parmlib member

suffix-value
Default suffix of the parmlib member.

System programmer response: No action is required.

User response: No action is required.

IZUG276I **Enter the member name suffix to use for the** *parmlib-member-name* **parmlib member:**

Explanation: The message prompts for the suffix to use for IEADMC and CEAPRM members.

System programmer response: Enter the parmlib suffix.

User response: No action is required.

IZUG277I **Enter the** *branch-country-name* **code, or press Enter to accept the default** *attribute-value***:**

Explanation: The message prompts for the country code or branch code value. A default is provided.

In the message text:

branch-country-name
Name of the branch or country

attribute-value
Default value for the branch or country.

System programmer response: Enter the country or branch code, or accept the default.

User response: No action is required.

IZUG278I **Enter the** *branch-country-name* **code:**

Explanation: The message prompts for the country code or branch code value.

In the message text:

branch-country-name
Name of the branch or country.

System programmer response: enter the country or branch code.

User response: No action is required.

IZUG279E **The** *branch-country-name* **code must be** *branch-country-range* **alphanumeric characters (A-Z, 0-9).**

Explanation: The value specified for the branch or country code does not conform to guidelines.

In the message text:

branch-country-name
Name of the branch or country

branch-country-range
Range for the branch or country attribute.

System programmer response: Specify the correct value.

User response: No action is required.

IZUG280I **Do you want to accept storage value** *storage-name***? (Y|N)?**

Explanation: The message prompts whether you want to use the existing specified storage option.

System programmer response: Enter Y or N.

User response: No action is required.

IZUG281I **What storage option do you want to use? Enter V for VOLSER or S for STORCLAS.**

Explanation: The message prompts for the storage option to use.

System programmer response: Enter a value.

User response: No action is required.

IZUG282I **Enter the name of the** *SMS-storage-class***:**

Explanation: The message prompts for the name of the specified SMS storage class.

In the message text:

SMS-storage-class
Type of storage option.

System programmer response: Enter a storage class name.

User response: No action is required.

IZUG283I **Specify one or more of the non-SMS direct access volumes to use. When you are finished entering the values, press Enter again without a value to complete:**

Explanation: The message prompts for the volumes to use for the storage option.

System programmer response: Enter the volume information. When you have entered all of the information for volume, to complete the input press Enter without specifying a value.

User response: No action is required.

IZUG284I **Enter the name of the source data set for your existing CEAPRM00 parmlib member. Specify the fully qualified data set name, or press Enter to accept the default** *parmlib-name***:**

Explanation: The message prompts you for the name of the data set that contains your existing CEAPRM00 parmlib member. A fully qualified data set name is expected.

In the message text:

parmlib-name
Default data set name.

System programmer response: Specify the fully qualified data set name, or press Enter to accept the supplied default if it is correct for your environment. If you specify the data set name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response: No action is required.

IZUG285I **Enter the name of the source data set for your existing CEAPRM00 parmlib member. Specify the fully qualified data set name, or press Enter to use SYS1.PARMLIB:**

Explanation: The message prompts you for the name of the data set that contains your existing CEAPRM00 parmlib member. A fully qualified data set name is expected.

System programmer response: Specify the fully qualified data set name, or press Enter to use SYS1.PARMLIB as the source for the CEAPRM00 member. If you specify the data set name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response: No action is required.

IZUG286W **Arguments are ignored.**

Explanation: The additional unknown arguments that have been supplied in the call will be ignored.

System programmer response: No action is required.

User response: No action is required.

IZUG287I **z/OSMF RACF** *racf-procedure* **processing complete. Review and run** *racf-rexx-file* **before proceeding with configuration.**

Explanation: RACF processing has completed for the specified procedure.

In the message text:

racf-procedure
Name of the RACF procedure being performed

racf-rexx-file
Name of the RACF REXX exec.

System programmer response: Review and run the REXX script before proceeding.

User response: No action is required.

IZUG288I **The .profile is being created for the user.**

Explanation: User .profile was not found. Attempting to create a .profile for the user.

System programmer response: No action is required.

User response: No action is required.

IZUG289I **The .profile is being updated with Common Information Model (CIM) environment variables.**

Explanation: User .profile does not contain Common Information model (CIM) environment variables. Attempting to update .profile with CIM environment variables.

System programmer response: No action is required.

User response: No action is required.

IZUG290E **An attempt to update** *file-name* **has failed.**

Explanation: Attempt to update the specified file failed.

In the message text:

file-name
File name.

System programmer response: Review log file for details.

User response: No action is required.

IZUG291I **The .profile update is complete.**

Explanation: The .profile has been updated.

System programmer response: No action is required.

User response: No action is required.

IZUG292W **Common Information Model (CIM) environment variables already set up in .profile:** *wbem-root-value*

Explanation: The .profile already contains Common Information model (CIM) environment variables.

In the message text:

wbem-root-value
Home directory of WBEM in the .profile.

System programmer response: Ensure that the value in .profile matches the value specified in the configuration.

User response: No action is required.

IZUG293I Procedure *procedure* is being started.

Explanation: An attempt to start the specified procedure has been made.

In the message text:

procedure
Procedure being started.

System programmer response: No action is required.

User response: No action is required.

IZUG294E Common Information Model (CIM) server failed to start.

Explanation: Attempt to start the Common Information Model (CIM) server failed.

System programmer response: Review log file for details.

User response: No action is required.

IZUG295E Verification process *ivp-name* has failed.

Explanation: The verification process has failed.

In the message text:

ivp-name
Name of the IVP task.

System programmer response: Review the log file for details.

User response: No action is required.

IZUG296I Verification process *ivp-name* has completed.

Explanation: The specified verification process has completed.

In the message text:

ivp-name
Name of the IVP task.

System programmer response: No action is required.

User response: No action is required.

IZUG297I Provider *provider-name* is already registered with Common Information Model (CIM).

Explanation: The specified provider was found to have been already registered with Common Information Model (CIM).

In the message text:

provider-name
Name of the provider.

System programmer response: No action is required.

User response: No action is required.

IZUG298E Provider *provider-name* is not registered with Common Information Model (CIM).

Explanation: The specified provider is not registered with Common Information Model (CIM).

In the message text:

provider-name
Name of the provider.

System programmer response: No action is required.

User response: No action is required.

IZUG299I The provider *provider-name* is being registered with Common Information Model (CIM).

Explanation: An attempt has been made to register the provider with Common Information Model (CIM).

In the message text:

provider-name
Name of the provider.

System programmer response: No action is required.

User response: No action is required.

IZUG300I Processing of script *script-name* has started at *date-and-time*.

Explanation: Script processing has started. The script name, data, and time are included.

In the message text:

script-name
Name of the script

date-and-time
Date and time that script processing started.

System programmer response: No action is required.

User response: No action is required.

IZUG301I **Log directory** *log-directory* **does not exist or is not writable: using temporary directory for log file.**

Explanation: For script processing, the named log directory (**logs**) within the z/OSMF data directory does not exist or the user who is executing the script does not have permission to write to this directory. The log file for processing of the script will be created in the temporary directory.

In the message text:

log-directory
Name of directory for the log files.

System programmer response: No action is required.

User response: No action is required.

IZUG302I **Log will be written to file** *log-file-path-and-name***.**

Explanation: The path name of the log file for script processing is provided.

In the message text:

log-file-path-and-name
Directory and file name of the log.

System programmer response: No action is required.

User response: No action is required.

IZUG303I **Environment name and value being used are** *env-var***.**

Explanation: The name and value for an environment setting is provided.

In the message text:

env-var Name and value of an environment setting.

System programmer response: No action is required.

User response: No action is required.

IZUG304E **An error occurred writing to log file** *log-file-path-and-name***: exiting script.**

Explanation: An error was encountered while attempting to write to the log file.

In the message text:

log-file-path-and-name
Directory and file name of the log.

System programmer response: Check for additional error messages on the screen that describe the error. Rerun after correcting the error.

User response: No action is required.

IZUG305E **The script** *script-name* **failed with reason code** *reason-code***; see log file** *log-file-path-and-name***.**

Explanation: The indicated script failed. A return code is provided to help indicate the cause of the error.

In the message text:

script-name
Script that failed

reason-code
Reason code for the error

log-file-path-and-name
Directory and file name of the log file.

For the **izuadmin.sh** script, the following reason codes are valid:

1 Script was called with incorrect arguments.

2 Problem with the log directory.

3 Error writing to the log file, or the log file is not accessible.

4 Required environment variable is missing or set incorrectly. Or, the izuadmin.env file does not exist.

5 Required environment setting is missing or incorrect. This error can occur if an expected configuration property or properties file, such as izuapps.properties, is not set, cannot be found, or is not readable.

6 Problem found during verification processing.

7 Installed z/OS level is incorrect for z/OSMF.

105 Exception encountered by an internal script.

For the **izuprime.sh** script, the following reason codes are valid:

1 Usage error.

2 Problem with the log directory.

3 Error writing to the log file.

4 Script encountered an error when running a z/OS UNIX shell command, such as mkdir or cp.

5 A repository already exists.

6 Specified user ID is not defined to the z/OS system.

System programmer response: For more information, see the z/OSMF log file for related messages. After correcting the error, run the script again. For reason code 105, contact IBM Support for assistance.

User response: No action is required.

IZUG306I **Script** *script-name* **was invoked with options** *input-options***.**

Explanation: The options specified as input to the named script are provided.

In the message text:

script-name
Name of the script

input-options
Options passed to the script.

System programmer response: No action is required.

User response: No action is required.

IZUG311E **IZU_APPSERVER_ROOT** *server-root-directory* **is not valid: exiting script.**

Explanation: The z/OSMF server root directory is not valid. The processing for the script stops.

In the message text:

server-root-directory
Root directory of the z/OSMF server.

System programmer response: Set IZU_APPSERVER_ROOT to the valid root directory and run again.

User response: No action is required.

IZUG312I **The administration request is being processed.**

Explanation: Processing of the administration request has started.

System programmer response: No action is required.

User response: No action is required.

IZUG313E **A usage error has occurred:** *error***.**

Explanation: A problem with the usage has occurred. Context of the error is provided.

In the message text:

error Explanation for the incorrect usage.

System programmer response: Correct the problem indicated by the explanation of the error and run again.

User response: No action is required.

IZUG314E **IZU_CODE_ROOT** *product-root-directory* **is not valid: exiting script.**

Explanation: The z/OSMF product root directory is not valid.

In the message text:

product-root-directory
Root directory of the z/OSMF product.

System programmer response: Set IZU_CODE_ROOT to the valid z/OSMF product root directory and run again.

User response: No action is required.

IZUG315E **An incorrect environment setting has been detected:** *env-var***.**

Explanation: A problem exists with a setting in the environment file. Context of the error is provided.

In the message text:

env-var Environment setting and associated problem.

System programmer response: Review the included environment setting and the associated problem. Correct the error and run again.

User response: No action is required.

IZUG316E **PEGASUS_HOME directory** *CIM-server-root-directory* **is not valid: exiting script.**

Explanation: The Common Information Model (CIM) server WBEM root directory is not valid. Processing for the script stops.

In the message text:

CIM-server-root-directory
WBEM root directory of the CIM server.

System programmer response: Set PEGASUS_HOME to the Common Information Model (CIM) server WBEM root directory and run the script again.

User response: No action is required.

IZUG317E **IZU_CONFIG_DIR** *configuration-directory* **is not valid: exiting script.**

Explanation: The z/OSMF configuration directory is not valid. Processing for the script stops.

In the message text:

configuration-directory
Configuration directory of the z/OSMF product.

System programmer response: Set IZU_CONFIG_DIR to the valid z/OSMF configuration directory and run again.

User response: No action is required.

IZUG318E **Path** *path-setting* **member** *member-name* **must exist: exiting script.**

Explanation: A directory or path that is a member of the specified path setting does not exist. Processing of the script stops.

In the message text:

path-setting
Name of the path setting

member-name
Directory or file specified in the path that does not exist.

System programmer response: Determine why the file or directory does not exist. Correct the problem and run again.

User response: No action is required.

IZUG319E **Data directory** *data-directory* **must exist and be writable: exiting script.**

Explanation: For script processing the z/OSMF data directory must exist and be capable of being written to. Processing of the script stops.

In the message text:

data-directory
Name of the data directory.

System programmer response: Ensure the z/OSMF data directory exists. Ensure that the user running the script has permission to write to the directory. After correcting the error run again.

User response: No action is required.

IZUG320E **Users will not be able to launch z/OSMF. The installed z/OS level** *installed-z/OS-level* **is earlier than the minimum z/OS level** *minimum-z/OS-level* **that is required by z/OSMF.**

Explanation: z/OSMF cannot be launched because it is installed on a system that is earlier than the minimum supported level of z/OS.

In the message text:

installed-z/OS-level
Installed operating system level

minimum-z/OS-level
Minimum operating system level that z/OSMF requires.

In the message text, the software level for the product (z/OS or z/OSMF) is indicated through a standard convention: *aa.bb.cc*, where:

- *aa* is the version
- *bb* is the release
- *cc* is the modification level.

You can correlate the returned value as follows:

- 04.02.00 indicates V2R2 for the product (z/OS)
- 04.01.00 indicates V2R1 for the product (z/OS or z/OSMF)
- 03.23.00 indicates V1R13 for the product (z/OS or z/OSMF)

Thus, for example, the value 04.02.00 indicates V2R2 of the product (z/OS).

System programmer response: Upgrade to a z/OS level that is supported by z/OSMF.

User response: No action is required.

IZUG321W **The installed z/OSMF level** *product-level* **is earlier than the z/OS level** *os-level***.**

Explanation: Your system is running z/OSMF level *product-level*, but a newer z/OSMF level might be available from IBM. Most likely, your installation has migrated to a new release of z/OS without upgrading the z/OSMF product. To allow z/OSMF to use the latest functions in z/OS level *os-level*, it is recommended that you upgrade z/OSMF to the latest level. Until you do so, z/OSMF will continue to operate at its current level of functionality.

In the message text:

product-level
Level of the installed z/OSMF product.

os-level Operating system level.

In the message text, the software level for the product (z/OS or z/OSMF) is indicated through a standard convention: *aa.bb.cc*, where:

- *aa* is the version
- *bb* is the release
- *cc* is the modification level.

You can correlate the returned value as follows:

- 04.02.00 indicates V2R2 for the product (z/OS)
- 04.01.00 indicates V2R1 for the product (z/OS or z/OSMF)
- 03.23.00 indicates V1R13 for the product (z/OS or z/OSMF)

Thus, for example, the value 04.02.00 indicates V2R2 of the product (z/OS).

System programmer response: Upgrade z/OSMF to the latest level that is supported on your z/OS system.

User response: No action is required.

IZUG333I **Enter the z/OSMF Unauthenticated *unauthenticated-UID*, or enter the keyword AUTOUID:**

Explanation: The message prompts you to input unauthenticated guest user UID in z/OSMF.

In the message text:

unauthenticated-UID
unauthenticated user UID.

System programmer response: Enter a valid value.

User response: No action is required.

IZUG334I **Enter the z/OSMF Unauthenticated *unauthenticated-UID*, or enter the keyword AUTOUID, or press Enter to accept the default *default-unauthenticated-UID*:**

Explanation: The message prompts you to input unauthenticated guest user UID in z/OSMF. To accept the default, press Enter.

In the message text:

unauthenticated-UID
unauthenticated guest user UID.

default-unauthenticated-UID
Default unauthenticated user UID.

System programmer response: Enter a valid value.

User response: No action is required.

IZUG335E **A symbolic link is required for the directory: /etc/zosmf. The link could not be created, however, because the directory already exists or etc/zosmf is already defined as the symbolic link for another directory.**

Explanation: While processing the izusetup.sh -finish script, z/OSMF detected that the z/OSMF configuration directory is set to use a directory name other than the product default: /etc/zosmf. This directory name is specified through the variable IZU_CONFIG_DIR. Most likely, your installation chose another name for this directory when configuring z/OSMF on your system.

Because the z/OSMF online help system requires /etc/zosmf as its mount point, z/OSMF attempts to create a symbolic link "etc/zosmf" that resolves to the path name of your specified directory. The link could not be created, however, either because directory /etc/zosmf already exists on your system, or "etc/zosmf" is already defined as a symbolic link for another directory.

System programmer response: To resolve this error, take one of the following actions, as appropriate:

- If the directory /etc/zosmf already exists on your system, examine the directory and its contents. Determine whether the directory can be deleted safely, or its contents moved to another directory. If so, take these steps to remove the directory. Then, run the configuration request again.
- Change your installation's specification for the IZU_CONFIG_DIR variable to the default value /etc/zosmf, and re-run the z/OSMF configuration process, starting with the izusetup.sh -config invocation. You can specify this directory name in the override file for variable IZU_CONFIG_DIR, or interactively, in response to the script prompt for the name of the z/OSMF configuration directory.

User response: Contact your z/OSMF administrator or system programmer.

IZUG336I **Work manager *work-manager-name* is being created.**

Explanation: The work manager is being created.

In the message text:

work-manager-name
Name of the work manager.

System programmer response: No action is required.

User response: No action is required.

IZUG337I **Work manager *work-manager-name* property *property-name* is being set to value *value*.**

Explanation: The work manager property is being set to the indicated value.

In the message text:

work-manager-name
Name of the work manager

property-name
Name of the property

value Value for the property.

System programmer response: No action is required.

User response: No action is required.

IZUG340I **Variable substitution entry *variable-name* is being updated with value *value*.**

Explanation: The variable substitution entry is being updated with the specified value.

In the message text:

variable-name
Name of the variable

value Value of the variable.

System programmer response: No action is required.

User response: No action is required.

IZUG341I **Variable substitution entry** *variable-name* **is being created with value** *value***.**

Explanation: The variable substitution entry is being created with the specified value.

In the message text:

variable-name
Name of the variable

value Value of the variable.

System programmer response: No action is required.

User response: No action is required.

IZUG343I **Shared library** *shared-library-name* **with class path** *class-path* **and native path** *native-path* **is being deleted.**

Explanation: The specified shared library with the specified class path and native path is being removed.

In the message text:

shared-library-name
Name of the shared library

class-path
classpath value

native-path
Native path value.

System programmer response: No action is required.

User response: No action is required.

IZUG344I **Shared library** *shared-library-name* **with class path** *class-path* **and native path** *native-path* **is being created.**

Explanation: The specified shared library with the specified class path and native path is being created.

In the message text:

shared-library-name
Name of the shared library

class-path
classpath value

native-path
Native path value.

System programmer response: No action is required.

User response: No action is required.

IZUG345I **Plug-in** *plugin-name* **is being removed.**

Explanation: The specified plug-in is being removed from z/OSMF.

In the message text:

plugin-name
Name of the plug-in.

System programmer response: No action is required.

User response: No action is required.

IZUG346I **Plug-in** *plug-in-name* **from location** *file-location* **is being installed.**

Explanation: The plug-in is being installed into z/OSMF from the specified location.

In the message text:

plugin-name
Name of the plug-in.

file-location
Location of the Enterprise Archive (EAR) file.

System programmer response: No action is required.

User response: No action is required.

IZUG347I **Reference to shared library** *shared-library-name* **with scope** *scope* **is being added.**

Explanation: A reference to the shared library is being added with the specified scope.

In the message text:

shared-library-name
Name of the shared library

scope Scope of the shared library reference.

System programmer response: No action is required.

User response: No action is required.

IZUG348I **Processing of your request has started. This process might require several minutes or more to complete.**

Explanation: The requested script processing is running, but might take some time to complete. As it runs, the script writes messages to the script log file.

System programmer response: No action is required.

User response: No action is required.

IZUG349I **The function** *function-name* **can be accessed at link** *link-name* **after the z/OSMF server is started on your system.**

Explanation: The requested configuration process completed. z/OSMF will be available to users at the indicated URL after the z/OSMF server is restarted on this system.

In the message text:

function-name
The z/OSMF function that is available.

link-name
The link for accessing z/OSMF.

System programmer response: No action is required.

User response: No action is required.

IZUG354I **Security option** *option-name* **with value** *option-value* **is being set.**

Explanation: A security setting in the z/OSMF server is being updated to the specified value.

In the message text:

option-name
Name of the option being set

option-value
Value of the option being set.

System programmer response: No action is required.

User response: No action is required.

IZUG356I **Plug-in** *plugin-name* **is being stopped.**

Explanation: The specified plug-in is being stopped.

In the message text:

plugin-name
Name of the plug-in.

System programmer response: No action is required.

User response: No action is required.

IZUG357I **Plug-in** *plugin-name* **is being started.**

Explanation: The specified plug-in is being started.

In the message text:

plugin-name
Name of the plug-in.

System programmer response: No action is required.

User response: No action is required.

IZUG358E **Server** *server-name* **does not exist.**

Explanation: The specified server does not exist.

In the message text:

server-name
Name of the server.

System programmer response: Specify a valid server name and repeat this operation.

User response: No action is required.

IZUG360I **Script option** *option-name* **is deprecated. The z/OSMF configuration process ignores this option.**

Explanation: The specified script option is deprecated. The z/OSMF process ignores the option and continues processing as normal. If you received this message when running the izusetup.sh script with the -service option, understand that the -service option is no longer required when you apply z/OSMF service to your system.

In the message text:

option-name
Option that was specified.

System programmer response: To avoid receiving this message in the future, do not specify the indicated option. If you received this message when applying z/OSMF service, you are using an obsolete option. Review the HOLDDATA section of the PTF for instructions on applying service to your system.

User response: No action is required.

IZUG361I **Do you want to create a Certificate Authority? For yes, enter Y. For no, enter N:.**

Explanation: The message prompts you to indicate whether (Y or N) the z/OSMF security setup should include the creation of a Certificate Authority (CA). The CA is used to sign server certificates that are used for secure (SSL) communication between the user's web browser and the z/OSMF server. Y is the default.

If you specify N, you must provide your own CA for enabling secure communications.

System programmer response: Enter a valid value.

User response: No action is required.

IZUG362I **Do you want to create a Certificate Authority? For yes, enter Y. For no, enter N. Or press Enter to accept the default value** *default-value***.**

Explanation: The message prompts you to indicate whether (Y or N) the z/OSMF security setup should include the creation of a Certificate Authority (CA). The CA is used to sign server certificates that are used for secure (SSL) communication between the user's web browser and the z/OSMF server. The default value is provided.

In the message text:

default-value
Default value for creating Certificate Authority (Y or N).

System programmer response: Enter the a valid value (Y or N) or press Enter to select the default value.

User response: No action is required.

IZUG363E **User** *user-name* **is not permitted to access the digital certificate** *certificate-label***.**

Explanation: The specified user lacks sufficient authorization to the indicated digital certificate.

In the message text:

user-name
Name of the user

certificate-label
Label of digital certificate.

System programmer response: Determine whether the user requires access to the digital certificate. If so, grant access to the user.

User response: No action is required.

IZUG364E **User** *user-name* **did not connect label** *certificate-label* **to keyring** *certificate-keyring***.**

Explanation: The specified user lacks sufficient authorization to the indicated keyring.

In the message text:

user-name
Name of the user.

certificate-label
Label of the digital certificate.

certificate-keyring
Keyring of the digital certificate.

System programmer response: Determine whether the user requires access to the keyring. If so, grant access to the user.

User response: No action is required.

IZUG365I **Process** *process-name* **with start command arguments is being updated to include value** *value-1***. The value of the arguments is now** *value-2***.**

Explanation: The specified argument is being added to the start command arguments for the specified process.

In the message text:

process-name
Name of the server process

value-1 Value of the new argument being added

value-2 New value of the start command arguments.

System programmer response: No action is required.

User response: No action is required.

IZUG366E **The supplied level of Java does not meet the minimum that is required by z/OSMF. Level found:** *found-java-level* **Level required:** *required-java-level***.**

Explanation: z/OSMF requires the indicated level of Java to be installed and operational on your system. During the configuration process, however, z/OSMF found an incorrect version of Java. To determine the installed level of Java, z/OSMF checks the location specified on the environment variable JAVA_HOME.

In the message text:

found-java-level
The level of Java that was found on your system.

required-java-level
The minimum level of Java that is required for z/OSMF operation.

System programmer response: Determine whether the minimum level of Java is installed and mounted on your system. If so, ensure that the environment variable JAVA_HOME specifies the correct location. If your installation uses a mount point other than the product default, update the z/OSMF environment variable JAVA_HOME to refer to the correct location. This action will not affect any other products requiring a different level of Java.

User response: No action is required.

IZUG367W **Member** *target-member-name* **specifies HLQ value** *hlq-value* **for incidents. This setting will be overwritten by member** *source-member-name* **and HLQLONG value** *hlqlong-value***. As a result, you might not be able to manage any previously created incidents. Do you want to continue? (Y|N)?**

Explanation: The existing HLQ value in the indicated source member will be replaced by the HLQLONG value specified in the target member.

In the message text:

target-member-name
The target member name.

hlq-value
The current HLQ value.

source-member-name
source member name.

hlqlong-value
HLQLONG value.

System programmer response: Enter Y to continue with this operation. Otherwise, enter N to cancel.

User response: No action is required.

IZUG368I **Enter the z/OSMF unauthenticated user name *unauthenticated-name*.**

Explanation: The message prompts you to input unauthenticated guest user name in z/OSMF.

unauthenticated-name
unauthenticated user name.

System programmer response: Enter a valid value.

User response: No action is required.

IZUG369I **Enter the z/OSMF unauthenticated user name *unauthenticated-name*, or press Enter to accept the default value *default-unauthenticated-name*.**

Explanation: The message prompts you for the unauthenticated guest user name in z/OSMF. To accept the default, press Enter.

unauthenticated-name
unauthenticated guest user name.

default-unauthenticated-name
Default unauthenticated user name.

System programmer response: Enter a valid value, or press Enter the accept the default value.

User response: No action is required.

IZUG370I **User registry is being initialized with user ID *user-id*.**

Explanation: The z/OSMF user registry is being initialized with the specified user ID.

In the message text:

user-id User ID with which the user registry is being initialized.

System programmer response: No action is required.

User response: No action is required.

IZUG371I **Role repository is being initialized for user ID *user-id*.**

Explanation: The z/OSMF role repository is being initialized for the specified user ID.

In the message text:

user-id User ID for which the role repository is being initialized.

System programmer response: No action is required.

User response: No action is required.

IZUG372E **Command *command-name* returned an error. Command return code is *return-code*.**

Explanation: An error was received from a command invocation.

In the message text:

command-name
Command that returned the error

return-code
Return code from the command.

System programmer response: Search the log for other error messages that indicate the problem. Correct the problem indicated by the messages and run again.

User response: No action is required.

IZUG373E **Repository *repository-name* was not initialized because it already exists: exiting script.**

Explanation: A z/OSMF repository was not initialized because it already exists. A z/OSMF repository can only be initialized if it does not exist. Processing of the script stops.

In the message text:

repository-name
Name of the existing repository.

System programmer response: Do not attempt to initialize the existing repository.

User response: No action is required.

IZUG374E **User ID *user-id* for the z/OSMF administrator must exist: exiting script.**

Explanation: The z/OSMF repositories were not initialized because the administrator user ID does not exist. Processing of the script stops.

In the message text:

user-id User ID that does not exist.

System programmer response: Search the log for other error messages that might indicate the problem. Correct the problem indicated by the messages and run again.

User response: No action is required.

IZUG375I **Verification has completed for *item-name*.**

Explanation: Verification has completed for the specified item.

In the message text:

item-name
Item that was verified.

System programmer response: No action is required.

User response: No action is required.

IZUG376E **Verification failed for** *item-name* **because of the following reason:** *reason*

Explanation: Verification failed for the item because of the specified reason. Context of the error is provided.

In the message text:

item-name
Item that failed verification

reason Reason verification failed.

System programmer response: Perform action to correct the problem based on the indicated reason.

User response: No action is required.

IZUG377E **Unable to write to** *directory-name***: exiting script.**

Explanation: Attempt to write to the specified directory failed.

In the message text:

directory-name
Name of the directory being written to.

System programmer response: Ensure user has access to write to the directory.

User response: No action is required.

IZUG378I **Process** *process-name* **JVM custom property** *property-name* **that has a value of** *value* **is being deleted.**

Explanation: The specified property for the named process is being removed.

In the message text:

process-name
Name of the server process

property-name
Name of the property

value Value of the property.

System programmer response: No action is required.

User response: No action is required.

IZUG379I **Process** *process-name* **JVM custom property** *property-name* **that has a value of** *value* **is being created.**

Explanation: The specified property for the named process is being added.

In the message text:

process-name
Name of the server process

property-name
Name of the property

value Value of the property.

System programmer response: No action is required.

User response: No action is required.

IZUG380E **Unable to unmount file system** *file-system-name***.**

Explanation: Attempt to unmount the indicated file system failed.

In the message text:

file-system-name
Name of the file system.

System programmer response: For more information, see the log file.

User response: No action is required.

IZUG381I **Unmounting** *file-system-name***.**

Explanation: The procedure to unmount the specified file system has started.

In the message text:

file-system-name
Name of the file system.

System programmer response: No action is required.

User response: No action is required.

IZUG382E **File system** *file-system-name* **does not exist.**

Explanation: The specified file system does not exist.

In the message text:

file-system-name
Name of the file system.

System programmer response: Specify a file system that does exist.

User response: No action is required.

IZUG383I **File system** *file-system-name* **is mounted at mount point** *mount-point***.**

Explanation: The indicated file system is mounted at that mount point.

In the message text:

file-system-name
Name of the file system

mount-point
Name of the mount point.

System programmer response: No action is required.

User response: No action is required.

IZUG384I Object *object-name* **property** *property-name*, **which has a value of** *value*, **is being deleted.**

Explanation: The indicated property for this object is being deleted. The current setting for the property is shown.

You have either selected to change the current setting of a property, or you are deleting the property altogether. When you change the value of a property, the property is first deleted and then created again with the new value. When you delete a property, z/OSMF uses the property default instead.

In the message text:

object-name
Name of the object

property-name
Name of the property

value Value of the property.

System programmer response: No action is required.

User response: No action is required.

IZUG385I The z/OSMF server is not started. To allow the -addlink request to complete, restart the z/OSMF server.

Explanation: The -addlink request cannot complete until you start the z/OSMF server.

System programmer response: Start the z/OSMF server.

After the server is started, see the z/OSMF log file for an indication of the success or failure of this request. The z/OSMF log file is named IZUG*n*.log, where *n* is a number from 0 to 9. The z/OSMF log file resides in the /logs subdirectory directory of the z/OSMF data file system. Your installation specified the z/OSMF data file system on the IZU_DATA_DIR variable when configuring z/OSMF. By default, this is directory /var/zosmf/data.

User response: No action is required.

IZUG386E The command is missing a required argument: *object-name*.

Explanation: The command is missing the indicated argument and thus, cannot be performed.

In the message text:

argument-name
Name of the missing argument.

System programmer response: Enter the command again with all of its required arguments.

User response: No action is required.

IZUG387I Setting *setting-name* **has a value of** *value*.

Explanation: The setting will be set to the indicated value. The current value of the setting in the z/OSMF configuration is shown.

In the message text:

setting-name
Name of the setting

value Value for the setting.

System programmer response: No action is required.

User response: No action is required.

IZUG388I Setting *setting-name* **is not set.**

Explanation: The indicated setting is not currently set in the z/OSMF configuration. z/OSMF will use the setting default.

In the message text:

setting-name
Name of the setting

value Value for the setting.

System programmer response: No action is required.

User response: No action is required.

IZUG397I The -addlink request was processed. To verify that the link was added, check the z/OSMF log file.

Explanation: To add a link to the z/OSMF navigation area, you invoked the izusetup.sh script with the -addlink option. For an indication of the success or failure of this request, see the z/OSMF log file.

System programmer response: No action is required.

User response: To verify that the link was added, check the z/OSMF log file. This file is named IZUG*n*.log, where *n* is a number from 0 to 9. The z/OSMF log file resides in the /logs subdirectory directory of the z/OSMF data file system. Your installation specified the z/OSMF data file system on the IZU_DATA_DIR variable when configuring z/OSMF. By default, this is directory /var/zosmf/data.

To modify or remove a link after it is added, you must use the Links task in the z/OSMF navigation area.

IZUG398I The z/OSMF server is not started. To allow the -addlink request to complete, start the server.

Explanation: The -addlink request cannot complete until you start the z/OSMF server.

System programmer response: Start the z/OSMF server.

After the server is started, see the z/OSMF log file for an indication of the success or failure of this request. The z/OSMF log file is named IZUG*n*.log, where *n* is a number from 0 to 9. The z/OSMF log file resides in the /logs subdirectory directory of the z/OSMF data file system. Your installation specified the z/OSMF data file system on the IZU_DATA_DIR variable when configuring z/OSMF. By default, this is directory /var/zosmf/data.

User response: No action is required.

IZUG399I Successfully copied *source-file-name* **to** *target-file-name***.**

Explanation: The input file was successfully copied to the destination.

In the message text:

source-file-name
Name of the source file

target-file-name
Name of the destination file.

System programmer response: No action is required.

User response: No action is required.

Part 4. Appendixes

© Copyright IBM Corp. 2009, 2016

Appendix A. Security configuration requirements for z/OSMF

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). z/OSMF provides sample jobs and the information in this document to assist your security administrator. Your security administrator can use the sample jobs to create the groups, user IDs, and resource profiles for your z/OSMF configuration. Subsequently, these z/OSMF constructs require additional permissions to a number of existing groups, user IDs, and resources on your system.

This appendix describes the security configuration requirements for z/OSMF. Included are the resource authorizations that are created when your installation runs the IZUSEC job for the core functions, and the IZU*xx*SEC jobs for the optional plug-ins. Also listed are the resource authorizations that your installation must define outside of the configuration process.

The security configuration requirements for z/OSMF are described in the sections that follow. Creating these permissions will require the assistance of your security administrator.

- "Class activations that z/OSMF requires"
- "SAF profile prefix for z/OSMF resources" on page 182
- "User IDs that z/OSMF creates during configuration" on page 183
- "Security groups that z/OSMF creates during configuration" on page 183
- "Resource authorizations for the z/OSMF core functions" on page 183
- "Resource authorizations for hardware compression" on page 188
- "Resource authorizations for hardware cryptography" on page 188
- "Resource authorizations for Common Information Model" on page 189
- "Resource authorizations for Capacity Provisioning Manager" on page 190
- "Resource authorizations for common event adapter (CEA)" on page 191
- "Resource authorizations for the z/OS jobs REST interface" on page 192
- "Resource authorizations for Workload Management" on page 192
- "Resource authorizations for the z/OSMF optional plug-ins" on page 193
- "Default profiles, resource names, and group assignments" on page 197.

Class activations that z/OSMF requires

For a RACF installation, the security classes shown in Table 15 must be active when you configure z/OSMF. Commands for activating the classes (with generic profile checking activated) are included in commented sections in the IZUxxSEC jobs. To have the commands issued when the jobs run, uncomment the sections. Or, ask your security administrator to enter the commands directly, as shown in Table 15.

Table 15. Class activations that z/OSMF requires

Class	Purpose	RACF commands for activating
ACCTNUM	Controls access to the account number used for the procedure for the z/OS data set and file REST interface services, as described in "Updating your system for the z/OS data set and file REST interface" on page 18.	`SETROPTS CLASSACT(ACCTNUM)`
APPL	Controls access to the z/OSMF application domain. This access is required by the z/OSMF started task user ID (IZUSVR, by default).	`SETROPTS CLASSACT(APPL)` `SETROPTS RACLIST(APPL) GENERIC(APPL)`

© Copyright IBM Corp. 2009, 2016

Table 15. Class activations that z/OSMF requires (continued)

Class	Purpose	RACF commands for activating
EJBROLE	Controls the user's ability to connect to the z/OSMF core functions and tasks. z/OSMF defines a resource name for each core function and task.	`SETROPTS CLASSACT(EJBROLE)` `SETROPTS RACLIST(EJBROLE) GENERIC(EJBROLE)`
FACILITY	Controls the user's access to profiles when the user takes some action. This access is required by the z/OSMF started task user ID (IZUSVR, by default). Examples include the profiles used to control privileges in the z/OS UNIX environment.	`SETROPTS CLASSACT(FACILITY)` `SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)`
SERVAUTH	Controls the user's ability to use CEA TSO/E address space services. In z/OSMF, this access is required by: • z/OSMF started task user ID (IZUSVR, by default) • Callers of the z/OS data set and file REST interface services • Users of the ISPF task.	`SETROPTS CLASSACT(SERVAUTH)` `SETROPTS RACLIST(SERVAUTH) GENERIC(SERVAUTH)`
SERVER	Allows the z/OSMF started task user ID to request services from z/OS system components, such as the system authorization facility (SAF), workload management (WLM), and SVCDUMP services.	`SETROPTS CLASSACT(SERVER)` `SETROPTS RACLIST(SERVER) GENERIC(SERVER)`
STARTED	Assigns an identity to the z/OSMF started task during the processing of an MVS START command. By default, the started task runs under the IZUSVR user ID.	`SETROPTS CLASSACT(STARTED)` `SETROPTS RACLIST(STARTED) GENERIC(STARTED)`
TSOPROC	Controls access to the procedure for the z/OS data set and file REST interface services, as described in "Updating your system for the z/OS data set and file REST interface" on page 18.	`SETROPTS CLASSACT(TSOPROC)`
ZMFAPLA	Controls the user's ability to use the z/OSMF core functions and tasks. z/OSMF defines a resource name for each core function and task.	`SETROPTS CLASSACT(ZMFAPLA)` `SETROPTS RACLIST(ZMFAPLA) GENERIC(ZMFAPLA)`

If your installation uses a security management product other than RACF, ask your security administrator to create equivalent commands for your security product.

SAF profile prefix for z/OSMF resources

During the configuration process, your security administrator runs the IZUxxSEC jobs to secure z/OSMF resources. In these jobs, your installation specifies a system authorization facility (SAF) profile prefix to be used for naming z/OSMF resources. The SAF prefix is prepended to the names of z/OSMF resource profiles, and is used in some of the RACF commands contained in the IZUxxSEC jobs.

In the examples in this document, the SAF prefix is shown as `<SAF-prefix>`. By default, the SAF prefix is `IZUDFLT`. If your installation selects to use a different value, substitute the value in the examples.

User IDs that z/OSMF creates during configuration

The IZUSEC job creates a set of product user IDs; see Table 16.

Table 16. User IDs that z/OSMF creates during the configuration process

User ID	Purpose	Default UID	Created by
IZUGUEST	User ID for the z/OSMF server task performing unauthenticated work.	9011	IZUSEC job
IZUSVR	User ID for the z/OSMF started tasks, which are named IZUANG1 and IZUSVR1, by default.	9010	IZUSEC job

Table 16 shows the IBM default values. Your security administrator can specify different user IDs in place of the IBM default values in the IZUSEC job.

Security groups that z/OSMF creates during configuration

The IZUSEC job creates a base set of security groups for your z/OSMF configuration. These groups are necessary for giving users the proper level of access to z/OSMF and z/OS system resources.

Your security team might determine that existing group names would be appropriate for this product. If so, you can use your existing group names in place of the supplied z/OSMF default group names. For example, you might already have a group aligned with administrators; if so, you could use that group, instead of the z/OSMF default group for administrators, IZUADMIN.

Table 17 lists the groups that the IZUSEC job creates. Note that the group names can change, based on the values you provide during the configuration process. Table 17 shows the IBM default values.

Table 17. Security groups that z/OSMF creates during the configuration process

Group	Purpose	Default group ID (GID)	Created by
IZUADMIN	Security group for the z/OSMF administrator role. Any user IDs connected to this group are considered to be z/OSMF administrators.	9003	IZUSEC job
IZUUSER	Security group for the z/OSMF user role.	9004	IZUSEC job
IZUSECAD	Security group for the z/OS security administrator role in z/OSMF.	9006	IZUSEC job
IZUUNGRP	Security group for the z/OSMF unauthenticated user ID.	9012	IZUSEC job

Resource authorizations for the z/OSMF core functions

Table 18 on page 184 describes the access requirements for the z/OSMF core functions. The IZUSEC job includes sample RACF commands for creating these authorizations on your system. Note that these values can change, based on the values you provide during the configuration process. Table 18 on page 184 shows the IBM default values.

Table 18. Security setup requirements for z/OSMF core functions

Resource class	Resource name	Who needs access?	Type of access required	Why
ACCTNUM	IZUACCT	IZUADMIN IZUUSER	READ	Allows callers to access the account number that is used for the procedure for the z/OS data set and file REST interface services, as described in "Updating your system for the z/OS data set and file REST interface" on page 18.
APPL	<*SAF-prefix*>	IZUSVR	READ	Allow access to the z/OSMF application domain.
CERT	DefaultzOSMFCert.<*SAF-prefix*>	Owned by the IZUSVR user ID	N/A	Needed for secure communications between the browser and the z/OSMF server.
CERT	zOSMFCA	N/A	N/A	Certificate authority; needed for secure communications between the browser and the z/OSMF server.
CSFSERV	CSF* profiles	IZUSVR	READ	z/OS Integrated Cryptographic Service Facility (ICSF) callable services. If your installation uses hardware cryptography with ICSF, you must permit the z/OSMF server user ID to these services, as described in "Resource authorizations for hardware cryptography" on page 188.
EJBROLE	<*SAF-prefix*>.IzuManagementFacility.izuUsers	IZUADMIN IZUUSER	READ	Allow a user to log on to z/OSMF and view the Welcome page.
EJBROLE	<*SAF-prefix*>.IzuManagementFacilityHelpApp.izuUsers	IZUADMIN IZUUSER	READ	Allow a user to connect to the z/OSMF online help system.
EJBROLE	<*SAF-prefix*>.IzuManagementFacilityWorkflow.izuUsers	IZUADMIN IZUUSER IZUSECAD	READ	Allow a user to connect to the Workflows task.
EJBROLE	<*SAF-prefix*>.IzuManagementFacilityRestJobs.izuUsers	IZUADMIN IZUUSER	READ	Allow a user to connect to the z/OS jobs REST interface.
EJBROLE	<*SAF-prefix*>.IzuManagementFacilityImportUtility.izuUsers	IZUADMIN IZUUSER	READ	Allow a user to use the Import Manager task to import plug-ins, event types, event handlers, and links into z/OSMF.
FACILITY	BBG.SYNC.<*SAF-prefix*>	IZUSVR	CONTROL	Allow the z/OSMF server to synchronize any RunAs identity with the OS identity.

Table 18. Security setup requirements for z/OSMF core functions (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
FACILITY	BPX.CONSOLE	IZUSVR	READ	Allow the user to filter z/OS UNIX messages. Specifically, this setting suppresses the BPXM023I message prefix from any write-to-operator (WTO) messages that z/OSMF writes to the console.
FACILITY	IRR.DIGTCERT.LIST	IZUSVR	READ	Allow the started task user ID to retrieve the status of the certificate.
FACILITY	IRR.DIGTCERT.LISTRING	IZUSVR	READ	Allow the started task user ID to list and get the certificate keyring.
KEYRING	IZUKeyring.<*SAF-prefix*>	IZUSVR	N/A	Needed for secure communications.
SERVAUTH	CEA.CEATSO.TSOREQUEST	IZUADMIN IZUUSER	READ	Allow the HTTP client applications on your z/OS system to start and manage TSO/E address spaces.
SERVAUTH	CEA.CEATSO.TSOREQUEST	IZUSVR	READ	Allow the z/OSMF server to start and manage TSO/E address space services.
SERVER	BBG.ANGEL	IZUSVR	READ	Allow the z/OSMF server to access the angel process.
SERVER	BBG.AUTHMOD.BBGZSAFM	IZUSVR	READ	Allow the z/OSMF server to access the SAF authorized registry.
SERVER	BBG.AUTHMOD.BBGZSAFM.SAFCRED	IZUSVR	READ	Allow the z/OSMF server to access the SAF authorization services.
SERVER	BBG.AUTHMOD.BBGZSAFM.ZOSWLM	IZUSVR	READ	Allow the z/OSMF server to access the WLM services.
SERVER	BBG.AUTHMOD.BBGZSAFM.TXRRS	IZUSVR	READ	Allow the z/OSMF server to access the transaction services.
SERVER	BBG.AUTHMOD.BBGZSAFM.ZOSDUMP	IZUSVR	READ	Allow the z/OSMF server to access the SVC dump services.
SERVER	BBG.SECCLASS.ZMFAPLA	IZUSVR	READ	Allow the z/OSMF server to authorize checks for the ZMFAPLA class.
SERVER	BBG.SECPFX.<*SAF-prefix*>	IZUSVR	READ	Allow the z/OSMF server to make authentication calls against the APPL-ID.
STARTED	IZUSVR1.*jobname*	IZUADMIN	N/A	Define the started task for the z/OSMF angel process.
STARTED	IZUANG1.*jobname*	IZUADMIN	N/A	Define the started task for the z/OSMF server process.

Table 18. Security setup requirements for z/OSMF core functions (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
TSOPROC	IZUFPROC	IZUADMIN IZUUSER	READ	Allows callers to access the procedure for the z/OS data set and file REST interface services, as described in "Updating your system for the z/OS data set and file REST interface" on page 18.
ZMFAPLA	<*SAF-prefix*>.ZOSMF	IZUADMIN IZUUSER IZUSECAD	READ	Designates the user as a z/OSMF user, rather than a guest user. This authorization is the minimum requirement for allowing a user to do more than log in to z/OSMF and view the Welcome page. Without this authorization, the logged-in user is treated as an authenticated guest. Use the other ZMFAPLA resource names that follow in this table to create specific controls for each core function and task. See Table Notes® 1 and 2.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.ADMINTASKS.APPLINKING	IZUADMIN	READ	Allow a user to access the Application Linking Manager task.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.ADMINTASKS.IMPORTMANAGER	IZUADMIN	READ	Allow a user to access the Import Manager task.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.ADMINTASKS.LINKSTASK	IZUADMIN	READ	Allow a user to access the Links task.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.ADMINTASKS.LOGGER	IZUADMIN	READ	Allow a user to manage the settings that control the behavior and content of the z/OSMF logs. This capability is used only in service situations.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.ADMINTASKS.UI_LOG _MANAGEMENT	IZUADMIN	READ	Allow a user to manage the settings that control the behavior of the user interface (UI) portion of z/OSMF logging. This capability is used only in service situations.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.LINK.*linkName*	IZUADMIN IZUUSER	READ	Allow a user to view an installation-specified link. See Table Notes 3 and 4.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.LINK.SHOPZSERIES	IZUADMIN IZUUSER	READ	Allow a user to view the ShopzSeries web site link.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.LINK.SUPPORT_FOR_Z_OS	IZUADMIN IZUUSER	READ	Allow a user to view the Support for z/OS web site link.

Table 18. Security setup requirements for z/OSMF core functions (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
ZMFAPLA	<*SAF-prefix*>.ZOSMF.LINK.SYSTEM_Z_REDBOOKS	IZUADMIN IZUUSER	READ	Allow a user to view the IBM Redbooks® web site link.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.LINK.WSC_FLASHES _TECHDOCS	IZUADMIN IZUUSER	READ	Allow a user to view the WSC Flashes and Techdocs web site link.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.LINK.Z_OS_BASICS _INFORMATION_CENTER	IZUADMIN IZUUSER	READ	Allow a user to view the z/OS Basic Skills Information Center web site link.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.LINK.Z_OS_HOME_PAGE	IZUADMIN IZUUSER	READ	Allow a user to view the z/OS Home Page web site link.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.LINK.Z_OS_INTERNET_LIBRARY	IZUADMIN IZUUSER	READ	Allow a user to view the z/OS Library web site link.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.NOTIFICATION.MODIFY	IZUADMIN IZUUSER	READ	Allow a user to compose a notification.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.NOTIFICATION.SETTINGS	IZUADMIN IZUUSER	READ	Allow a user to define an mail account for receiving notifications from z/OSMF. This action is performed through the Notification Settings task of z/OSMF.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.NOTIFICATION.SETTINGS.ADMIN	IZUADMIN	READ	Allow a user to manage the z/OSMF notification settings for mobile devices, push services, and SMTP server properties.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.SETTINGS.FTP_SERVERS	IZUADMIN IZUUSER	READ	Allow a user to access the FTP Servers task.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.SETTINGS.FTP_SERVERS.VIEW	IZUADMIN IZUUSER	READ	Allow a user to access the FTP Servers task *View* function.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.SETTINGS.FTP_SERVERS.MODIFY	IZUADMIN	READ	Allow a user to access the z/OSMF Task Settings task *Modify* function.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.SETTINGS.SYSTEMS	IZUADMIN IZUUSER	READ	Allow a user to access the Systems task.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.SETTINGS.SYSTEMS.VIEW	IZUADMIN IZUUSER	READ	Allow a user to access the Systems task *View* function.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.SETTINGS.SYSTEMS.MODIFY	IZUADMIN	READ	Allow a user to access the z/OSMF Task Settings task *Modify* function.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.WORKFLOW.ADMIN	IZUADMIN	READ	Allow a user to change the assigned owner of a workflow.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.WORKFLOW.WORKFLOWS	IZUADMIN IZUSECAD IZUUSER	READ	Allow a user to access the z/OSMF Workflows task. See Table Note 5.

1. User authorizations to functions, tasks, and links are controlled through the system authorization facility (SAF) profile prefix. By default, the SAF prefix is IZUDFLT.
2. Users require READ access to at least the profile <*SAF-prefix*>.ZOSMF to do work in z/OSMF. Without this authorization, the user is treated as an authenticated guest, that is, able to log in to z/OSMF and display the Welcome page, but not able to access the z/OSMF functions and tasks.
3. In a default z/OSMF configuration, all users are granted authority to all links through a wildcarded profile: <*SAF-prefix*>.ZOSMF.LINK.* *
4. You must provide a SAF resource name prefix for any links that you add to z/OSMF. You can control access to specific links by specifying a unique resource name for the link, for example, by including the link name as part of the resource name. For example: `IZUDFLT.ZOSMF.LINK.mylink`

   For information about defining links to z/OSMF, see Chapter 12, "Adding links to z/OSMF," on page 95.
5. A user with access to the Workflows task can access any of the workflows that are displayed in the Workflows task. By default, the z/OSMF defined security groups IZUADMIN, IZUSECAD, and IZUUSER have access to the Workflows task.
6. If your installation uses hardware cryptography with z/OS Integrated Cryptographic Service Facility (ICSF), be aware that services such as CSFRNGL, CSFDSV, CSFOWH, CSFIQF, and others, might be protected through profiles established in your security product. In some cases, z/OSMF uses these services; therefore, you must permit the z/OSMF started task user ID to these profiles. For information, see "Resource authorizations for hardware cryptography."
7. All z/OSMF users must have a TSO segment defined in your installation's security database. Failure to have a TSO segment will cause some z/OSMF functions not to work.

Resource authorizations for hardware compression

If your installation uses hardware compression through IBM z Systems Data Compression (zEDC), the z/OSMF server requires READ access to the FPZ.ACCELERATOR.COMPRESSION resource in the FACILITY class. Otherwise, if this authorization is not in place, the z/OSMF server runs without the use of hardware compression. The system issues an error message, such as the following:

```
XAT1 IZUSVRU  IZUSVR1 RACF ACCESS violation for IZUSVRU:
(READ,NONE) on FACILITY FPZ.ACCELERATOR.COMPRESSION
```

You can ignore the message.

Table 19 shows which permissions must be granted to the z/OSMF server user ID. Commands for the creating the permissions are included in commented sections in the IZUSEC job. To have the commands issued when the job runs, uncomment the sections.

Table 19. Security setup requirements for hardware compression with zEDC

Resource class	Resource name	Who needs access?	Type of access required	Why
FACILITY	FPZ.ACCELERATOR. COMPRESSION	IZUSVR	READ	Enable the z/OSMF server to run with hardware compression.

Resource authorizations for hardware cryptography

If your installation uses hardware cryptography with z/OS Integrated Cryptographic Service Facility (ICSF), the z/OSMF server requires access to the ICSF callable services. shows which permissions must be granted to the z/OSMF server user ID. Commands for the creating the permissions are included in commented sections in the IZUSEC job. To have the commands issued when the job runs, uncomment the sections.

Table 20. Security setup requirements for hardware cryptography with ICSF

Resource class	Resource name	Who needs access?	Type of access required	Why
CSFSERV	CSFIQF	IZUSVR	READ	ICSF query facility callable service.
CSFSERV	CSFENC	IZUSVR	READ	Encipher callable service.
CSFSERV	CSFCVE	IZUSVR	READ	Cryptographic variable encipher callable service.
CSFSERV	CSFDEC	IZUSVR	READ	Decipher callable service.
CSFSERV	CSFSAE	IZUSVR	READ	Symmetric algorithm encipher callable service.
CSFSERV	CSFSAD	IZUSVR	READ	Symmetric algorithm decipher callable service.
CSFSERV	CSFOWH	IZUSVR	READ	One-way hash generate callable service.
CSFSERV	CSFRNG	IZUSVR	READ	Random number generate callable service.
CSFSERV	CSFRNGL	IZUSVR	READ	Random number generate long callable service.
CSFSERV	CSFPKG	IZUSVR	READ	PKA key generate callable service.
CSFSERV	CSFDSG	IZUSVR	READ	Digital signature generate service.
CSFSERV	CSFDSV	IZUSVR	READ	Digital signature verify callable service.
CSFSERV	CSFPKT	IZUSVR	READ	PKA key generate callable service.
CSFSERV	CSFRKL	IZUSVR	READ	Retained key list callable service.
CSFSERV	CSFPKX	IZUSVR	READ	PKA Public Key Extract callable service.
CSFSERV	CSFPKE	IZUSVR	READ	PKA encrypt callable service.
CSFSERV	CSFPKD	IZUSVR	READ	PKA decrypt callable service.
CSFSERV	CSFPKI	IZUSVR	READ	PKA key import callable service.
CSFSERV	CSFCKM	IZUSVR	READ	Multiple clear key import callable service.
CSFSERV	CSFKGN	IZUSVR	READ	Multiple clear key import callable service.
CSFSERV	CSFEDH	IZUSVR	READ	ECC Diffie-Hellman callable service.

Resource authorizations for Common Information Model

If your z/OSMF configuration includes tasks that use the Common Information Model (CIM) server on the host z/OS system, users of the plug-ins require the proper level of access to CIM server resources.

These authorizations are required for using any of the following optional plug-ins or core functions:
- Capacity Provisioning
- Incident Log
- Workload Management
- The asynchronous job notifications function of z/OSMF, which is described in Chapter 11, "Configuring your system for asynchronous job notifications," on page 85.

CIM includes the CFZSEC job to help you create these authorizations. See the chapter on CIM server quick setup and verification in *z/OS Common Information Model User's Guide*. IBM supplies the CFZSEC job in SYS1.SAMPLIB. If your installation does not plan to run the CFZSEC job, ensure that z/OSMF users, and, if configuring the Workload Management plug-in, the z/OSMF server user ID, have UPDATE access to the CIMSERV profile in the WBEM class. If necessary, refresh the WBEM class.

For more information about CIM authorization requirements, see "Reviewing your CIM server setup" on page 201.

Table 21 on page 190 lists the CIM security groups that are required for the optional plug-ins.

Table 21. CIM groups that might be required for the optional plug-ins

Group	Purpose	Default group ID (GID)	Created by
CFZADMGP	Security group for the CIM administrator role.	9502	Member CFZSEC in SYS1.SAMPLIB.
CFZUSRGP	Security group for the CIM user role. This group grants a user access to all resources that are managed through CIM. Depending on how granular you want to control user access to CIM, your installation might have created additional groups to allow access to only a subset of resources managed through CIM.	9503	Member CFZSEC in SYS1.SAMPLIB.

With the IZUAUTH job, your security administrator can supply the names of the CIM groups, based on your selection of optional plug-ins. These values include the names of the CIM administrators group (by default, CFZADMGP) and the CIM users group (by default, CFZUSRGP). The IZUAUTH job contains commands for connecting users to the groups and thus, depend on the groups to exist.

Resource authorizations for Capacity Provisioning Manager

If your z/OSMF configuration includes the Capacity Provisioning plug-in, users of the plug-in must be defined and authorized for all resources accessed by the Provisioning Manager. IBM provides the CPOSEC1 and CPOSEC2 jobs in SYS1.SAMPLIB to help you create these authorizations when you set up a Capacity Provisioning domain. For more information, see the topic on setting up a Capacity Provisioning domain in *z/OS MVS Capacity Provisioning User's Guide*.

Table 22 lists the default values for the Provisioning Manager. Note that your installation might have selected to use different values for these settings.

Table 22. Name information for a Capacity Provisioning domain

Provisioning Manager setting	Default value
Domain name	DOMAIN1
Started task procedure name	CPOSERV
High-level qualifier for runtime data set	CPO
Provisioning Manager user	CPOSRV

With the IZUCPSEC job, your security administrator can supply the names of the security groups that your installation has created for authorizing users to the Provisioning Manager on your system. The IZUAUTH job contains commands for connecting users to the groups and thus, depend on the groups to exist.

Table 23 lists the security groups that are required for the Capacity Provisioning plug-in.

Table 23. Security groups required for the Capacity Provisioning plug-in

Group	Purpose	Default group ID (GID)	Created by
CPOCTRL	Security group for users of the Capacity Provisioning task *Edit* function.	None; your installation must specify a GID for this group.	Member CPOSEC1 in SYS1.SAMPLIB.

Table 23. Security groups required for the Capacity Provisioning plug-in (continued)

Group	Purpose	Default group ID (GID)	Created by
CPOQUERY	Security group for users of the Capacity Provisioning task *View* function.	None; your installation must specify a GID for this group.	Member CPOSEC1 in SYS1.SAMPLIB.

Resource authorizations for common event adapter (CEA)

If your z/OSMF configuration includes tasks that use the common event adapter (CEA) component on the z/OS host system, users of the plug-ins require the proper level of access to CEA resources. IBM provides the CEASEC job in SYS1.SAMPLIB to help you create these authorizations.

These authorizations are needed if you plan to use one or more of the following z/OSMF tasks:
- Incident Log
- ISPF.

CEA has security profiles in the SERVAUTH class for protecting different portions of its processing. When you run the IZUILSEC job, you permit the z/OSMF groups to the CEA resources.

For more information, see the topic on customizing for CEA in *z/OS Planning for Installation*.

Resource authorizations for the z/OS data set and file REST interface

The z/OS data set and file REST interface requires access to local resources on your z/OS system. Table 24 describes the security requirements for the z/OS data set and file REST interface.

For information about the z/OS data set and file REST interface services, see *IBM z/OS Management Facility Programming Guide*.

Table 24. Security setup requirements for the z/OS data set and file REST interface

Resource class	Resource name	Who needs access?	Type of access required	Why
ACCTNUM	IZUACCT	IZUADMIN IZUUSER	READ	Allows callers to access the account number that is used for the procedure for the z/OS data set and file REST interface services, as described in "Updating your system for the z/OS data set and file REST interface" on page 18.
SERVAUTH	CEA.CEATSO.TSOREQUEST	IZUADMIN IZUUSER	READ	Allows callers to access the CEA TSO/E address space services. This setting allows HTTP client applications on your z/OS system to start and manage TSO/E address spaces.
SERVAUTH	CEA.CEATSO.TSOREQUEST	IZUSVR	READ	Allows the z/OSMF server to access the CEA TSO/E address space services. This setting allows the z/OSMF server to start and manage TSO/E address space services.
TSOPROC	IZUFPROC	IZUADMIN IZUUSER	READ	Allows callers to access the procedure for the z/OS data set and file REST interface services, as described in "Updating your system for the z/OS data set and file REST interface" on page 18.

Resource authorizations for the z/OS jobs REST interface

The z/OS jobs REST interface requires access to local resources on your z/OS system. Table 25 describes the security requirements for the z/OS jobs REST interface. These authorizations allow the CIM server to interact with the common event adapter (CEA) component. CIM includes the CFZSEC job to help you create these authorizations.

Table 25. Security setup requirements for the z/OS jobs REST interface

Resource class	Resource name	Who needs access?	Type of access required	Why
SERVAUTH	CEA.CONNECT	CFZSRV	READ	If your installation uses the z/OS jobs REST interface, this setting is needed for interactions with the common event adapter (CEA) component.
SERVAUTH	CEA.SUBSCRIBE.*	CFZSRV	READ	If your installation uses the z/OS jobs REST interface, this setting allows HTTP client applications on your z/OS system to receive asynchronous job notifications.
SERVAUTH	CEA.SUBSCRIBE.ENF_0078*	CFZSRV	READ	If your installation uses the z/OS jobs REST interface, this setting allows HTTP client applications on your z/OS system to receive asynchronous job notifications.

For programs that use the z/OS jobs REST interface services to perform job modify operations, the caller's user ID must be authorized to the appropriate resources in the JESJOBS class, as shown in Table 26.

Table 26. JESJOBS class authorizations needed for performing job modify operations

Operation	JESJOBS resource	Access required
Hold a job	HOLD.nodename.userid.jobname	UPDATE
Release a job	RELEASE.nodename.userid.jobname	UPDATE
Change the job class	MODIFY.nodename.userid.jobname	UPDATE
Cancel a job	CANCEL.nodename.userid.jobname	ALTER
Delete a job (cancel a job and purge its output)	CANCEL.nodename.userid.jobname	ALTER

For information about the z/OS jobs REST interface services, see *IBM z/OS Management Facility Programming Guide*. For information about JESJOBS class, see *z/OS Security Server RACF Security Administrator's Guide*.

If run asynchronously, the z/OS jobs REST interface services also require that the caller's user ID be authorized to the CIM server and permitted to the JES2-JES3Jobs CIM provider. CIM includes 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 *z/OS Common Information Model User's Guide*. IBM supplies the CFZSEC job in SYS1.SAMPLIB.

Resource authorizations for Workload Management

If your z/OSMF configuration includes the Workload Management plug-in, users require the proper level of access to workload management (WLM) resources on your system. This access allow a user to view or update the WLM policies.

With the IZUWMSEC job, your security administrator can supply the name of the WLM security group that your installation uses for authorizing users to the z/OS Workload Management component on your system. The IZUAUTH job contains commands for connecting users to the group and thus, depend on the groups to exist.

Table 27 describes the security group that is required for the Workload Management plug-in.

Table 27. Security group required for the Workload Management plug-in

Group	Purpose	Default group ID (GID)	Created by
WLMGRP	Security group for users of the Workload Management task.	9600	ADDGROUP command or an equivalent security command for creating user groups.

Resource authorizations for the z/OSMF optional plug-ins

The z/OSMF optional plug-ins require access to local resources on your z/OS system. Table 28 describes the security requirements that are required for the z/OSMF optional plug-ins. The IZUxxSEC jobs include sample RACF commands for creating these authorizations.

Note that these values can change, based on the values you provide. The values in Table 28 are based on the defaults. If your installation uses a different value, such as a different group name, the generated values can change.

Table 28. Security setup requirements for the z/OSMF optional plug-ins

Resource class	Resource name	Who needs access?	Type of access required	Why
Capacity Provisioning. The following access controls must be set for the Capacity Provisioning plug-in. For additional authorizations, see Table Notes 1 and 2.				
EJBROLE	<*SAF-prefix*>.IzuManagementFacilityCapacityProvisioning.izuUsers	IZUADMIN IZUUSER	READ	Allow a user to connect to the Capacity Provisioning task.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT	IZUADMIN	READ	Allow a user to access the Capacity Provisioning task *Edit* function.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT.DOMAIN	IZUADMIN	READ	Allow a user to use the Capacity Provisioning task *Edit* function to edit a Capacity Provisioning domain.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT.POLICY	IZUADMIN	READ	Allow a user to use the Capacity Provisioning task *Edit* function to edit a Capacity Provisioning policy.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.VIEW	IZUADMIN IZUUSER	READ	Allow a user to access the Capacity Provisioning task *View* function.
Configuration Assistant. The following access controls must be set for the Configuration Assistant plug-in.				

Table 28. Security setup requirements for the z/OSMF optional plug-ins (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
EJBROLE	<*SAF-prefix*>.IzuConfigurationAssistant.izuUsers	IZUADMIN IZUUSER	READ	Allow a user to connect to the Configuration Assistant task.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.CONFIGURATION_ ASSISTANT.CONFIGURATION_ASSISTANT	IZUUSER	READ	Allow a user to access the Configuration Assistant task.
Incident Log. The following access controls must be set for the Incident Log plug-in. For additional authorizations, see Table Notes 1 and 3.				
ALIAS	CEA	N/A	N/A	If your installation has a user catalog set-up instead of using the master catalog, you may need to define CEA alias to the user catalog.
DATASET	CEA.*	IZUADMIN IZUUSER	ALTER	Allow the user to create data sets using the CEA high level qualifier (HLQ).
DATASET	*your_master_catalog*	IZUADMIN IZUUSER	UPDATE	If your installation has master catalog setup, you might need to permit a user to the master catalog data set class.
EJBROLE	<*SAF-prefix*>.IzuManagementFacilityIncidentLog.izuUsers	IZUADMIN IZUUSER	READ	Allow a user to connect to the Incident Log task.
JESSPOOL	*your_system_name*.+MASTER+.SYSLOG.*.*	CEA	READ	If your installation is using the system log (SYSLOG) as the source for diagnostic log snapshots, the CEA user ID requires READ access to the JESSPOOL class. This authorization allows the JES subsystem to access SYSLOG on behalf of the common event adapter (CEA) component.
SERVAUTH	CEA.CEADOCONSOLECMD	IZUADMIN IZUUSER	READ	Allow the calling program to issue operator commands to accomplish its function.
SERVAUTH	CEA.CEADOCMD	IZUADMIN IZUUSER	READ	Allow a user to cancel the FTP job.

Table 28. Security setup requirements for the z/OSMF optional plug-ins (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
SERVAUTH	CEA.CEAGETPS	IZUADMIN IZUUSER	READ	Allow a user to obtain information about the FTP job.
SERVAUTH	CEA.CEAPDWB.CEACHECKSTATUS	IZUADMIN IZUUSER	READ	Allow a user to check status and return incident information.
SERVAUTH	CEA.CEAPDWB.CEADELETEINCIDENT	IZUADMIN IZUUSER	READ	Allow a user to delete selected incidents, including the dumps, all diagnostic snapshot files and the corresponding sysplex dump directory entry.
SERVAUTH	CEA.CEAPDWB.CEAGETINCIDENT	IZUADMIN IZUUSER	READ	Allow a user to obtain data associated with a specific incident.
SERVAUTH	CEA.CEAPDWB.CEAGETINCIDENTCOLLECTION	IZUADMIN IZUUSER	READ	Allow a user to obtain collection of incident data for all incidents matching a filter.
SERVAUTH	CEA.CEAPDWB.CEAPREPAREINCIDENT	IZUADMIN IZUUSER	READ	Allow a user to prepare data for FTP (locate and compress/terse).
SERVAUTH	CEA.CEAPDWB.CEASETINCIDENTINFO	IZUADMIN IZUUSER	READ	Allow a user to set information associated with the incident, such as the Notes field.
SERVAUTH	CEA.CEAPDWB.CEASETPROBLEMTRACKINGNUMBER	IZUADMIN IZUUSER	READ	Allow a user to set a problem ID, such as a PMR number, or problem management tracking ID.
SERVAUTH	CEA.CEAPDWB.CEAUNSUPPRESSDUMP	IZUADMIN IZUUSER	READ	Allow user to allow a dump that has been marked for suppression through DAE to be taken.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.INCIDENT_LOG.INCIDENT_LOG	IZUADMIN IZUUSER	READ	Allow a user to access the Incident Log task.
ISPF. The following access controls must be set for the ISPF plug-in. For additional authorizations, see Table Note 3.				
EJBROLE	*<SAF-prefix>*.IzuManagementFacilityISPF.izuUsers	IZUADMIN IZUUSER	READ	Allow a user to connect to the ISPF task.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.ISPF.ISPF	IZUADMIN IZUUSER	READ	Allow a user to access the ISPF task.
Resource Monitoring. The following access controls must be set for the Resource Monitoring plug-in.				

Table 28. Security setup requirements for the z/OSMF optional plug-ins (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
EJBROLE	<*SAF-prefix*>.IzuManagementFacilityResourceMonitoring.izuUsers	IZUADMIN IZUUSER	READ	Allow a user to connect to the Resource Monitoring and System Status tasks.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.RESOURCE_MONITORING.PERFDESKS	IZUADMIN IZUUSER	READ	Allow a user to access the Resource Monitoring task.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.RESOURCE_MONITORING.OVERVIEW	IZUADMIN IZUUSER	READ	Allow a user to access the System Status task.
Software Deployment. The following access controls must be set for the Software Deployment plug-in.				
EJBROLE	<*SAF-prefix*>.IzuManagementFacilitySoftwareDeployment.izuUsers	IZUADMIN IZUUSER	READ	Allow a user to connect to the Deployment task.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT	IZUADMIN IZUUSER	READ	Allow a user to access the Deployment task.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.*objectType.objectSuffix* For information about possible values for *objectType* and *objectSuffix*, see "Creating access controls for the Software Management task" on page 227.	IZUADMIN IZUUSER	CONTROL	Allow a user to access the Deployment task objects.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.PRODUCT _INFO_FILE.RETRIEVE	IZUADMIN	READ	Allow a user to access the Deployment task *Product Information File Retrieve* function.
Workload Management. The following access controls must be set for the Workload Management plug-in. For additional authorizations, see Table Note 1.				
EJBROLE	<*SAF-prefix*>.IzuManagementFacilityWorkloadManagement.izuUsers	IZUADMIN IZUUSER	READ	Allow a user to connect to the Workload Management task.
FACILITY	MVSADMIN.WLM.POLICY	IZUSVR	READ	Allow the z/OSMF server to access the WLM policies.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.VIEW	IZUADMIN IZUUSER	READ	Allow a user to access the Workload Management *View* function.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.MODIFY	IZUADMIN	READ	Allow a user to access the Workload Management *Modify* function.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.INSTALL	IZUADMIN	READ	Allow a user to access the Workload Management *Install* function.

Table Notes:

1. This plug-in requires the CIM server; thus, you must also create the authorizations described in "Resource authorizations for Common Information Model" on page 189.

2. Users of this plug-in must be authorized for resources that are accessed by the Provisioning Manager. IBM provides the CPOSEC1 and CPOSEC2 jobs in SYS1.SAMPLIB to help you create these authorizations. For more information, see the topic on setting up a Capacity Provisioning domain in *z/OS MVS Capacity Provisioning User's Guide*.
3. Users of this plug-in must be authorized for resources that are accessed by the common event adapter (CEA) component of z/OS. IBM provides the CEASEC job in SYS1.SAMPLIB to help you create these authorizations. See "Resource authorizations for common event adapter (CEA)" on page 191.

Default profiles, resource names, and group assignments

For your reference, Table 29 on page 198 shows the relationship of profiles, resource names, and group assignments for z/OSMF. Resource profiles in z/OSMF are qualified by a SAF prefix, which is shown as `<SAF-prefix>` in Table 29 on page 198. By default, the prefix is `IZUDFLT`.

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 29. Default profiles, resource names, and group assignments for z/OSMF

Resource profile	Resource name	Protects	Permitted groups
<*SAF-prefix*>.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.VIEW	ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.VIEW	Capacity Provisioning *View* function	IZUADMIN IZUUSER
<*SAF-prefix*>.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT.**	ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT	Capacity Provisioning *Edit* function	IZUADMIN
<*SAF-prefix*>.ZOSMF.CONFIGURATION_ASSISTANT .**	ZOSMF.CONFIGURATION_ASSISTANT.CONFIGURATION_ASSISTANT	Configuration Assistant task	IZUADMIN IZUUSER
<*SAF-prefix*>.ZOSMF.SOFTWARE_DEPLOYMENT.**	ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT	Software Management task	IZUADMIN IZUUSER
<*SAF-prefix*>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.**	ZOSMF.SOFTWARE_DEPLOYMENT.DATA.*objectType.objectSuffix* For information about possible values for *objectType* and *objectSuffix*, see "Creating access controls for the Software Management task" on page 227.	Software Management task objects	IZUADMIN IZUUSER
<*SAF-prefix*>.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.PRODUCT_INFO_FILE.*	ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.PRODUCT_INFO_FILE.RETRIEVE	Software Management *Product Information File Retrieve* function	IZUADMIN
<*SAF-prefix*>.ZOSMF.INCIDENT_LOG .**	ZOSMF.INCIDENT_LOG.INCIDENT_LOG	Incident Log task	IZUADMIN IZUUSER
<*SAF-prefix*>.ZOSMF.ISPF.**	ZOSMF.ISPF.ISPF	ISPF task	IZUADMIN IZUUSER
<*SAF-prefix*>.ZOSMF.RESOURCE_MONITORING.**	ZOSMF.RESOURCE_MONITORING.PERFDESKS	Resource Monitoring task	IZUADMIN IZUUSER
<*SAF-prefix*>.ZOSMF.RESOURCE_MONITORING.**	ZOSMF.RESOURCE_MONITORING.OVERVIEW	System Status task	IZUADMIN IZUUSER
<*SAF-prefix*>.ZOSMF.WORKLOAD_MANAGEMENT.VIEW	ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.VIEW	Workload Management *View* function	IZUADMIN IZUUSER
<*SAF-prefix*>.ZOSMF.WORKLOAD_MANAGEMENT.MODIFY	ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.MODIFY	Workload Management *Modify* function	IZUADMIN
<*SAF-prefix*>.ZOSMF.WORKLOAD_MANAGEMENT.INSTALL	ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.INSTALL	Workload Management *Install* function	IZUADMIN
<*SAF-prefix*>.ZOSMF.LINK.**	ZOSMF.LINK.SHOPZSERIES ZOSMF.LINK.SUPPORT_FOR_Z_OS ZOSMF.LINK.SYSTEM_Z_REDBOOKS ZOSMF.LINK.WSC_FLASHES_TECHDOCS ZOSMF.LINK.Z_OS_BASICS_INFORMATION_CENTER ZOSMF.LINK.Z_OS_HOME_PAGE ZOSMF.LINK.Z_OS_INTERNET_LIBRARY	Links task	IZUADMIN IZUUSER
	<*SAF-prefix*>.ZOSMF.LINK.*linkName* To control access to an installation-supplied link, include the link name (*linkName*) in the resource name, as shown here. For information about defining links to z/OSMF, see Chapter 12, "Adding links to z/OSMF," on page 95.	Links task	IZUADMIN IZUUSER
<*SAF-prefix*>.ZOSMF.ADMINTASKS.**	ZOSMF.ADMINTASKS.APPLINKING ZOSMF.ADMINTASKS.LINKSTASK ZOSMF.ADMINTASKS.LOGGER ZOSMF.ADMINTASKS.UI_LOG_MANAGEMENT	z/OSMF Administration tasks	IZUADMIN

Table 29. Default profiles, resource names, and group assignments for z/OSMF (continued)

Resource profile	Resource name	Protects	Permitted groups
<*SAF-prefix*>.ZOSMF.SETTINGS.FTP_SERVERS*	ZOSMF.SETTINGS.FTP_SERVERS	z/OSMF Settings FTP Servers task	IZUADMIN IZUUSER
	ZOSMF.SETTINGS.FTP_SERVERS.VIEW	z/OSMF Settings FTP Servers *View* function	IZUADMIN IZUUSER
	ZOSMF.SETTINGS.FTP_SERVERS.MODIFY	z/OSMF Settings FTP Servers*Modify* function	IZUADMIN
<*SAF-prefix*>.ZOSMF.SETTINGS.SYSTEMS*	ZOSMF.SETTINGS.SYSTEMS	z/OSMF Settings Systems task	IZUADMIN IZUUSER
	ZOSMF.SETTINGS.SYSTEMS.VIEW	z/OSMF Settings Systems *View* function	IZUADMIN IZUUSER
	ZOSMF.SETTINGS.SYSTEMS.MODIFY	z/OSMF Settings Systems *Modify* function	IZUADMIN
<*SAF-prefix*>.ZOSMF.WORKFLOW.*	ZOSMF.WORKFLOW.WORKFLOWS	Workflows task.	IZUADMIN IZUSECAD IZUUSER

Appendix B. Customizing your z/OS system for the z/OSMF plug-ins

This appendix describes the z/OS system customization steps that are required for enabling the optional plug-ins in z/OSMF. Which steps you will need to complete depend on which plug-ins you plan to deploy on your system.

Review the system setup requirements for each plug-in, as described in this topic. When doing the work, you might find it easier to start with plug-ins that require little or no system customization, such as Configuration Assistant or ISPF, and then progress to plug-ins with more extensive requirements, such as Incident Log.

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 following topics:
- "Using FTP in your network"
- "Reviewing your CIM server setup"
- "Updating z/OS for the Capacity Provisioning plug-in" on page 203
- "Updating z/OS for the Configuration Assistant plug-in" on page 205
- "Updating z/OS for the Incident Log plug-in" on page 205
- "Updating z/OS for the ISPF plug-in" on page 223
- "Updating z/OS for the Resource Monitoring Plug-in" on page 224
- "Updating z/OS for the Software Deployment plug-in" on page 227
- "Updating z/OS for the Workload Management plug-in" on page 235.

Using FTP in your network

Some z/OSMF tasks 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 Task Settings task.

Reviewing your CIM server setup

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

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.

Ensure that the administrator role 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 group has the proper level of access to CIM server resources. In effect, the z/OSMF administrator 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*. After the job is run, your security administrator must connect the z/OSMF administrator user IDs to the CFZADMGP group.

© Copyright IBM Corp. 2009, 2016

If your installation does not plan to run the CFZSEC job, your security administrator can perform these tasks manually, as follows:

1. Grant the z/OSMF administrator group UPDATE access to the CIMSERV profile in the WBEM class. 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 z/OSMF administrator user ID 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 group. 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 group and authorize it. If necessary, refresh the SURROGAT class.

These updates should be made before logging in to z/OSMF as the administrator, as described in "Step 5: Log into z/OSMF" on page 36.

Customizing the administrator role for running CIM commands

The CIM server commands are UNIX style programs that run in the z/OS UNIX shell. To ensure that the z/OSMF administrator can use the CIM commands, verify that the administrator role is properly set up for the z/OS UNIX shell environment, as described in this topic.

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 your installation used the job CFZRCUST from the installation SAMPLIB to customize the file systems and directories used by the CIM server, this setup is already done.

If your installation did not run the CFZRCUST job, you can perform this setup manually. Copy the contents of the **profile.add** file to the .profile file in the home directory of the z/OSMF administrator user ID. Modify the appropriate settings if you do not plan to use the defaults. The .profile file should be owned by the z/OSMF administrator; this person requires read-write-execute access to the file.

Or, you can use the following command to include the CIM profile settings for the duration of a shell session: `. /usr/lpp/wbem/install/profile.add`

Here, you must enter this command whenever the z/OSMF administrator logs into the z/OS UNIX shell to run CIM command-line utilities.

Ensure that the CIM server is started

If your configuration includes a plug-in that uses the CIM server, ensure that the CIM server is active on your system when using z/OSMF. 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* to start it. 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.

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*.

Updating z/OS for the Capacity Provisioning plug-in

If you have selected to configure the Capacity Provisioning plug-in, you might have system customization to perform, as described in this topic. These actions are needed to ensure that users of the Capacity Provisioning task have access to the capacity provisioning domain.

This topic contains the following information:

- "System customization for the Capacity Provisioning task"
- "Enabling PassTicket creation for Capacity Provisioning task users."

System customization for the Capacity Provisioning task

Table 30 describes the z/OS system changes that are required or recommended. Some of this work might already be done on your system, or might not be applicable. If so, you can skip the particular setup action.

Table 30. z/OS setup actions for the Capacity Provisioning task

	z/OS setup action	**Check when task is completed**
1	Ensure that a Capacity Provisioning Domain is implemented in your enterprise. For information about setting up and implementing Capacity Provisioning, see *z/OS MVS Capacity Provisioning User's Guide*.	
2	Ensure that potential users of the Capacity Provisioning task are defined to the Provisioning Manager query security group on the provisioning system (by default, the CPOQUERY group). On a system with RACF, you can query the users in a group through the `LISTGRP` command. For example: `LISTGRP CPOQUERY`	
3	Determine whether the CIM server on the provisioning system is currently configured to use PassTicket authentication. If so, proceed to Step 4. Otherwise, you must perform this set-up, following the steps described in *z/OS MVS Capacity Provisioning User's Guide*.	

4	Determine whether the Provisioning Manager is running in the same security domain as the z/OSMF system. If so, grant the z/OSMF started task user ID at least UPDATE access authority to the profile IRRPTAUTH.CFZAPPL.* in the PTKTDATA class. On a system with RACF, you can create this authorization through the `PERMIT` command.
	
	For example:
	`PERMIT IRRPTAUTH.CFZAPPL.* CLASS(PTKTDATA)`
	`ID(passticket_creator_userid) ACCESS(UPDATE)`
	`SETROPTS RACLIST(PTKTDATA) REFRESH`
	
	where `passticket_creator_userid` is the z/OSMF started task user ID. By default, this is IZUSVR.
	
	Otherwise, if the Provisioning Manager is running in a different security domain, follow the steps in "Enabling PassTicket creation for Capacity Provisioning task users."	

Enabling PassTicket creation for Capacity Provisioning task users

Use the following procedure to ensure that Capacity Provisioning task users on the z/OSMF system can access the CIM server on the provisioning system.

About this task

In this procedure, you will do the following:

- Ensure that PassTickets are enabled for every Capacity Provisioning task user who might require access to the provisioning system
- Verify that the z/OSMF started task user ID is authorized to generate PassTickets.

The 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.

Understand that PassTicket setup must be done on both systems, as follows:

- System on which the PassTicket is to be verified (the provisioning system). This work is assumed to be done; otherwise, you must set up authentication on the provisioning system, as described in *z/OS MVS Capacity Provisioning User's Guide*.
- System on which the PassTicket is to be generated (the z/OSMF system), which is described here.

For more information about PassTickets, see *z/OS Security Server RACF Security Administrator's Guide*.

Procedure

1. On the z/OSMF system, activate the security class PTKTDATA, if this class is not already active. If you plan to use generic profiles for the PTKTDATA class, include the GENERIC option on the **SETROPTS** command, for example:

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

2. Define the profile CFZAPPL 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 provisioning system). 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. If a common cryptographic architecture (CCA) product is installed on the systems with the secured signon function, you can encrypt the secured signon key using a KEYENCRYPTED value. If not, you can mask the secured signon key by using the SSIGNON option and a 64-bit KEYMASKED value, as shown in the preceding example. If you plan to use a KEYENCRYPTED value, note that additional authorizations are required, such as access to security profiles in the CSFSERV class, and additional profiles for PassTicket creation and PassTicket validation. Be sure to review the RACF setup requirements for the CCA product.

3. To enable PassTicket creation for Capacity Provisioning task users, define the profile IRRPTAUTH.CFZAPPL.* in the PTKTDATA class, set the universal access authority to NONE. 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 z/OSMF started task user ID. By default, this is IZUSVR.

4. Grant the z/OSMF started task user ID permission to generate PassTickets for users. For example:

   ```
   PERMIT IRRPTAUTH.CFZAPPL.* CLASS(PTKTDATA) ID(passticket_creator_userid)
   ACCESS(UPDATE)
   SETROPTS RACLIST(PTKTDATA) REFRESH
   ```

where *passticket_creator_userid* is the z/OSMF started task user ID. By default, this is `IZUSVR`.

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

Updating z/OS for the Configuration Assistant plug-in

If your installation uses the Windows desktop version of Configuration Assistant, you can optionally transfer your existing configuration data into the z/OSMF environment.

About this task

The Windows desktop version of Configuration Assistant for z/OS Communications Server allows you to keep your configuration data in a file called the *backing store file*. You can manage separate sets of configuration information by keeping them in separate backing store files. You can store one or more backing store files on your local drive, a LAN drive, or on z/OS.

If you want to continue using your existing data in z/OSMF, you can use the following procedure to transfer your backing store files into the z/OSMF environment.

Procedure

1. Determine the location of your existing backing store files. The files 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 file location.
2. If the backing store files reside on your Windows local drive or LAN drive, copy the files to the z/OS system on which z/OSMF is running. A backing store file is binary and can be placed in a data set or in the z/OS UNIX file system.
3. From the Configuration Assistant task in z/OSMF, use the **Open** > **Tools** > **Manage Backing Stores** > **Actions** > **Transfer** option to perform the transfer.
4. Enter the name and path of your existing backing store files on z/OS. This required value can be a data set or a z/OS UNIX file.
5. Click **Transfer** to copy the backing store files into z/OSMF.

What to do next

You have now transferred the backing store files into the z/OSMF environment. This data can be used in all subsequent Configuration Assistant task 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.

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 the sections that follow.

System components used by the Incident Log task

As shown in Figure 41 on page 206, a number of base z/OS functions are involved when the Incident Log task is used to manage diagnostic data for your system.

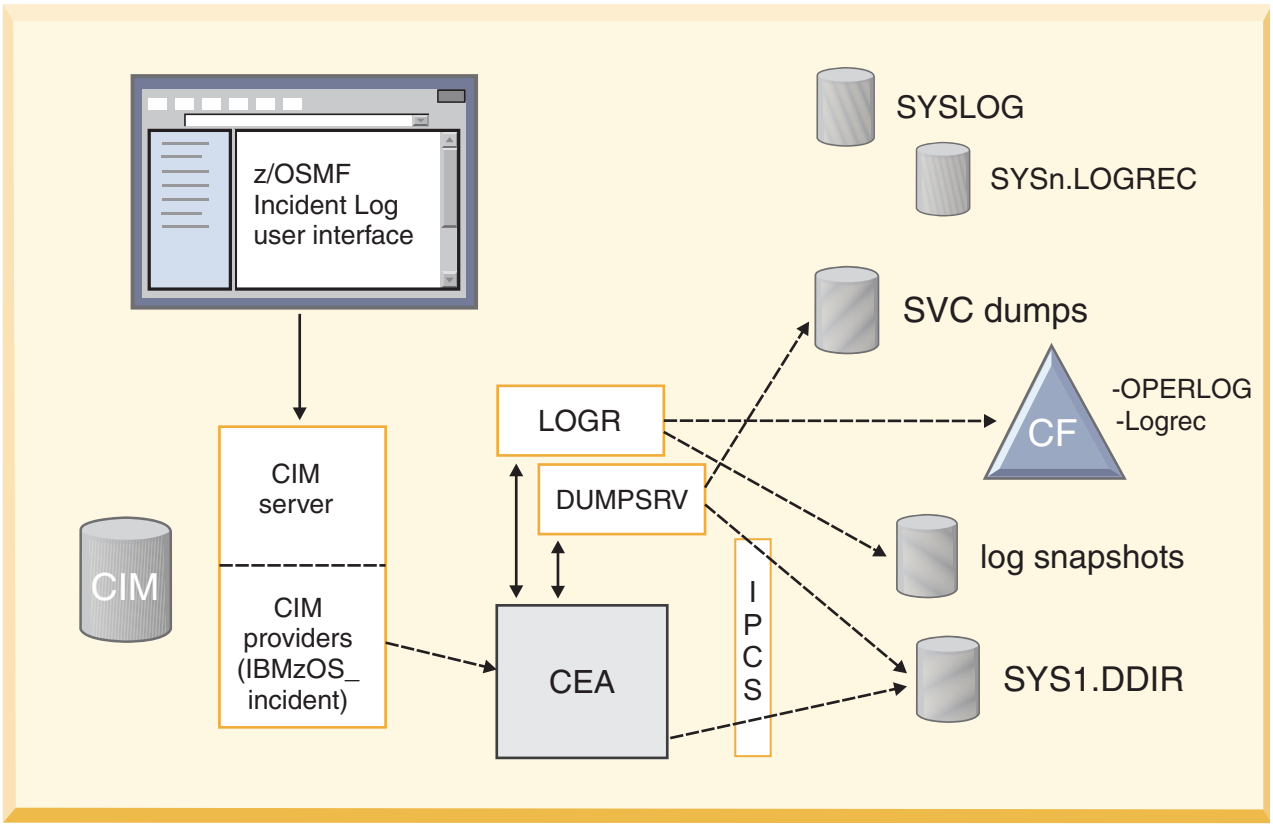


Figure 41. z/OS components that are used in Incident Log task processing

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* function of the Incident Log task
- Environmental Record Editing and Printing (EREP) program for formating 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 (`1D0`)
- 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 C, "Common event adapter (CEA) reason codes," on page 239.

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 31 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 31.

Table 31. z/OS setup actions for the Incident Log task

	z/OS setup action	**Where described**	**Check when task is completed**
1	Ensure that the Common Information Model (CIM) server is configured on your system, including security authorizations and file system customization.	CIM includes jobs to help you perform these tasks (CFZSEC and CFZRCUST). See the chapter on CIM server quick setup and verification in *z/OS Common Information Model User's Guide*.	

Table 31. z/OS setup actions for the Incident Log task (continued)

	z/OS setup action	Where described	Check when task is completed
2	Define a couple data set for the system logger component of z/OS.	See "Defining a couple data set for system logger."	
3	Enable message log snapshots on the host system, or, optionally, on a sysplex-wide basis.	See the following topics: • "Setup considerations for log snapshots" on page 210 • "Enabling the operations log (OPERLOG)" on page 211 • "Defining and activating the LOGREC log stream" on page 213 • "Defining diagnostic snapshot log streams" on page 214 • "Enabling SYSLOG for diagnostic snapshots" on page 215.	
4	Enable error log snapshots on the host system, or, optionally, on a sysplex-wide basis.	See the following topics: • "Setup considerations for log snapshots" on page 210 • "Enabling the operations log (OPERLOG)" on page 211 • "Defining and activating the LOGREC log stream" on page 213 • "Defining diagnostic snapshot log streams" on page 214 • "Enabling SYSLOG for diagnostic snapshots" on page 215.	
5	Set up and configure automatic dump data set allocation (auto-dump).	See "Configuring automatic dump data set allocation" on page 215.	
6	Configure dump analysis and elimination (DAE) to suppress duplicate SVC dumps and use a sysplex-wide scope.	See "Configuring dump analysis and elimination" on page 216.	
7	Verify that a sysplex dump directory is defined for your system. If not, create a sysplex dump directory.	See "Creating the sysplex dump directory" on page 217.	
8	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.	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 "Ensure that common event adapter (CEA) is configured and active" on page 219.	
9	Ensure that System REXX (SYSREXX) is set up and active on your system.	See "Ensuring that System REXX is set up and active" on page 221.	
10	If your installation has chosen to rename a dump data set, ensure that the data set name in the sysplex dump directory is correct.	See "Ensuring that dump data set names are correct" on page 222.	

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:

```
D XCF,COUPLE,TYPE=LOGR
```

Figure 42 shows the expected results:

```
IXC358I  15.15.26  DISPLAY XCF 038
LOGR COUPLE DATA SETS
PRIMARY    DSN: UTCXCF.SVPLEX6.LOGRR13.PRI
           VOLSER: X6CPLP     DEVN: 3D09
           FORMAT TOD         MAXSYSTEM
           10/21/2012 12:05:59       32
           ADDITIONAL INFORMATION:
            LOGR COUPLE DATA SET FORMAT LEVEL: HBB7705
             LSR(2000) LSTRR(1000) DSEXTENT(10)
             SMDUPLEX(1)
ALTERNATE  DSN: UTCXCF.SVPLEX6.LOGRR13.ALT
           VOLSER: X6CPLA     DEVN: 3E08
           FORMAT TOD         MAXSYSTEM
           10/21/2012 12:17:05       32
           ADDITIONAL INFORMATION:
            LOGR COUPLE DATA SET FORMAT LEVEL: HBB7705
             LSR(2000) LSTRR(1000) DSEXTENT(10)
             SMDUPLEX(1)
LOGR IN USE BY ALL SYSTEMS
```

Figure 42. Expected results from the **D XCF,COUPLE,TYPE=LOGR** *command*

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.

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:

```
//FMTLGCDS JOB  MSGLEVEL=(1,1)
//         EXEC PGM=IXCL1DSU
//* S SUBMIT,JOB=LOGGER.ZOS17.JCL(FORMAT17)
//* SETXCF COUPLE,ACOUPLE=(LOGGER.OSR13.LARGE.INVNTRY,LOGR3),TYPE=LOGR
//* SETXCF COUPLE,PSWITCH,TYPE=LOGR
//SYSPRINT DD   SYSOUT=*
//SYSIN    DD   *
 DEFINEDS SYSPLEX(PLEX1) DSN(LOGGER.OSR13.LARGE.INVNTRY) VOLSER(LOGR3)
   DATA TYPE(LOGR)
     ITEM NAME(LSR)      NUMBER(2000)
     ITEM NAME(LSTRR)    NUMBER(25)
     ITEM NAME(DSEXTENT) NUMBER(15)
     ITEM NAME(SMDUPLEX) NUMBER(1)
//
```

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, 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.

Setup considerations for log snapshots

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

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 211.
  - 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 214.
  - Defining a couple data set for sysplex-wide logging through system logger. See “Defining a couple data set for system logger” on page 208.

  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. See “Enabling SYSLOG for diagnostic snapshots” on page 215.

- 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 213.

  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.

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."

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,HC
```

Figure 43 shows the expected results:

```
CNZ4100I 15.19.16 CONSOLE DISPLAY 056
 CONSOLES MATCHING COMMAND: D C,HC
 MSG:CURR=0    LIM=9000 RPLY:CURR=0    LIM=9999  SYS=P02      PFK=00
 HARDCOPY  LOG=(SYSLOG,OPERLOG)  CMDLEVEL=CMDS
       ROUT=(ALL)
 LOG BUFFERS IN USE: 0       LOG BUFFER LIMIT: 9999
```

Figure 43. Expected results from the **D C,HC** *command*

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.

Before you begin

You must define the logger subsystem.

Procedure

1. Define the OPERLOG 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)
```

2. Activate the CFRM policy through the **SETXCF START,POLICY,TYPE=CFRM,POLNAME=***polname* command, or through the COUPLExx parmlib member.
3. 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(LOGR24K)
HLQ(IXGLOGR)
LS_SIZE(1024)
LOWOFFLOAD(0)
HIGHOFFLOAD(80)
STG_DUPLEX(NO)
RETPD(0)
AUTODELETE(No)
```

4. 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.
5. Define the hardcopy device as `OPERLOG` in the HARDCOPY statement of the CONSOLxx parmlib member. You can change this setting using the **V OPERLOG,HARDCPY** command.
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.

Results

To verify the completion of this work, enter the **DISPLAY CONSOLES,HARDCOPY** command to display the OPERLOG status.

What to do next

If you need to deactivate OPERLOG, you can use the **V OPERLOG,HARDCPY,OFF** command.

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:

```
D LOGREC
```

Figure 44 shows the expected results:

```
IFB090I   15.22.12  LOGREC DISPLAY 062
 CURRENT MEDIUM = DATASET
    MEDIUM NAME = SYS1.P02.LOGREC
```

Figure 44. 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/. 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.

Before you begin

You must define the logger subsystem.

Procedure

1. IPL each system using its own logrec data set specified in the IEASYSxx 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 IEASYSxx, as follows:

   ```
   IEASYSxx with logrec data set:
   LOGCLS=L,
   LOGLMT=010000,
   LOGREC=SYS1.&SYSNAME..LOGREC,   or  LOGREC=LOGSTREAM,
   MAXUSER=128,
   MLPA=00
   ```

2. Define the LOGREC log stream structure definition in the CFRM policy. For example:

```
//LOGREC JOB CLASS=A,MSGCLASS=A
//POLICY EXEC PGM=IXCMIAPU
//SYSPRINT DD SYSOUT=A
//SYSIN DD *
DATA TYPE(CFRM)
STRUCTURE NAME(LOGREC)
SIZE(2048)
INITSIZE(1024)
PREFLIST(FACIL01,FACIL02)
```

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 **DISPLAY LOGREC** command 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 45 on page 215 shows the expected results:

```
IXG601I   15.26.03  LOGGER DISPLAY 070
INVENTORY INFORMATION BY LOGSTREAM
LOGSTREAM                  STRUCTURE        #CONN  STATUS
---------                  ---------        ------ ------
SYSPLEX.OPERLOG            LOGGER_STR1      000004 IN USE
  SYSNAME: P00
    DUPLEXING: LOCAL BUFFERS
  SYSNAME: P01
    DUPLEXING: LOCAL BUFFERS
  SYSNAME: P02
    DUPLEXING: LOCAL BUFFERS
  SYSNAME: P03
    DUPLEXING: LOCAL BUFFERS
  GROUP: PRODUCTION

NUMBER OF LOGSTREAMS:  000001
```

Figure 45. Expected results from the **D LOGGER** *command*

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.

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.

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 enter RACF commands like those shown in Figure 46, where *CEA_userid* is the user ID that you use to access CEA.

```
RDEFINE JESSPOOL SY1.+MASTER+.SYSLOG.*.* UACC(NONE)
PERMIT SY1.+MASTER+.SYSLOG.*.* CLASS(JESSPOOL) ID(CEA_userid) ACC(READ)
SETROPTS RACLIST(JESSPOOL)
```

Figure 46. RACF commands to enable CEA to access SYSLOG

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
- Topic on SVC dump in z/OS MVS Diagnosis: Tools and Service Aids.

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 222.

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

To avoid capturing duplicate problems in the Incident Log task display, ensure that dump analysis and elimination (DAE) is running on the z/OS host system. 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 for all of the systems in the sysplex (or all systems that you want the Incident Log task to represent). Doing so 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* action on the Incident Log page 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* action allows you to collect diagnostic data for the next new occurrence of the same problem.

To configure DAE processing for Incident Log processing, create a pair of ADYSETxx parmlib members with the appropriate options specified. Use one member to start DAE processing and the other member to stop DAE processing.

Consider using the following steps:

1. Create an ADYSETxx member for starting DAE. To do so, copy the IBM-supplied ADYSET00 member in SYS1.PARMLIB to a new member, for example, `ADYSETAA`. Do not modify the IBM-supplied member itself.
2. Create an ADYSETxx member for stopping DAE. To do so, copy the IBM-supplied ADYSET01 member in SYS1.PARMLIB to a new member, for example, `ADYSETBB`. Again, do not modify the IBM-supplied member itself.
3. Edit the new members, as follows:
   - In the DAE start-up member, specify the option SUPPRESSALL on the SVCDUMP parameter to suppress duplicate SVC dumps. Also, include the options SHARE, DSN and GLOBAL to use DAE in a sysplex-wide scope. 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)
```

     In this example, DSN specifies a cataloged data set `SYS1.DAESH2` that resides on a DASD volume with shared access to all of the systems in the sysplex.
   - In the DAE shut-down member, include the option GLOBALSTOP on the DAE= parameter. For example:

```
DAE=STOP,GLOBALSTOP
```

4. Ensure that the active IKJTSOxx parmlib member includes the program name ADYOPCMD in the AUTHCMD NAMES section. For information, see the topic on accessing the DAE data set in z/OS MVS Diagnosis: Tools and Service Aids.
5. To start DAE processing, enter the MVS command **SET DAE=xx** from the operator console, where *xx* is the suffix of the DAE start-up member. Enter the command for each system in the sysplex, for example, by using the **ROUTE** command to direct the **SET DAE=xx** command to the other systems:

   ```
   RO *ALL,SET DAE=xx
   ```

   To ensure that DAE processing is started automatically at IPL-time, include this command in the COMMNDxx parmlib member for the affected systems. If you choose to defer this step, you will need to manually start DAE on each system after each IPL.
6. Thereafter, for the IPLed systems in the sysplex, starting or stopping DAE on any one system will result in the other participating systems automatically starting or stopping DAE processing with the same options.

For more information about how to set up DAE, see z/OS MVS Diagnosis: Tools and Service Aids. For more information about the IBM-supplied ADYSETxx parmlib members, see *z/OS MVS Initialization and Tuning Reference*.

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 does not already have a sysplex dump directory, this topic describes the steps for creating one.

How to check if this step is done

A sysplex dump directory might already exist for your system. This data set is defined through the SYSDDIR statement, which is typically specified in the parmlib member BLSCUSER. An example of the SYSDDIR statement follows:

```
SYSDDIR SYS1.DDIR ENV(ESAME)
```

IBM recommends that you define the SYSDDIR statement in member BLSCUSER. Alternatively, your installation might have specified this statement in member BLSCECT or BLSCECTX, or another member.

If you locate the SYSDDIR statement, verify that the specified sysplex dump directory data set exists, and is accessible to all of the systems in the sysplex (or all of the systems that you want the Incident Log task to represent).

Otherwise, you must create the sysplex dump directory, as described in the section that follows.

Steps for creating the sysplex dump directory

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)'
   ```

   where:
   - `DSNAME` specifies the data set name for the sysplex dump directory. As supplied by IBM, the CLIST specifies the name, `SYS1.DDIR`.
   - `VOLUME` specifies the DASD volume. 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 volume with shared access to all of the systems in the sysplex (or all systems that you want the Incident Log task to represent).
   - `RECORDS` specifies the data set size in records. The Incident Log task requires a sysplex dump directory data set with at least 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.

   The CLIST creates SYS1.DDIR as a VSAM data set with SHAREOPTIONS(1,3).

   This data set must be cataloged on the current system and any other backup systems running the CIM server, to allow for access by the Incident Log task.
2. Specify the dump directory name on the SYSDDIR statement in member BLSCUSER. Alternatively, your installation might use another member, such as BLSCECT or BLSCECTX.
3. Recycle the DUMPSRV address space through the command **`CANCEL DUMPSRV`**. The DUMPSRV address space restarts automatically. This action registers the dump directory name with the DUMPSRV address space.
4. Start BLSJPRMI through the command **`START BLSJPRMI`**. This action registers the dump directory name to IPCS.

For more information about 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 requests are not being satisfied, check for contention on the sysplex dump directory using the command **D GRS,C**. 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 command **IPCS COPYDDIR** 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.

Ensure that common event adapter (CEA) is configured and 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.

Ensure that the common event adapter (CEA) component is configured on your system, including security authorizations. IBM provides the CEASEC job to help you create the security authorizations for CEA; see member CEASEC in SYS1.SAMPLIB.

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 "Resource authorizations for common event adapter (CEA)" on page 191.

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*.

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 "Updating z/OS for the ISPF plug-in" on page 223.

How to check if CEA is active

To determine whether the CEA address space is active, enter the following command:

```
D A,CEA
```

Figure 47 shows the expected results:

```
IEE115I 15.32.17 2010.132 ACTIVITY 109
  JOBS     M/S    TS USERS    SYSAS    INITS   ACTIVE/MAX VTAM     OAS
 00018    00040    00002      00043    00246    00002/03500       00043
  CEA      CEA      IEFPROC  NSWPR*O  A=001A   PER=YES  SMC=000
                                     PGN=N/A  DMN=N/A  AFF=NONE
                                     CT=000.425S  ET=45.32.29
                                     WKL=SYSTEM   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 47. Expected results from the **D A,CEA** *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*.

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"
- "Starting the SYSREXX address space" on page 222

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 Programming: Authorized Assembler Services Guide*
- *z/OS MVS Initialization and Tuning Reference*.

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.

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:

```
D A,AXR
```

Figure 48 shows the expected result:

```
IEE115I 15.34.46 2010.132 ACTIVITY 111
  JOBS     M/S    TS USERS    SYSAS    INITS   ACTIVE/MAX VTAM     OAS
 00018    00040    00002      00043    00246    00002/03500       00043
  AXR      AXR      IEFPROC  NSWPR*   A=0019   PER=YES  SMC=000
                                     PGN=N/A  DMN=N/A  AFF=NONE
                                     CT=000.088S  ET=45.34.45
                                     WKL=STC_WLD  SCL=STCLOW   P=1
                                     RGP=N/A      SRVR=NO  QSC=NO
                                     ADDR SPACE ASTE=05A34640
                                     DSPNAME=AXRTRDSP ASTE=1002D880
                                     DSPNAME=AXRRXENV ASTE=06BED200
                                     DSPNAME=AXRREQCP ASTE=06029180
```

Figure 48. Expected result from the **D A,AXR** *command*

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 *z/OS V2R2 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 49 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=*
//SYSTSIN DD *
IPCS
ALTER DSNAME('OldDump') NEWNAME(DSNAME('NewDump'))
END
/*
```

Figure 49. Sample JCL to rename SVC dumps in the sysplex dump directory

In the example:

- Modify the keyword `DSN=SYS1.DDIR` to specify the name of your sysplex dump directory (the default name is SYS1.DDIR)
- Modify the values *OldDump* and *NewDump* to use the correct dump data set names.

Updating z/OS for the ISPF plug-in

If you have selected to configure the ISPF plug-in, you must ensure that each user of the ISPF task is an existing TSO/E user with a valid password.

Specifically, for each user of the ISPF task, ensure that the corresponding user ID:

- Is authorized to TSO/E on the z/OS host system and has a valid password.
- Is authorized to a valid logon procedure and TSO/E account number.
- 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 uses the logon procedure IKJACCNT, which is supplied by IBM in your ServerPac order, and an asterisk ('*') for the account number. A user can select to use a different logon procedure or account number, as long as the user's logon procedure is properly configured for ISPF and the account number is valid.

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.

For more information about the RACF TRUSTED attribute, see the topic on associating started procedures and jobs with user IDs in *z/OS Security Server RACF System Programmer's Guide*, and the topic on using started procedures in *z/OS Security Server RACF Security Administrator's Guide*.

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*, specifically, the descriptions of the RECONTIME and RECONSESSIONS statements. By default, reconnectable user sessions are not enabled.

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.

Updating z/OS for the Resource Monitoring Plug-in

If you selected to configure the Resource Monitoring plug-in, you might have system customization to perform, as described in this topic.

This topic contains the following information:

- “System customization for the Resource Monitoring and System Status tasks”
- “Enabling PassTicket creation for Resource Monitoring task users” on page 225
- “Browser consideration for the Resource Monitoring task” on page 226.

System customization for the Resource Monitoring and System Status tasks

Table 32 describes the z/OS system changes that are required or recommended. Some of this work might already be done on your system, or might not be applicable. If so, you can skip the particular setup action.

Table 32. z/OS setup actions for the Resource Monitoring and System Status tasks

	z/OS setup action	**Check when task is completed**
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.	
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 GPMSERVE address spaces in your sysplex: `ROUTE *ALL,D A,GPMSERVE` If your installation uses RMF Cross Platform Monitoring (RMF XP), the RACF profile name for the RMF XP DDS is GPM4CIM, rather than GPMSERVE. For information about setting up the DDS and RMF XP, see *z/OS RMF User's Guide*, SC33-7990.	

Table 32. z/OS setup actions for the Resource Monitoring and System Status tasks (continued)

	z/OS setup action	Check when task is completed
3	Determine whether the DDS on the target system is currently configured to require authentication. To check, use the following command to display the active DDS options: `MODIFY GPMSERVE,OPTIONS` If your installation uses RMF XP, the RACF profile name for the RMF XP DDS is GPM4CIM, rather than GPMSERVE. In the command output, check for the HTTP_NOAUTH setting, which indicates the scope of authentication for the DDS, as follows: **HTTP_NOAUTH()** All hosts must authenticate **HTTP_NOAUTH(*)** No authentication is required **HTTP_NOAUTH(***specific_host_or_mask***)** All hosts except those matching the mask must authenticate. If DDS authentication is not required in your enterprise, you are done. Otherwise, proceed to Step 4.	
4	Determine whether your installation security procedures require that the DDS should require authentication from the z/OSMF system and its users, and perform one of the following actions: • If DDS authentication is required from the z/OSMF system, you must ensure that the PassTicket is set up properly, and that the z/OSMF started task user ID is authorized to generate the PassTicket. See "Enabling PassTicket creation for Resource Monitoring task users." • If DDS authentication is not required from the z/OSMF system, you can disable DDS authentication for the system on which z/OSMF is running. Doing so allows the Resource Monitoring and System Status tasks to access the DDS on behalf of z/OSMF users without potentially encountering authentication errors. To disable DDS authentication for the system on which z/OSMF is running (the server host name or IP address), modify the HTTP_NOAUTH statement in the GPMSRVxx parmlib member on the DDS system. In the following example, the HTTP_NOAUTH statement is updated to bypass DDS authentication for the host system represented by *`host_system_IP_address`*: `HTTP_NOAUTH(`*`host_system_IP_address`*`)` For more information about DDS authentication, see *z/OS RMF User's Guide*, SC33-7990.	

Enabling PassTicket creation for Resource Monitoring task users

If the RMF Distributed Data Server (DDS) requires authentication from the z/OSMF system and its users, follow the steps in this procedure to set up the PassTicket support.

About this task

In this procedure, you ensure that the PassTicket is set up properly, and that the z/OSMF started task user ID is authorized to generate the PassTicket. The procedure shows how this setup can be done for a system that uses RACF as its security management product.

Note: If your installation uses RMF Cross Platform Monitoring (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 procedure.

Procedure

1. On the z/OSMF system, activate the security class PTKTDATA, if this class is not already active. If you plan to use generic profiles for the PTKTDATA class, include the GENERIC option on the **SETROPTS** command, for example:

   ```
   SETROPTS CLASSACT(PTKTDATA)
   SETROPTS RACLIST(PTKTDATA) GENERIC(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(KEYMASKED(key))
   SETROPTS RACLIST(PTKTDATA) REFRESH
   ```

   where *key* is a user-supplied 16-digit value used to generate the PassTicket. If a common cryptographic architecture (CCA) product is installed on the systems with the secured signon function, you can encrypt the secured signon key using a KEYENCRYPTED value. If not, you can mask the secured signon key by using the SSIGNON option and a 64-bit KEYMASKED value, as shown in the preceding example. If you plan to use a KEYENCRYPTED value, note that additional authorizations are required, such as access to security profiles in the CSFSERV class, and additional profiles for PassTicket creation and PassTicket validation. Be sure to review the RACF setup requirements for the CCA product.

3. To enable PassTicket creation for Resource Monitoring 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 started task user ID permission to generate PassTickets for users.
   - 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 z/OSMF started task user ID. By default, this is IZUSVR.

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

Browser consideration for the Resource Monitoring task

Users who plan to use the Internet Explorer with Resource Monitoring task, and who plan to export the data collected in a dashboard to a CSV file, should ensure that the browser is enabled for automatic prompting for file downloads. This setting prevents the file download blocker from being invoked when the user downloads service definitions to the workstation.

Otherwise, if automatic prompting is disabled (the default setting), the download blocker prompts the user to accept these file downloads, causing the browser session to be reloaded and the active tabs to be closed. Users can avoid this disruption by enabling automatic prompting for file downloads.

For more information, see “Enabling automatic prompting for file downloads” on page 112.

Updating z/OS for the Software Deployment plug-in

If you selected to configure the Software Deployment plug-in, you might have system customization to perform, as described in this topic.

The Software Deployment plug-in contains the Software Management task, which becomes available to users in the navigation area when you configure the plug-in.

The Software Management task:

- Allows all users of the task to access deployment objects. Optionally, your installation can further restrict these authorizations, as described in the topic "Creating access controls for the Software Management task."
- Works only with systems in the local sysplex. Optionally, your installation can allow the Software Management task to work with other sysplexes in your installation, as described in "Configuring a primary z/OSMF for communicating with secondary instances" on page 74.

Creating access controls for the Software Management task

The Software Management 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 Software Management task. Creating access controls for the actual physical resource is outside the scope of z/OSMF.

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 Software Management task and its objects are controlled through the following default resource profiles, which are defined in the ZMFAPLA class:

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.**
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.**
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.PRODUCT_INFO_FILE.*
```

With the default access authorities, z/OSMF users and administrators are allowed to perform all actions for all software instances, deployments, categories, and global zones, and only z/OSMF administrators are allowed to retrieve information from product information files.

Important: All users of the Software Management task should be permitted at least READ access to profile <SAF-prefix>.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 Software Management task uses this z/OS system when performing SAF authorization checking.

Use the SAF resource names, which are generated by the Software Management 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:

```
<SAF-prefix>.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 in the Systems 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.ZOS220.CSI that can be accessed by system AQFT, the SAF resource name for the global zone would be

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.GZN.AQFT.MVSBUILD.ZOS220.CSI
```

Table 33 lists the access authorities you can assign to global zone resources and the actions that are permitted for each access authority. The Software Management 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 33. Actions users can take against global zones by access authority

Access Authority	Actions Allowed
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:

```
<SAF-prefix>.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 in the Systems task.
- **instanceName** is the name of the software instance.

For example, if you have a software instance named z/OSV2R2_Test that can be accessed by system AQFT and is assigned to categories z/OS and Test, its SAF resource names would be:

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.SWI.z/OS.AQFT.z/OSV2R2_Test
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.SWI.Test.AQFT.z/OSV2R2_Test
```

Table 34 lists the access authorities you can assign to software instance resources and the actions that are permitted for each access authority. The Software Management 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 34. Actions users can take against software instances by access authority

Access Authority	Actions Allowed
READ	• View the properties of the software instance. • View information about the products, features, and FMIDs contained in a software instance. • View information about the data sets contained in a 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 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. • Retrieve information from SMP/E about the products, features, and FMIDs contained in the software instance and make that information available to z/OSMF.
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** action 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:

```
<SAF-prefix>.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_R21_Production that is not assigned to any category, its SAF resource name would be

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.DEP.NOCATEGORY.z/OS_R21_Production
```

Table 35 lists the access authorities you can assign to deployment resources and the actions that are permitted for each access authority. The Software Management 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 35. Actions users can take against deployments by access authority

Access Authority	Actions Allowed
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:

```
<SAF-prefix>.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

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.CAT.z/OS
```

Table 36 lists the access authorities you can assign to category resources and the actions that are permitted for each access authority. Note that the Software Management 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 36. Actions users can take against categories by access authority

Access Authority	Actions Allowed
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:

```
<SAF-prefix>.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 +
(IZUDFLT.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.*.DB2.**) UACC(NONE)
PERMIT +
IZUDFLT.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.*.DB2.** +
CLASS(ZMFAPLA) ID(DB2PROG) ACCESS(CONTROL)
PERMIT +
IZUDFLT.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:

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.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 +
(IZUDFLT.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.CATEGORIES.MODIFY) +
UACC(NONE)
PERMIT +
IZUDFLT.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.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:

```
<SAF-prefix>.ZOSMF.SOFTWARE_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 +
(IZUDFLT.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.*.NOCATEGORY.**) UACC(NONE)
```

Controlling who can retrieve product information files

A product information file is a file that contains information about one or more products, such as the product announce date and end of service date. Information extracted from these files are displayed in several views and reports in the Software Management task, such as in the *Products* view and in the End of Service report.

When you retrieve a product information file, z/OSMF reads the file and loads the extracted content into the database where data for the Software Management task is stored. The scope of this action is broad and spans all products in the database; therefore, this action should be carefully controlled.

To control who can retrieve product information files, permit users READ access to the following resource:

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.PRODUCT_INFO_FILE.RETRIEVE
```

By default, only z/OSMF administrators are permitted READ access to this resource. That is, by default, only z/OSMF administrators can retrieve product information files.

Creating product information files for the Software Management task

A *product information file* is a flat file, such as a text file, that contains information about one or more products. This information includes, for example, the product announce date, general availability date, and end of service date. You can create your own product information files or obtain them from a provider, such as IBM, another vendor, or a third party.

z/OSMF displays data from product information files in several views in the Software Management task. For example, this information is displayed in the Products page, the Products, Features, and FMIDs page, and the End of Service report.

Syntax for product information files

To be processed by z/OSMF, product information files must be formatted as JSON data and have the following syntax:

```
{
  "Version": "date-modified",
  "Products":
  [
    {
      "prodName": "product-name",
      "prodId": "product-identifier",
      "prodVRM": "version-release-modification",
      "GAAnnounceDate": "date-announced",
      "GADate": "general-availability-date",
      "URL": "URL",
      "EOSDate": "end-of-service-date",
      "country": "country"
    }
  ]
}
```

where,

date-modified
: Date the file was created or last updated. The date must have the format YYYY-MM-DD. The date is required.

product-name
: Name of the product. The name is optional, and is not used by z/OSMF. To omit the product name, exclude the field, type `null` as the value, or set the value equal to an empty string.

product-identifier
: Identifier of the product. The product ID is required.

version-release-modification
: Version, release, and modification level of the product. The value has the format *VV.RR.MM*, where *VV* is the two-digit version, *RR* is the two-digit release, and *MM* is the two-digit modification level. The version, release, and modification level are required.

date-announced
Date the vendor publicly announced the details of the product. The date must have the format YYYY-MM-DD. The date is optional. To omit the date, exclude the field or type `null` as the value.

general-availability-date
Date that a version or release of the product is available to all users. The date must have the format YYYY-MM-DD. The date is optional. To omit the date, exclude the field or type `null` as the value.

URL URL that links to additional information about the product. This information can include, for example, product life cycle dates, product highlights, planning information, and technical descriptions. The URL is optional. To omit the URL, exclude the field, type `null` as the value, or set the value equal to an empty string.

end-of-service-date
Last date on which the vendor will deliver standard support services for a given version or release of the product. This date is the general end of service date. It does not account for lifecycle extensions. The date must have the format YYYY-MM-DD. The date is optional. To omit the date, exclude the field or type `null` as the value.

country
Country for which the end of service date is applicable. The country is optional. To omit the country, exclude the field, type `null` as the value, or set the value equal to an empty string.

The information for each product must be contained within separate braces ({ }) inside the brackets ([ ]), and each set of braces must be comma separated. For a sample file that contains the information for two products, see Figure 50.

Sample product information file

```
{
  "Version": "2011-06-30",
  "Products":
  [
    {
      "prodName": "z/OS",
      "prodId": "5694-A01",
      "prodVRM": "01.10.00",
      "GAAnnounceDate": "2008-08-05",
      "GADate": "2008-09-26",
      "URL": "http://www-03.ibm.com/systems/z/os/zos/",
      "EOSDate": "2011-09-30",
      "country": "US"
    },
    {
      "prodName": "z/OS",
      "prodId": "5694-A01",
      "prodVRM": "01.13.00",
      "GAAnnounceDate": "2011-07-12",
      "GADate": null,
      "URL": "",
      "country": "US"
    }
  ]
}
```

Figure 50. Sample product information file for the Software Management task

Working with the IBM product information file

The product information file that IBM supplies for System z® software is located at the following URL: http://public.dhe.ibm.com/services/zosmf/JSONs/IBMProductEOS.txt .

To load the contents of the file into z/OSMF, do one of the following:

- Load directly from the URL.
- Manually download the file at the URL to your local workstation.
- Manually download the file at the URL to a z/OS data set or UNIX file that the primary z/OSMF host system can access.

When transferring the file from a workstation to a z/OS data set or UNIX file, transfer the file in binary format. To avoid errors, do not convert the file to the EBCDIC character set.

After you store the file in your desired location, to retrieve its contents, complete the steps provided in the *Retrieving product information from product information files* topic in the z/OSMF online help.

Updating z/OS for the Workload Management plug-in

If you selected to configure the Workload Management plug-in, you might have system customization to perform, as described in this topic.

This topic contains the following sections:

- "Authorizing users to the MVSADMIN.WLM.POLICY profile"
- "Authorizing the z/OSMF started task user ID to the MVSADMIN.WLM.POLICY profile" on page 236
- "Using authorization levels for the Workload Management task" on page 236
- "Using a browser with WLM service definitions" on page 237.

Authorizing users to the MVSADMIN.WLM.POLICY profile

Users of the Workload Management task require UPDATE access to resources that are protected by the profile MVSADMIN.WLM.POLICY in class FACILITY. If you run the CFZSEC job when setting up the Common Information Model (CIM) server for z/OSMF, all users who are authorized for the CIM server are automatically authorized for this profile. If this set of authorizations is acceptable in your environment, no further steps are needed.

If not all CIM server users should have access to the MVSADMIN.WLM.POLICY profile, however, you must perform additional steps to avoid creating unwanted authorizations. To do so, complete the following steps:

- Edit the CFZSEC 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. Give the group UPDATE access to profile MVSADMIN.WLM.POLICY. If such a group already exists in your environment, you can use the existing group instead of creating a new group.

  As an example, the following steps show sample RACF commands for creating a separate WLM group and authorizing it to the MVSADMIN.WLM.POLICY profile:

  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 your changes take effect:

     ```
     SETROPTS RACLIST(FACILITY) REFRESH
     ```

- During the z/OSMF configuration process, edit the IZUSEC job before running it and add the name of the WLM security group that your installation uses for authorizing users to the z/OS Workload Management component on your system. The IZUSEC job contains commands for connecting users to the group.

Authorizing the z/OSMF started task user ID to the MVSADMIN.WLM.POLICY profile

The Workload Management task performs periodic queries of WLM on the z/OS host system. To perform the queries, the Workload Management task uses the z/OSMF started task user ID. Therefore, you must ensure that the z/OSMF started task user ID has READ access to the profile MVSADMIN.WLM.POLICY and authorization to the CIM server.

To manually authorize the z/OSMF started task user ID for the MVSADMIN.WLM.POLICY profile and the CIM server, complete the following steps:

1. Grant the z/OSMF started task user ID read access to the profile MVSADMIN.WLM.POLICY. By default, this user ID is IZUSVR.

   In RACF, you can use the following command:

   ```
   PERMIT MVSADMIN.WLM.POLICY
   CLASS(FACILITY) ID(IZUSVR) ACCESS(READ)
   ```

2. Connect the z/OSMF started task user ID to the CIM user group. By default, the CIM user group is CFZUSRGP.

   In RACF, you can use the following command:

   ```
   CONNECT IZUSVR GROUP(CFZUSRGP)
   ```

Ensure that the user ID under which the CIM server is running has SURROGAT access for the z/OSMF started task user ID. If a generic BPX.SRV.** profile is already authorized in the SURROGAT class (for example, because you ran the CFZSEC job when setting up the CIM server), no additional action is required. Otherwise, define a discrete profile for the z/OSMF started task user ID and authorize it. If necessary, refresh the SURROGAT class.

Using authorization levels for the Workload Management task

Using predefined authorization levels, your installation can authorize users to specific functions within the Workload Management task.

The Workload Management task supports the following authorization levels:

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 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 to invoke the Workload Management task. To install service definitions and activate service policies, the user must also be authorized for the Install level.

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

Your installation can manage user authorizations through your security management product, such as RACF. Grant access authority to the users and groups, as appropriate, as described in Table 37 on page 237.

Table 37. Workload Management task authorizations for z/OSMF

Required authorization level of user or group	Required SAF access authority
View	READ access for profile <*SAF-prefix*>.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.VIEW
Install	READ access for profile <*SAF-prefix*>.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.INSTALL
Modify	READ access for profile <*SAF-prefix*>.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.MODIFY

If these default settings do not meet your needs, you can change the SAF authority of these respective groups for the profiles shown in Table 37.

Alternatively, you can define new custom groups for the Workload Management task. For example, the following RACF commands can be used to define a custom group `WLMPOLOP`, which is authorized for the View and Install functions. This set of authorizations 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:

```
CONNECT "userid" GROUP(WLMPOLOP)
```

Understand that the IZUSEC job does not process any custom groups you might have created. Instead, you must connect users to your custom groups manually.

Using a browser with WLM service definitions

Users who plan to use the Internet Explorer browser to work with WLM service definitions should ensure that the browser is enabled for automatic prompting for file downloads. This setting prevents the file download blocker from being invoked when the user downloads service definitions to the workstation. Otherwise, if automatic prompting is disabled (the default setting), the download blocker prompts the user to accept these file downloads, causing the browser session to be reloaded and the active tabs to be closed. Users can avoid this disruption by enabling automatic prompting for file downloads. For more information, see “Enabling automatic prompting for file downloads” on page 112.

Appendix C. 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 the error.

"CEA reason codes for the Incident Log task" describes the CEA reason codes you might encounter during the configuration of the task. "CEA reason codes for the z/OS jobs REST interface services" on page 242 describes the CEA reason codes that an HTTP client application might encounter when using the z/OS jobs REST interface services. For other CEA reason codes, see the topic on using CEA TSO/E address space services in *z/OS MVS Programming: Callable Services for High-Level Languages*.

CEA reason codes for the Incident Log task

Table 38 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 38. CEA reason codes related to Incident Log task processing

Reason code (decimal)	Reason code (hex)	Description	System programmer action	CIM message	z/OSMF message	IBM Support information
256	100	The CEA address space is not running.	Follow the steps in "Ensure that common event adapter (CEA) is configured and active" on page 219.	CEZ05002E	IZUP634E	CEAUNAVAIL
289	121	CIM indication processing is not available because the CEA address space is running in minimum (MIN) mode. To support Incident Log processing, CEA must be operated in full mode.	Use the **MODIFY CEA,MODE** command to change the CEA mode of operation to full mode. To do so, enter the command, as follows, from the operator console: `F CEA,MODE=FULL` Running CEA in full mode requires that z/OS UNIX system services is available.	CEZ05013E		CEAFORCEMINMODE
813	32D	The user is not authorized for this request.	Define the appropriate authority for the user.	CEZ05003E	IZUP635E	CEANOINSTRAUTH
830	33E	An abend occurred in the CEA task that interacts with the IPCS environment.	Report the problem to IBM Support.	CEZ05001E	IZUP639E	CEAIPRQSERVER ABENDED
834	342	The sysplex dump directory is empty.	Ensure that the sysplex dump directory is not empty.			CEASDDIREMPTY
835	343	A dump incident was not found. Most likely, the incident was deleted by another user.	No action is required.	CEZ05004E	IZUP636E	CEAADDFAILED

© Copyright IBM Corp. 2009, 2016

Table 38. CEA reason codes related to Incident Log task processing (continued)

Reason code (decimal)	Reason code (hex)	Description	System programmer action	CIM message	z/OSMF message	IBM Support information
850	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 216.		IZUP637E	CEADAEDSN NOTAVAILABLE
855	357	The called function could not generate a prepared data set name (DSN).	Verify that the compiled REXX exec CEACDMPP exists and can be run by System REXX.			CEAGENPREPARED DSNFAIL
857	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
866	362	The source description for a requested dump incident was not found in the sysplex dump directory.	Determine why the dump incident was not identified in the sysplex dump directory. Possible reasons include: • Dump has not yet been taken • Dump has not yet been written out • Dump is being entered into a different sysplex dump directory than the one that is used by the Incident Log task.	CEZ05001E	IZUP631E	CEADMPINCIDENT NOTFOUND
869	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 221.	CEZ05005E	IZUP640E	CEASYSREXX NOTACTIVE
870	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 221.	CEZ05006E	IZUP643E	CEASYSREXXBAD ENVIRONMENT
871	367	System REXX cannot process the exec at this time.	Try the request again later.	CEZ05007W	IZUP644E	CEAEXECTIMEOUT
872	368	System REXX cannot schedule the exec to run at this time.	Try the request again later.	CEZ05008W	IZUP645E	CEASYSREXX OVERLOADED
879	36F	The user is not authorized to view the operations log (OPERLOG) snapshot information.	Ask the security administrator to authorize the user to the data set, which is specified in the CEAPRMxx parmlib member.	CEZ05010E		CEANOSAF OPERLOGSNAP

Table 38. CEA reason codes related to Incident Log task processing (continued)

Reason code (decimal)	Reason code (hex)	Description	System programmer action	CIM message	z/OSMF message	IBM Support information
880	370	The system logger component is not available.	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 "Defining a couple data set for system logger" on page 208. For information about the IXGCON macro, see z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG.	CEZ05011E		CEALOGGER NOTAVAIL
881	371	The function that prepares incident materials to be sent through FTP could not allocate a new data set for the tersed diagnostic snapshot.	Check the CIM trace file for system messages associated with the return code indicating the reason for the failure. For assistance, contact IBM Support.			CEABADALLOCNEW
882	372	The function that prepares an incident to be sent through FTP could not allocate the data set to be tersed.	Check the CIM trace file for system messages associated with the return code indicating the reason for the failure. For assistance, contact IBM Support.			CEATERSE BADALLOC1
886	376	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.	Check SYSLOG for message CEA0600I, which contains the return and reason codes.			CEANOSNAPSHOT
888	378	No log data was accumulated in diagnostic snapshot.	If this problem occurs frequently, adjust the DUMPCAPTURETIME setting in the CEAPRMxx parmlib member.			CEAPDWB DIAGDATAEMPTY
889	379	An incorrect format or value was supplied for the IBM PMR number.	Correct the IBM PMR number and try again. The format of the IBM PMR number should be *nnnnn.ccc.bbb* where *nnnnn* is the PMR number, *bbb* is the branch code, and *ccc* is the country code.			CEAWRONG IBMPMRFORMAT
893	37D	An attempt to obtain the enqueue on the sysplex dump directory failed; another program already holds the enqueue.	Ensure that only one user is attempting to access the dump information at one time. To check for enqueue contention, enter the command **D GRS,C** at the operator console. Wait for the enqueue to be released and try again.	CEZ05017E	IZUP641E	CEAIPCSENQ ERROR
894	37E	The requested function failed to open the sysplex dump directory.	Verify that the sysplex dump directory (default name SYS1.DDIR) is set up and usable. For more information, see "Creating the sysplex dump directory" on page 217.	CEZ05016E	IZUP642E	CEASDDIR OPENERROR
898	382	The component table is corrupted.	Report the problem to IBM Support.			CEAXMLTAGS TOODEEP
901	385	The diagnostic data to be sent is currently in use.	Try the request again later.			CEAPREPARE OBJINUSE
902	386	The diagnostic data to be sent is currently in use.	Try the request again later.			CEAPREPAREENQERR

Table 38. CEA reason codes related to Incident Log task processing (continued)

Reason code (decimal)	Reason code (hex)	Description	System programmer action	CIM message	z/OSMF message	IBM Support information
908	38C	The sysplex dump directory has no space available to record new SVC dumps.	See "Establishing a larger sysplex dump directory" on page 219.			CEACKST INVALIDALLOC VALUE
913	391	The JES subsystem is not available.	Determine why the JES subsystem is not accessible. Perhaps, it has not been started.			CEAJESNOT AVAILABLE
919	397	The Set Incident field data was truncated at 256 characters.	Specify a smaller amount of data for the user comment field to prevent truncation. Retry the request.			CEASETINCIFVAL DATATRUNC
920	398	The request failed because one or more of the affected dump data sets are migrated.	If the data set is migrated and automatic recall is enabled for the hierarchical storage manager (HSM), the system issues a recall request for the data set. Wait for the recall request to complete and then retry the request.			CEAMIGRATED DATASETS
921	399	The request failed because one or more of the requested dump data sets are migrated and the hierarchical storage manager (HSM) encountered an error occurred when attempting to recall the data sets.	Determine why HSM is not functioning properly. The problem might be that HSM is inactive or unresponsive. Correct the problem and retry the request.			CEAMIGRATED DATASETSWHSMERR
922	39A	The request failed because CEA could not allocate an internal buffer to satisfy the request.	Try the request again. If the problem persists, determine why there is insufficient storage on the system. Consider reducing the number of inactive incidents on your system through the **ceatool** program, which is described in Chapter 13, "Deleting incidents and diagnostic data," on page 99. Correct the problem and retry the request. If the problem persists, contact IBM Support.			CEAUNABLETO ALLOCATE3

CEA reason codes for the z/OS jobs REST interface services

Table 39 describes the CEA reason codes that an HTTP client application might encounter when using the z/OS jobs REST interface services.

Table 39. CEA reason codes related to z/OS jobs REST interface processing

Reason code (decimal)	Reason code (hex)	Description	System programmer action	IBM Support information
923	39B	The request failed because the caller is not authorized to modify the job.	Check with your installation's security administrator to ensure that the caller's user ID is authorized to the appropriate resources in the JESJOBS class. For the specific authorizations required, see "Resource authorizations for the z/OS jobs REST interface" on page 192.	CEANOJESAUTHORITY
925	39D	An internal CEA error occurred.	Report the problem to IBM Support.	CEANOENTITY POSSIBLE
926	39E	The request failed because the specified job was not found on the system.	Examine the request to determine whether the job was identified correctly, either through the job name and job ID (jobname/jobid), or the job correlator.	CEASSIJOBNOTFOUND

Appendix D. Accessibility

Accessible publications for this product are offered through the z/OS Information Center, which is available at http://www.ibm.com/systems/z/os/zos/bkserv/.

If you experience difficulty with the accessibility of any z/OS information, please send a detailed message to mhvrcfs@us.ibm.com or to the following mailing address:

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Building 707
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 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.

Accessibility features for the z/OSMF GUI

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully. IBM strives to provide products with usable access for everyone, regardless of age or ability.

The following list includes the major accessibility features in the z/OSMF GUI:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers.

Keyboard navigation

This product uses standard operating system navigation keys. You can use keys or key combinations to perform operations and initiate menu actions that can also be done through mouse actions. You can navigate the z/OSMF GUI from the keyboard by using the shortcut keys for your browser or screen-reader software. See the z/OSMF online help for a list of shortcut keys that z/OSMF supports.

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.

© Copyright IBM Corp. 2009, 2016

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.

Notices

This information was developed for products and services offered in the U.S.A. or elsewhere.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

© Copyright IBM Corp. 2009, 2016

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

Site Counsel
IBM Corporation
2455 South Road
Poughkeepsie, NY 12601-5400
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

COPYRIGHT LICENSE:

This information might contain sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Policy for unsupported hardware

Various z/OS elements, such as DFSMS, HCD, JES2, JES3, and MVS, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Minimum supported hardware

The minimum supported hardware for z/OS releases identified in z/OS announcements can subsequently change when service for particular servers or devices is withdrawn. Likewise, the levels of other software products supported on a particular release of z/OS are subject to the service support lifecycle of those products. Therefore, z/OS and its product publications (for example, panels, samples, messages, and product documentation) can include references to hardware and software that is no longer supported.

- For information about software support lifecycle, see: IBM Lifecycle Support for z/OS (http://www.ibm.com/software/support/systemsz/lifecycle/)
- For information about currently-supported IBM hardware, contact your IBM representative.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available at Copyright and Trademark information (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, its affiliates, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names might be trademarks or service marks of others.

Index

Special characters

_BPXK_AUTOCVT environment variable 114
/tmp directory 115
  modifying the default 23
.profile file
  defining for the administrator 202

A

About page
  description 113
About this document ix, xi
accessibility 243
  features of the GUI 243
administration task
  links 97
AGGRGROW setting
  used for z/OSMF 19, 30
Application Linking Manager task
  overview 83
authenticated guest
  description 66
automatic dump data set allocation (auto-dump)
  using 215
automount facility
  consideration for using 20
automount process
  consideration for using 19
AUTOMOVE setting
  consideration for using 19
AXR address space
  verifying active state 221

B

backing store file
  transferring into z/OSMF 205
base configuration
  creating 27
  description 13
BLSCDDIR CLIST
  example 219
  using 218
BLSJPRMI program
  using 219
BPXPRMxx parmlib member
  settings for 19
browser
  See web browser

C

CA
  See certificate authority
Capacity Provisioning task
  overview 47
  z/OS customization 203
CBPDO tape
  configuration steps to use 27
CEA
  See common event adapter (CEA)
CEA high-level qualifier 99
CEAPRMxx parmlib member
  specifying an eighth volume 221
  specifying in IEASYSxx member 219, 220
  specifying the HLQ for snapshot data sets 99
CEASEC job
  using 219
CEASNPLG member of SYS1.SAMPLIB 99, 209, 214
ceatool program
  description 99
  examples 101
  invoking 100
certificate authority (CA)
  using 74, 85, 91
certificate error
  troubleshooting 119, 120, 121
CFZSEC job
  using 189, 201
CIM
  See Common Information Model
CIM class 86
CIM indication 85, 86
CIM indication provider
  subscription 86
CIM server
  commands 87
  customizing the administrator profile 87
CIMSERV profile in the WBEM class 189, 201
class activation 29, 181
client side log data 115, 116
common event adapter (CEA)
  address space
    assigning the TRUSTED attribute 220, 223
    disconnecting from the sysplex dump directory 127
    used during Incident Log task processing 205
    verifying active state 219
  authorizing the z/OSMF administrator 219
  CEAPRMxx parmlib member 209, 220, 221
  deleting diagnostic data 99
  deleting incidents 99
  ensuring that CEA is active 219, 220
  full function mode 219
  high-level qualifier 99
  log stream recommendation 214
  modifying settings 221
  overview 4
  RACF security profiles 191, 192, 193
common event adapter (CEA) *(continued)*
  reason codes 239
  starting at IPL 209
Common Information Model (CIM)
  .profile file
    defining for the administrator 202
  server
    automatic startup 201
    logging 103
    overview 4
    security authorizations 189, 201
    starting 87, 202
    timeout setting 201
    trace 103
configuration
  for z/OSMF 13
Configuration Assistant for z/OS Communications Server
  transferring backing store file 205
Configuration Assistant task
  collecting information for troubleshooting 124
  common problems 124
  overview 48
  troubleshooting 124
  z/OS customization 205
configuration file
  description 13
configuration process
  authorizations needed 28
  overview 13
  performers 27
configuration script
  prerequisites 27
  selecting a user ID 28
Configuration Workflow 67
core functions
  in a base configuration 45
CSFSERV class profiles 188

D

disability 243
dump analysis and elimination (DAE)
  configuring 216
DUMPSRV address space
  recycling 219
dynamic VIPA
  using 72

E

environment checker tool
  using 104

F

file system 72
Firefox browser
  certificate error 120

© Copyright IBM Corp. 2009, 2016

firewall consideration 201
FTP job
  modifying the device default 23
  status codes 128
full function mode for CEA 219
full system replacement installation
  considerations 5, 27

G

generic profile checking
  enabled for security classes 181
guest user
  access to resources 66
  customized Welcome page 81

H

high availability
  planning for 71
high level qualifer (HLQ)
  for CEA data sets 99
HLQLONG statement 99
host name
  specifying in IZUPRMxx 23
host system
  required software 27

I

IBM 64-bit SDK for z/OS, Java Technology Edition 4
IBM z Systems Data Compression (zEDC)
  security authorizations 188
IBM z/OS Management Facility
  base configuration 13, 27
  component overview 4
  configuration process 13
  Lightweight Third Party Authentication (LTPA) 77
  multiple instances 71, 73, 74, 77
  overview ix, 3, 4, 5, 6
  planning checklist 7
  post-configuration 79
  publications ix
  single sign-on (SSO) 77
  summary of IT roles and skills 7
  tasks overview 46
  troubleshooting 103
    information for 103
  web site ix
IBMzOS_JobsIndicationProvider 86
IKJTSOxx member 118
Incident Log task
  CEA reason codes 239
  common problems 126
  configuration updates
    reference information 205
  device for storing data 23
  modifying the device default 23
  overview 49
  temporary directory 23
  troubleshooting 126
  z/OS customization 207
incidents
  deleting 99, 101
installation verification program (IVP)
  System REXX check 221
installer user ID
  creating a base configuration 27
  logging in to z/OSMF 36
  requirements for 28
Integrated Cryptographic Service Facility (ICSF)
  security authorizations 188
ipl-time mount commands 31
ISPF task
  common problems 125
  overview 51
  troubleshooting 125
  z/OS customization 223
IXCMIAPU utility program 214
IZUANG1 started task
  cataloged procedure 16, 17
IZUDFLT profile prefix 64
IZUFPROC logon procedure
  cataloged procedure 16, 18
  permissions 16, 18
  specifying in IZUPRMxx 23, 25
IZUG0.log.lck file 114
IZUGn.log file 113, 114
izugwrkmanwlmclass setting 23
IZUKeyring.SAF_PREFIX
  description 74
izumigrate.sh script 41
IZUMKFS job 30
IZUPRMxx parmlib member
  description 22
  syntax rules 22
IZUSEC job 28, 63
IZUSVR user ID
  permissions 16, 17, 188
IZUSVR1 started task
  cataloged procedure 16, 17
IZUxxSEC job 63

J

job
  IZUMKFS job 30
  IZUSEC job 28, 63
  IZUxxSEC job 63
  priming the user file system 30
job control language (JCL)
  sample for renaming dumps in the sysplex dump directory 222

L

link
  managing security in z/OSMF 97
link properties file 95
log data 115
  client side 116
  server side 115
log file
  description 113
  working with 114
log format 115
log lock file 114
logging in to z/OSMF 23, 36, 122
LOGREC log stream
  setting up 213
LTPA
  See Lightweight Third Party Authentication (LTPA)
ltpatimeout setting 122

M

mainframe education ix
managing log lock files 114
MAXPROCUSER value
  consideration 117
messages for z/OSMF 129
messages.log file 113
migration
  description 39
  migrating the configuration values 41
  steps 39
mount point 72
mounting file system
  ipl-time mount commands 31
multilevel secure (MLS) 16

N

network consideration 201
Notices 245
Notifications Settings task
  overview 53
Notifications task
  overview 52

O

operations log (OPERLOG)
  setting up 211
operator console messages 113

P

PassTicket creation 203, 204, 224
planning checklist 7
plug-in
  planning your selections 45
port number
  specifying in IZUPRMxx 23
post-configuration
  for z/OSMF 79
primary instance
  configuring 74, 77
PROCUSERMAX value
  consideration 117
product information files 233
profile.add file 202
project plan 7
PTKTDATA security class
  activating 204, 225

R

RACDCERT command
  error message 118
  using 93

RACF SPECIAL attribute 27
re-authenticating 23, 122
reason codes
  for common event adapter 239
Resource Monitoring task
  browser consideration 226
  overview 55
  z/OS customization 224
runtime log 113, 114, 115

S

SAF
  See system authorization facility
SAF profile prefix
  defining 182
screen resolution
  minimum supported 16
script
  izumigrate.sh script 41
  startServer.sh script 35
secondary instance
  configuring 74, 77
Secure Sockets Layer (SSL) connection
  enabling between client programs and z/OSMF 85, 91
  enabling between instances of z/OSMF 74
security administration
  overview 64
security administrator
  actions performed by 64
  managing links 97
security class
  activating 29, 181
security concepts 15
security setup
  default for z/OSMF 181
Send Diagnostic Data wizard
  troubleshooting 128
server log files 114
server side log data
  description 115
ServerPac order
  considerations ix, 5, 27
service
  applying updates to z/OSMF 6
session expiration setting 23
single sign-on (SSO)
  enabling between instances of z/OSMF 77
Software Management task
  z/OS customization 74, 227
software upgrade installation
  considerations 5, 27
SSL
  See Secure Sockets Layer (SSL)
SSO
  See single sign-on (SSO)
startServer.sh script
  using 35
subscription
  choosing a user ID 86
  creating 87
  customizing the administrator profile 87
summary of changes xiii
superuser authority
  required for user ID 28
SYS1.SAMPLIB data set
  CEASNPLG member 209, 214
sysplex dump directory
  creating 218
  migrating to a larger directory 219
  renaming dumps in the directory 222
  space shortage 219
  using the BLSCDDIR CLIST 218
SYSREXX
  See System REXX (SYSREXX) component
system authorization facility
  overview 4
system log (SYSLOG)
  capturing data from 215
system logger couple data set
  creating 209
system prerequisites for z/OSMF
  overview 201
System REXX (SYSREXX) component
  ensuring that it is active 221
System Status task
  overview 59
  z/OS customization 224

T

temporary directory
  modifying the default 23
tools for troubleshooting 104
trademarks 247
troubleshooting
  action or link not available 123
  browser problems 104
  certificate error 119, 120, 121
  checking the About page 113
  common problems 117
  Configuration Assistant task 124
  configuration problems 117
  EJBROLE class not defined 123
  Firefox 107
  help not available 123
  Incident Log task 126
  Internet Explorer 110
  ISPF task 125
  link not available 123
  logon errors 122
  messages 129
  overview 103
  Send Diagnostic Data wizard 128
  tools for 103, 104
  user interface problems 118
  using the runtime logs 113, 114
  workstation problems 104
TRUSTED attribute
  assigning to the CEA addresss space 220, 223

U

user file system
  mounted at IPL 19
  priming during configuration 30
user ID
  selecting for configuration 28
user login error 122

W

web browser
  common problems 107, 110, 119
  enabling prompting for file downloads 112, 226, 237
  Internet Explorer 226, 237
  recommended settings 107, 110, 112
  supported browsers 16
  troubleshooting
    Firefox 107
    Internet Explorer 110, 112
WebSphere Liberty profile 4
  messages 129
  troubleshooting 103
Welcome page
  accessing 35
  customizing for guests 81
Workflows task
  overview 60
Workload Management task
  browser consideration 237
  overview 61
  z/OS customization 235
workstation
  logon errors 122
  required software 16

Z

z/OS Basic Skills information center ix
z/OS data set and file REST interface
  cataloged procedure 16, 18
  RACF security profiles 191
  setting up 16, 18
z/OS jobs REST interface
  CEA reason codes 242
  post-configuration tasks 85, 86, 91
  RACF security profiles 192
z/OSMF
  See IBM z/OS Management Facility
z/OSMF administrator
  defining 201
z/OSMF installer user ID
  increasing the PROCUSERMAX value 117
z/OSMF server
  cataloged procedures 16, 17
  defining in COMMNDxx member 34
  displaying status 33
  setting up 16, 17
  started tasks 16, 17
  starting 31
  stopping 34
  verifying operation 31

Product Number: 5650-ZOS

Printed in USA

SC27-8419-02