

z/OS



IBM z/OS Management Facility Configuration Guide

Version 2 Release 1

Note

Before using this information and the product it supports, read the information in “Notices” on page 339.

This edition applies to Version 2 Release 1 of IBM z/OS Management Facility (product number 5610-A01) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2009, 2015.**

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

Contents

Figures	vii
----------------	------------

Tables	ix
---------------	-----------

About this document	xi
----------------------------	-----------

Who should use this document	xi
Where to find more information	xi
How to read syntax diagrams	xi

How to send your comments to IBM	xv
---	-----------

If you have a technical problem	xv
---------------------------------	----

Summary of Changes	xvii
---------------------------	-------------

Changes made in z/OSMF Version 2 Release 1, SA38-0657-03	xvii
Changes made in z/OSMF Version 2 Release 1, SA38-0657-02	xvii
Changes made in z/OSMF Version 2 Release 1, SA38-0657-01	xviii
Changes made in z/OSMF Version 2 Release 1, SA38-0657-00	xx
Information applicable to all releases	xxiii

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	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
Selecting a user ID for configuration	14
Security concepts in z/OSMF	15
Input for the core functions	16
Planning for additional instances of z/OSMF	21
Using an override file	21
Choosing a script mode: Interactive or fastpath	21
Reviewing the z/OSMF advanced settings	22
Preparing your workstation for z/OSMF	24
Installing the z/OSMF cataloged procedures	24
Updating your system for the z/OSMF started procedures	25

Updating your system for the z/OS data set and file REST interface	26
Updating the BPXPRMxx member of parmlib	27
Creating a base z/OSMF configuration	29
Before you begin	29
Step 1: Create the initial configuration	33
Step 2: Run the security commands for the z/OSMF resources	36
Step 3: Run the security commands for your user ID	37
Step 4: Verify the RACF security setup	38
Step 5: Complete the setup	39
Step 6: Start the z/OSMF server	41
Step 7: Access the z/OSMF Welcome page	44
Logging into z/OSMF	45

Chapter 4. Migrating to a new release of z/OSMF	47
--	-----------

Pre-migration actions for z/OSMF V2R1	47
Review the ServerPac process	48
Actions to perform before installing z/OSMF V2R1	48
Converting to SAF Authorization Mode	48
Actions to perform before configuring z/OSMF V2R1	50
Retaining the ZOSMFAD user ID from previous releases	50
Migration considerations for the Software Management task	50
Authorize the z/OSMF server to create PassTickets	51
Installing the z/OSMF cataloged procedures	51
Migrating your configuration file and override file	53
Configuring the new release of z/OSMF	55
Considerations for reverting to a previous release of z/OSMF	57
Actions to perform after activating z/OSMF V2R1	58
Notify users of the correct URL to use for z/OSMF V2R1	58
Clean-up actions to perform when satisfied with the new release	58
Review the new z/OSMF service process	58
Review the SAF profile prefix	59
Check the security for ports 32207 and 32208	59
Remove ZOSMFAD owned objects and authorizations from previous releases	59
Remove WebSphere constructs from previous releases	60
Remove the APF authorization for SYS1.MIGLIB(AMATERSE)	60
Remove the SURROGAT class profiles for z/OSMF V1R12	60
Migration action for the September 2014 enhancements	61

Remove the most-generic profile for z/OSMF authorizations	61
---	----

Chapter 5. Planning for the optional z/OSMF plug-ins 63

Overview of z/OSMF system management tasks	64
Capacity Provisioning task overview	65
Configuration Assistant task overview	66
Incident Log task overview	67
ISPF task overview	69
Notifications in z/OSMF	70
Resource Monitoring task overview	71
Software Management task overview	73
System Status task overview	75
Workflows task overview	76
Workload Management task overview	77
Planning security for the z/OSMF plug-ins	79
Setting up security for the z/OSMF tasks and links	80
Planning worksheets for the z/OSMF plug-ins	82
Planning your plug-in selections	82
Input for the Capacity Provisioning task	83
Input for the Incident Log task	84
Input for the Workload Management task	86

Chapter 6. Customizing your system for the z/OSMF plug-ins 87

Using FTP in your network	88
Reviewing your CIM server setup	88
Selecting a user ID for adding plug-ins	89
Updating z/OS for the Capacity Provisioning plug-in	90
Enabling PassTicket creation for Capacity Provisioning task users	91
Updating z/OS for the Configuration Assistant plug-in	92
Updating z/OS for the Incident Log plug-in	93
Defining a couple data set for system logger	96
Setup considerations for log snapshots	98
Enabling the operations log (OPERLOG)	98
Defining and activating the LOGREC log stream	100
Defining diagnostic snapshot log streams	102
Enabling SYSLOG for diagnostic snapshots	102
Configuring automatic dump data set allocation	103
Configuring dump analysis and elimination	104
Creating the sysplex dump directory	105
Ensure that common event adapter (CEA) is configured and active	107
Ensuring that System REXX is set up and active	109
Ensuring that dump data set names are correct	110
Updating z/OS for the ISPF plug-in	111
Updating z/OS for the Resource Monitoring Plug-in	112
Enabling PassTicket creation for Resource Monitoring task users	113
Browser consideration for the Resource Monitoring task	114
Updating z/OS for the Software Deployment plug-in	115

Creating access controls for the Software Management task	115
Creating product information files for the Software Management task	121
Updating z/OS for the Workload Management plug-in	123

Chapter 7. Adding plug-ins to a z/OSMF configuration 127

Chapter 8. Authorizing users to z/OSMF 131

Creating the commands to authorize a user ID	131
Authorizing a user ID	133

Chapter 9. Using z/OSMF in a multi-system environment 135

Configuring z/OSMF for high availability	135
Scenario for using a virtualized instance of z/OSMF	137
Cloning a primary instance of z/OSMF	140
Modifying the z/OSMF host name	141
Additional considerations for a multi-system environment	143
Configuring a primary z/OSMF for communicating with secondary instances	144
Enabling single sign-on between z/OSMF instances	147

Part 3. Post-configuration 149

Chapter 10. Modifying the z/OSMF default keyring name 151

Chapter 11. Customizing the Welcome page for guest users 153

Chapter 12. Linking z/OSMF tasks and external applications 155

Chapter 13. Configuring your system for asynchronous job notifications 157

Creating the CIM indication provider subscription	157
Procedure for creating a subscription	159
Enabling secure job completion notifications for your programs	163

Chapter 14. Adding links to z/OSMF through the izusetup.sh script 167

Managing security for links in z/OSMF	170
---	-----

Chapter 15. Using the verify function as needed	171
--	------------

Chapter 16. Deleting incidents and diagnostic data	173
---	------------

Chapter 17. Troubleshooting problems	177
---	------------

Resources for troubleshooting	177
Tools and techniques for troubleshooting	178
Verifying your workstation with the environment checker	178
Finding information about z/OSMF	186
Working with z/OSMF messages	186
Working with z/OSMF runtime log files	187
Enabling tracing and logging for z/OSMF	188
Examples of working with z/OSMF runtime logs	190
Common problems and scenarios	192
Problems during configuration	192
Problems identified by the Incident Log installation verification program (IVP)	197
Problems when accessing the user interface	204
Problems when using Configuration Assistant	210
Problems when using the ISPF task	210
Problems when using the Incident Log task	212
Problems when attempting to send data	213

Chapter 18. Configuration messages	215
IZUG000-IZUG399	215

Part 4. Appendixes	265
-------------------------------------	------------

Appendix A. Security configuration requirements for z/OSMF	267
---	------------

Appendix B. izusetup.sh script	285
---	------------

Appendix C. Default configuration file and default override file	289
---	------------

Appendix D. Modifying the advanced settings for the z/OSMF configuration .	293
---	------------

Appendix E. Common event adapter (CEA) reason codes	297
--	------------

Appendix F. Contents of the RACF commands execs.	301
---	------------

Appendix G. Format of the installation verification program report	325
---	------------

Appendix H. Example of the migration report.	329
---	------------

Appendix I. Summary of message changes for z/OSMF V2R1	335
New messages	335
Changed messages	336
Deleted messages	336

Appendix J. Accessibility	337
Using assistive technologies	337
Accessibility features for the z/OSMF GUI	337

Notices	339
Policy for unsupported hardware.	340
Minimum supported hardware	341
Programming interface information	341
Trademarks	341

Glossary of terms and abbreviations	343
--	------------

Index	361
------------------------	------------

Figures

1.	z/OSMF 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	25
5.	Format of the RACF ALTUSER command	30
6.	Contents of the izu_env.sh file	32
7.	Expected results from the D A,IZUANG1 command	43
8.	Expected results from the D A,IZUSVR1 command	43
9.	Expected results from the STOP commands	44
10.	z/OSMF Welcome page (before login).	45
11.	z/OSMF Welcome page (after login)	46
12.	Override file updated for SAF Authorization Mode	49
13.	RACF commands for defining the started procedures to the STARTED class	53
14.	Capacity Provisioning task: Main page	65
15.	Configuration Assistant task main page	66
16.	Incident Log sample view.	68
17.	ISPF task main page	69
18.	Notifications main page	71
19.	Resource Monitoring sample view	72
20.	Software Management page	74
21.	System Status sample view	76
22.	Workflows main page	77
23.	Workload Management task main page	78
24.	SAF authorizations in z/OSMF	80
25.	SAF authorizations in z/OSMF: The default setup.	81
26.	z/OS components used in Incident Log task processing	93
27.	Expected results from the D XCF,COUPLE,TYPE=LOGR operator command	96
28.	Expected results from the D C,HC command	99
29.	Expected results from the D LOGREC operator command.	101
30.	Expected results from the D LOGGER operator command.	102
31.	RACF commands to enable CEA to access SYSLOG	103
32.	Expected results from the D A,CEA operator command.	108
33.	Expected results from the D A,AXR operator command.	110
34.	Sample JCL to rename SVC dumps in the sysplex dump directory	110
35.	Sample product information file	122
36.	Override file edited to add a plug-in	128
37.	z/OSMF Welcome page (after you add the optional plug-ins)	130
38.	Output from the izuauthuser.sh script when -list roles is specified	132
39.	Updating the izu_env.sh file	139
40.	Updating the override file	139
41.	Bootstrap properties for z/OSMF	143
42.	Trust relationship when server certificates are signed by the same CA certificate.	146
43.	Trust relationship when the server certificates are signed by different CA certificates	147
44.	Customizable areas of the z/OSMF Welcome page	153
45.	Content of the Welcome page properties file	154
46.	Example of a Welcome page properties file	154
47.	Key components in the application linking process.	155
48.	Sample RACF commands for creating CIM authorizations	159
49.	Subscription values for asynchronous job notification	159
50.	Content of the link properties file.	167
51.	Example of a link definition.	169
52.	Syntax for adding a link to z/OSMF.	169
53.	Example: Defining a link resource name and permitting a group to it	170
54.	Format of the ceatool command	174
55.	Example output from the environment checker tool	179
56.	Sample results from the MODIFY LOGGING operator command.	190
57.	Sample results from the MODIFY LOGGING RESET operator command	190
58.	Portion of a z/OSMF server side log data	190
59.	Example of z/OSMF client side log data	191
60.	Example of the "garbage characters" problem	195
61.	Invoking the Incident Log task IVP as a batch job	198
62.	Checking the sysplex dump directory—sample job for creating an IPCS report	201
63.	Specifying a larger time interval for error log snapshots	204
64.	Digital ring information for the z/OSMF server user ID	206
65.	Default override file	292
66.	Settings that are processed through the izusetup.sh -modify script	295
67.	Sample RACF commands for configuring the core functions of z/OSMF (Part 1 of 5)	302
68.	Sample RACF commands for configuring the core functions of z/OSMF (Part 2 of 5)	303
69.	Sample RACF commands for configuring the core functions of z/OSMF (Part 3 of 5)	304
70.	Sample RACF commands for configuring the core functions of z/OSMF (Part 4 of 5)	305
71.	Sample RACF commands for configuring the core functions of z/OSMF (Part 5 of 5)	306
72.	Sample RACF command for authorizing users to the CIM server resources.	307
73.	Sample RACF commands for configuring the Capacity Provisioning plug-in (Part 1 of 2).	308

74.	Sample RACF commands for configuring the Capacity Provisioning plug-in (Part 2 of 2).	309	84.	Sample RACF commands for configuring the Software Deployment plug-in (Part 1 of 2).	319
75.	Sample RACF commands for configuring the Configuration Assistant plug-in (Part 1 of 2).	310	85.	Sample RACF commands for configuring the Software Deployment plug-in (Part 2 of 2).	320
76.	Sample RACF commands for configuring the Configuration Assistant plug-in (Part 2 of 2).	311	86.	Sample RACF commands for configuring the Workload Management plug-in (Part 1 of 3).	321
77.	Sample RACF commands for configuring the Incident Log plug-in (Part 1 of 3).	312	87.	Sample RACF commands for configuring the Workload Management plug-in (Part 2 of 3).	322
78.	Sample RACF commands for configuring the Incident Log plug-in (Part 2 of 3).	313	88.	Sample RACF commands for configuring the Workload Management plug-in (Part 3 of 3).	323
79.	Sample RACF commands for configuring the Incident Log plug-in (Part 3 of 3).	314	89.	Format of the installation verification program report (Part 1 of 3).	325
80.	Sample RACF commands for configuring the ISPF plug-in (Part 1 of 2).	315	90.	Format of the installation verification program report (Part 2 of 3).	326
81.	Sample RACF commands for configuring the ISPF plug-in (Part 2 of 2).	316	91.	Format of the installation verification program report (Part 3 of 3).	327
82.	Sample RACF commands for configuring the Resource Monitoring plug-in (Part 1 of 2).	317	92.	Sample migration report file (Part 1 of 4).	330
83.	Sample RACF commands for configuring the Resource Monitoring plug-in (Part 2 of 2).	318	93.	Sample migration report file (Part 2 of 4).	331
			94.	Sample migration report file (Part 3 of 4).	332
			95.	Sample migration report file (Part 4 of 4).	333

Tables

1. Planning checklist for a first-time installation	7	27. Summary of tools and information for troubleshooting problems with z/OSMF	177
2. Planning checklist for a migration to a new release	8	28. Columns in the environment checker tool results page	178
3. Planning checklist for adding one or more plug-ins to a configuration	9	29. Recommended settings for Firefox	180
4. Worksheet for the core functions variables	16	30. Recommended settings for Internet Explorer	183
5. Modes for running the izusetup.sh script	22	31. Authorizing the z/OSMF installer user ID for operator commands	194
6. z/OSMF advanced settings	23	32. Responding to system setup errors indicated in the izuincidentlogverify.report file	198
7. Security authorizations created for the z/OS data set and file REST interface	27	33. Class activations that z/OSMF requires	267
8. Sample MOUNT commands for z/OSMF file systems	28	34. User IDs that z/OSMF creates during the configuration process	269
9. Actions and performers for configuring z/OSMF on your z/OS system	29	35. Security groups that z/OSMF creates during the configuration process	269
10. Worksheet for the z/OSMF environment variables	31	36. Security setup requirements for z/OSMF core functions	270
11. Optional plug-ins and associated tasks in z/OSMF V2R1	63	37. Security setup requirements for hardware cryptography with ICSF	274
12. Worksheet for planning your plug-in selections	83	38. CIM groups that might be required for the optional plug-ins	275
13. Worksheet for the Capacity Provisioning task variables	83	39. Name information for a Capacity Provisioning domain	276
14. Worksheet for the Incident Log task variables	84	40. Security groups required for the Capacity Provisioning plug-in	276
15. Worksheet for the Workload Management task variable	86	41. Security setup requirements for the z/OS data set and file REST interface	277
16. z/OS setup actions for the Capacity Provisioning task	90	42. Security setup requirements for the z/OS jobs REST interface	277
17. z/OS setup actions for the Incident Log task	95	43. JESJOBS class authorizations needed for performing job modify operations	277
18. z/OS setup actions for the Resource Monitoring and System Status tasks	112	44. Security group required for the Workload Management plug-in	278
19. Actions users can take against global zones by access authority	116	45. Security setup requirements for the z/OSMF optional plug-ins	278
20. Actions users can take against software instances by access authority	117	46. Default profiles, resource names, and group assignments for z/OSMF	283
21. Actions users can take against deployments by access authority	118	47. Default configuration file	289
22. Actions users can take against categories by access authority	119	48. z/OSMF advanced settings	293
23. Workload Management task authorizations for z/OSMF	125	49. CEA reason codes related to Incident Log task processing	297
24. What variable settings are important for a multi-system environment?	136	50. CEA reason codes related to z/OS jobs REST interface processing	300
25. Script options for verification	171		
26. Sample ceatool commands	175		

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 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 refer to this document for information about completing various post-installation actions, such as configuring the optional plug-ins.

Installations that install z/OSMF from a Custom-Built Product Delivery Option (CBPDO) software delivery package, or from a ServerPac order using the software upgrade method of installation, should plan to manually run the configuration script procedures described in this document. In contrast, installations that install z/OSMF as part of a ServerPac full system replacement will have these scripts run automatically during the ServerPac post-installation process.

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 basic concepts and help them prepare for a career as a z/OS professional, such as a z/OS system programmer.

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

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

To access the z/OS Basic Skills Information Center, open your web browser to the following web site, which is available to all users (no login required): <http://publib.boulder.ibm.com/infocenter/zos/basics/index.jsp>.

How to read syntax diagrams

Throughout this document, diagrams are used to illustrate the programming syntax. The following list tells you how to interpret the syntax diagrams:

- Read the diagrams from left-to-right, top-to-bottom, following the main path line. Each diagram begins on the left with double arrowheads and ends on the right with two arrowheads facing each other.

» Syntax Diagram «

- Required keywords and values appear on the main path line. You must code required keywords and values.

» REQUIRED_KEYWORD «

If several mutually exclusive required keywords or values exist, they are stacked vertically in alphanumeric order.

» REQUIRED_KEYWORD_OR_VALUE_1
REQUIRED_KEYWORD_OR_VALUE_2 «

- Optional keywords and values appear below the main path line. You can choose not to code optional keywords and values.

» KEYWORD «

If several mutually exclusive optional keywords or values exist, they are stacked vertically in alphanumeric order below the main path line.

» KEYWORD_OR_VALUE_1
KEYWORD_OR_VALUE_2 «

- A word in all uppercase is a keyword or value you must spell exactly as shown. In this example, you must code **KEYWORD**.

» KEYWORD «

If a keyword or value can be abbreviated, the abbreviation is discussed in the text associated with the syntax diagram.

- If a diagram shows a character that is not alphanumeric (such as parentheses, periods, commas, and equal signs), you must code the character as part of the syntax. In this example, you must code **KEYWORD=(001,0.001)**.

» KEYWORD=(001,0.001) «

- Default keywords and values appear above the main path line. If you omit the keyword or value entirely, the default is used.

» DEFAULT
KEYWORD «

- A word in all lowercase italics is a *variable*. Where you see a variable in the syntax, you must replace it with one of its allowable names or values, as defined in the text.

» *variable* «

- Some diagrams contain *syntax fragments*, which serve to break up diagrams that are too long, too complex, or too repetitious. Syntax fragment names are in mixed case and are shown in the diagram and in the heading of the fragment. The fragment is placed below the main diagram.

▶▶ | Reference to Syntax Fragment | ◀◀

Syntax Fragment:

|—1ST_KEYWORD,2ND_KEYWORD,3RD_KEYWORD—|

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
SA38-0657-03
- 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>).

Summary of Changes

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

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 147.

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 11, “Customizing the Welcome page for guest users,” on page 153.

The following topic is new: “CEA reason codes for the z/OS jobs REST interface services” on page 300.

New messages were added; see “New messages” on page 335.

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. Usage information is provided in the online help for each task.

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 allows you to create z/OSMF tasks that route requests between z/OSMF instances. To that end, references to the Software Management task in the section about “Configuring a primary z/OSMF for communicating with secondary instances” on page 144 were removed.

Changes made in z/OSMF Version 2 Release 1, SA38-0657-02

This document contains information previously presented in *IBM z/OS Management Facility Configuration Guide*, SA38-0657-01, 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 PI20091 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 PI20091 and the corequisite APARs.

New information

The following topic is new: “Configuring z/OSMF for high availability” on page 135.

z/OSMF adds support for Microsoft Internet Explorer 10. For the complete list of supported browsers and operating systems, see the z/OSMF Supported Browsers web page.

Enhancements are made to the z/OSMF application programming interfaces (APIs). For information, see *IBM z/OS Management Facility Programming Guide*.

Enhancements are made to the existing z/OSMF tasks, as follows:

- The **Incident Log** task supports the use of SSH File Transfer Protocol (SFTP) for sending dumps and logs to IBM or another vendor.
- The **Software Management** task is enhanced, as follows:
 - Supports the use of SFTP for transferring files between remote systems.
 - Allows the user to:
 - View, edit, run, and review the results for jobs generated for a deployment operation directly within the Software Management task
 - View UNIX files.
 - The process of retrieving product information files from the End of Service report is simplified.
- The **Workflows** task is enhanced, as follows:
 - A workflow step can be designed to save its output in a separate file called the *output file*. On completion of the step, the contents of the output file become available for use by subsequent steps in the workflow instance, or by other workflow instances.
 - A workflow step can be designed to be performed conditionally, based on whether a logical condition is satisfied on the z/OS system. For example, a conditional step might become eligible to be performed if a job run by another step ends with a particular return code.

Changed information

If your security management product currently uses the most-generic profile for z/OSMF authorizations (<SAF-prefix>.ZOSMF.**.), it is recommended that you replace it with more discrete authorizations. For information, see “Remove the most-generic profile for z/OSMF authorizations” on page 61.

Changes made in z/OSMF Version 2 Release 1, SA38-0657-01

This document contains information previously presented in *IBM z/OS Management Facility Configuration Guide*, SA38-0657-00, which supported IBM z/OS Management Facility Version 2 Release 1.

New functionality is available for z/OSMF V2R1 when you install APAR PM98630 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 PM98630 and the corequisite APARs.

New information

Import Manager is a new task in the z/OSMF Administration category. Administrators can use the Import Manager task to import plug-ins, event types, event handlers, and links into z/OSMF. For more information, see the online help for the Import Manager task.

Enhancements are made to the existing z/OSMF tasks, as follows:

- The **Application Linking Manager** task allows you to define new event types and handlers by importing a properties file into z/OSMF.

- The **Incident Log** task is enhanced, as follows:
 - Supports the use of a comma, period, or blank as the separator between the different parts of a problem number
 - Provides a new file name format for dumps and logs that are sent to IBM or another vendor.
- The **ISPF** task is enhanced, as follows:
 - You can use the CTRL key as the Enter key
 - You can log in with a logon procedure that omits the account number.
- The **Links** task allows you to define new links by importing a properties file into z/OSMF.
- The **Resource Monitoring** task is enhanced, as follows:
 - Adds support for retrieving and viewing performance data the RMF™ Distributed Data Server collected in the past for all or a subset of the metric groups contained in a monitoring dashboard
 - Allows you to export the data collected in monitoring dashboards into CSV format files on your local workstation, for further data evaluation using a spreadsheet application.
- The **Software Management** task is enhanced, as follows:
 - Provides a data set search capability that allows you to simultaneously add multiple non-SMP/E managed data sets to a software instance
 - Adds support for simultaneously modifying the mount points of multiple UNIX file system data sets while configuring a deployment
 - Provides a list of the UNIX file system data sets that are included in a software instance, and lists the UNIX directories that are contained in each data set.
- The **Workflows** task is enhanced, as follows:
 - You can pre-populate a workflow with user inputs at creation time through a separate properties file that you import
 - Workflow steps can be performed automatically (that is, without user interaction) when the required inputs are provided through a properties file.
- The **Workload Management** task allows you to 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.

The **z/OS data set and file REST interface** is a new application programming interface (API). This API allows an HTTP client application to work with z/OS data sets and UNIX files on the z/OSMF host system. For information about the z/OS data set and file REST interface services, see *IBM z/OS Management Facility Programming Guide*.

The **z/OS data set and file REST interface** requires that a procedure be installed in your system proclib. IBM supplies a default procedure, IZUFPROC, which you must install prior to configuration. Information is provided, as follows:

- For a first-time installation of z/OSMF, see “Installing the z/OSMF cataloged procedures” on page 24 and “Updating your system for the z/OS data set and file REST interface” on page 26.
- If migrating from an earlier release of z/OSMF, see “Installing the z/OSMF cataloged procedures” on page 51.

The **z/OS jobs REST interface** services API is enhanced, as follows:

- A calling application can submit a job to run on a secondary JES2 subsystem. In previous releases, jobs could be submitted to run on the primary JES subsystem only.
- New services are added to allow a calling application to:
 - Hold a job to make it ineligible for processing
 - Release a job that has been held so that it can be selected for processing.

For information about the z/OS jobs REST interface services, see *IBM z/OS Management Facility Programming Guide*.

Changes made in z/OSMF Version 2 Release 1, SA38-0657-00

This document contains information previously presented in *IBM z/OS Management Facility Configuration Guide*, SA38-0652-07, which supported IBM z/OS Management Facility Version 1 Release 13.

New information

In this release, z/OSMF offers reduced resource requirements and faster startup time. In addition:

- You no longer need to set up and configure an instance of IBM WebSphere® Application Server OEM Edition for z/OS for each instance of z/OSMF.
- z/OSMF processing is now managed through the z/OSMF server, which runs as a pair of started tasks on your system. You can control the z/OSMF server through standard z/OS operator commands, such as START and STOP. Ensure that the IBM-supplied cataloged procedures reside in your system proclib, as described in “Updating your system for the z/OSMF started procedures” on page 25.

Prior to configuring z/OSMF, you must ensure that the following product is installed and operational on your system:

IBM 64-bit SDK for z/OS, Java™ Technology Edition, Version 7 (program number 5655-W44). For the required PTFs, see *Program Directory for IBM z/OS Management Facility*, GI11-9847.

In this release, user authorizations to z/OSMF resources (tasks and links) are always managed through your security product. In previous releases, you could manage user authorizations through the Users and Roles tasks. This earlier form of authorization, referred to as *Repository Authorization Mode*, is no longer supported in z/OSMF. Further, z/OSMF no longer uses the concept of *authorization modes*. SAF-based security, previously referred to as *SAF Authorization Mode*, is now the only supported means of managing user authorizations in z/OSMF. As in previous releases, z/OSMF provides shell scripts to assist your security administrator in creating the required definitions (the groups and profiles) in your security product.

If your installation is migrating from an earlier release of z/OSMF that used Repository Authorization Mode, this release includes a REXX exec program to help with converting your existing user authorizations to SAF profiles and groups. See Chapter 4, “Migrating to a new release of z/OSMF,” on page 47.

Appendix A, “Security configuration requirements for z/OSMF,” on page 267 is new in this release. This appendix describes the security configuration requirements for z/OSMF.

The requirement for a special administrator user ID (ZOSMFAD) is removed. The z/OSMF configuration process no longer creates this user ID. Instead, your installation can use any user ID with superuser authority for running the configuration scripts. This user ID is referred to as the *installer user ID* in this document.

The following system management tasks are new in this release:

- **Notifications.** Use this task to view and act on the z/OSMF notifications that have been assigned to you. For an overview, see “Notifications in z/OSMF” on page 70.
- **Workflows.** Use this task to perform a guided set of steps, for example, to configure components or products in your installation. For an overview, see “Workflows task overview” on page 76.

The role z/OS Security Administrator is added in this release. Users with this group authority can perform particular actions in the Workflows task.

You can use the asynchronous job notifications function of z/OSMF to allow your HTTP applications to be notified when submitted jobs complete. With this function, a program that submits a job through the z/OS jobs REST interface services POST 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. This

function is available for the JES2 subsystem only; it is not available for the JES3 subsystem. For instructions on enabling this capability, see Chapter 13, “Configuring your system for asynchronous job notifications,” on page 157.

The following script options are new in this release:

- `-role` is added to the **izuauthuser.sh** script. This option allows you to assign new users to pre-defined roles in z/OSMF.
- `-list roles` is added to the **izuauthuser.sh** script. This option allows you to display the predefined roles in z/OSMF
- `-modify` is added to the **izusetup.sh** script. This option allows you to modify advanced settings for your configuration.

As with previous releases, z/OSMF includes environment variables that control particular aspects of your z/OS UNIX shell session during the configuration process. The following environment variables are new in this release:

JAVA_HOME

Specifies the home directory for IBM 64-bit SDK for z/OS, Java Technology Edition Version 7

PEGASUS_HOME

Specifies the path for the Common Information Model (CIM) server WBEM root directory.

For information, see “Setting the z/OSMF environment variables for your shell session” on page 30.

New messages are added in this release; see “New messages” on page 335.

Changed information

In V2R1, the recommended approach to configuring z/OSMF is changed to provide a smoother configuration experience. New installations are advised to create a base configuration first (with no optional plug-ins selected). When satisfied with the base configuration, you can add plug-ins to the configuration through the `izusetup.sh -add` script, and perform the associated system customizations. After the plug-ins are added, you complete the configuration process by authorizing users to one or more of the defined z/OSMF security groups.

Previously, it was recommended that you create a functionally robust instance of z/OSMF in the initial pass through the configuration scripts, with all or most of the optional plug-ins selected.

For ServerPac installers, if you select the full system replacement installation type, a base configuration is created through a ServerPac post-installation job, using IBM-supplied defaults. Unlike 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. After completing a ServerPac install, you can add plug-ins to z/OSMF through the provided shell scripts, which are described in this document. For details, see “Software delivery options for z/OSMF” on page 5.

As in previous releases, migrating to the new release of z/OSMF includes running the script **izumigrate.sh** to convert your configuration file and override file to the latest formats. This activity produces a report of the configuration variables that are new, changed or removed in the new release. For the specific configuration settings that are changed or removed in z/OSMF V2R1, and for recommendations on migrating an existing RACF® setup, see the report that is generated for your new configuration.

For information about the migration actions for z/OSMF V2R1 and prior releases, see Chapter 4, “Migrating to a new release of z/OSMF,” on page 47.

Some messages are changed in this release; see “Changed messages” on page 336.

Moved information

Information for application programming interfaces (APIs) is moved to a new publication, *IBM z/OS Management Facility Programming Guide*, SA32-1066. These functions include:

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

Descriptions of messages you might encounter while configuring z/OSMF are consolidated in this document, in Chapter 18, “Configuration messages,” on page 215. Previously, these messages were described in the publication , SA38-0654, which is discontinued in this release.

Removed information

Because z/OSMF no longer requires the separate installation and configuration of IBM WebSphere Application Server OEM Edition for z/OS, references to IBM WebSphere Application Server OEM Edition for z/OS in this document are revised or removed.

Also removed are references to the configuration variables associated with the configuration of IBM WebSphere Application Server OEM Edition for z/OS. The removed variables are:

- IZU_WAS_CONFIG_FILE_KNOWN
- IZU_WAS_CONFIG_FILE_LOCATION
- IZU_APPSERVER_GROUP
- IZU_APPSERVER_ROOT
- IZU_WAS_PROFILE_PREFIX
- IZU_CLUSTER_TRANSITION_NAME
- IZU_CELL_SHORT_NAME
- IZU_SERVANT_USERID
- IZU_CONTROL_USERID
- IZU_ORB_PORT.

With the removal of Repository Authorization Mode as a security setup option, references to *authorization mode*, *SAF Authorization Mode*, and *Repository Authorization Mode* are removed from this document. References to related configuration options and functions are likewise removed, as follows:

- References to the IZU_AUTH_MODE configuration variable are removed
- Information about the Users task and Roles task in the z/OSMF Administration category is removed.

As of this release, z/OSMF discontinues support for the following web browser: Microsoft Internet Explorer 7. Users are advised to upgrade to a supported web browser; see the z/OSMF Supported Browsers web page.

References to the configuration variable, IZU_WBEM_ROOT, are removed. This value is now set through the PEGASUS_HOME environment variable, which is described in “Setting the z/OSMF environment variables for your shell session” on page 30.

The script **izuupdate.sh** script is removed. To modify the z/OSMF advanced settings, you can run the script **izusetup.sh** with the new option `-modify`, instead. For information, see “Reviewing the z/OSMF advanced settings” on page 22

Some messages are removed in this release; see “Deleted messages” on page 336.

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 xv. 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.

Chapter 1. Overview of z/OSMF

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



Figure 1. z/OSMF welcome page

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.

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 online help.

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 tasks. These components make up the environment necessary for using the z/OSMF functions. z/OSMF does not provide a separate client installation. You will need to provide a compatible browser to access the z/OSMF web application.

z/OSMF includes the following software:

- 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.

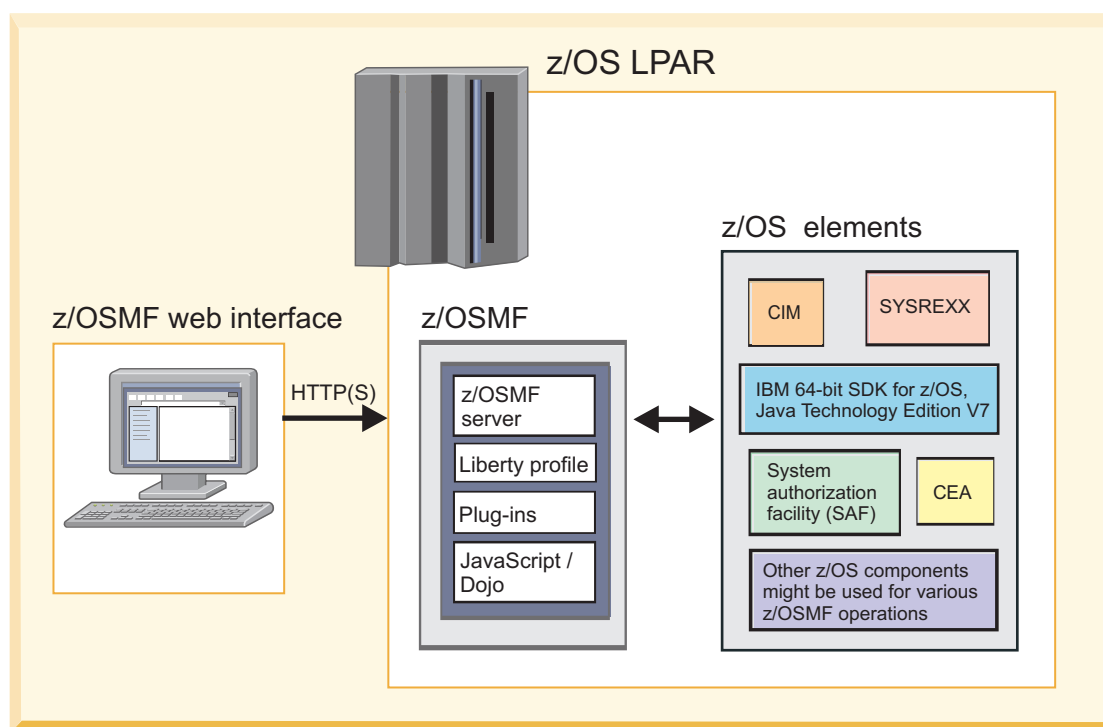


Figure 2. z/OSMF and related system components

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, Version 7. 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. Unlike 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. The steps for adding plug-ins to an existing z/OSMF configuration are described in Chapter 7, “Adding plug-ins to a z/OSMF configuration,” on page 127.
- 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 use the provided shell scripts to set up z/OSMF on your system, and add 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 must set up z/OSMF through shell scripts that are provided with the product.

Software prerequisites

Determine on which z/OS operating system image you want to run this product. z/OSMF V2R1 must be run on z/OS Version 2 Release 1.

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

IBM 64-bit SDK for z/OS, Java Technology Edition, Version 7 (program number 5655-W44). For the required PTFs, see *Program Directory for IBM z/OS Management Facility*, GI11-9847.

This set-up must be done before you run the z/OSMF configuration scripts. By default, the SDK resides in the directory `/usr/lpp/java/` on your system. If you installed it in another location, be sure to include the `JAVA_HOME` export in your shell session, as shown in “Setting the z/OSMF environment variables for your shell session” on page 30.

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.

Installations that install z/OSMF from a Custom-Built Product Delivery Option (CBPDO) software delivery package, or from a ServerPac order using the software upgrade method of installation, should plan to manually run the configuration script procedures described in this document. In contrast, installations that install z/OSMF as part of a ServerPac full system replacement will have these scripts run automatically during the ServerPac post-installation process.

What setup is needed for z/OSMF?

z/OSMF is a z/OS product, and as such, requires careful planning to ensure a smooth installation and configuration process.

Enabling z/OSMF on your system will involve the following phases:

- Planning for z/OSMF.
- Ordering z/OSMF through one of the supported software delivery options: ServerPac or Custom-Built Product Delivery Option (CBPDO).
- Installing z/OSMF. This phase includes the SMP/E installation of z/OSMF, as described in *Program Directory for IBM z/OS Management Facility*, GI11-9847.
- Configuring an instance of z/OSMF in your sysplex. This phase requires certain z/OS resources to be set up, shell scripts to be run, and security set up 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 scripts and the information in this document to assist your security administrator. Information about security setup is provided in "Planning security for the z/OSMF plug-ins" on page 79.

When you migrate to a new release of z/OSMF, you can re-use much of the customization from your current configuration. Migration information for z/OSMF is provided in Chapter 4, "Migrating to a new release of z/OSMF," on page 47.

Receiving service updates for z/OSMF

As with other IBM software products, 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, review the product Preventive Service Planning (PSP) bucket, as referenced in *Program Directory for IBM z/OS Management Facility*, GI11-9847. 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, go to 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 installing z/OSMF for the first time? Or, are you migrating an existing system to the latest release of z/OSMF? Or, perhaps, you only want to add another plug-in to your existing system? 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 required for each task, and provide links to further details.

- “First-time installation”
- “Migrating to the latest release” on page 8
- “Adding a plug-in 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, 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. z/OSMF is available through the usual software delivery methods (ServerPac and CBPDO).	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” on page 5
	Learn about the z/OSMF configuration process and the izusetup.sh script.	System programmer	“The configuration process” on page 13
	Learn what authorities are needed to create a base configuration.	System programmer	“Selecting a user ID for configuration” on page 14
	Gather information about your environment, to be used as input when you run the izusetup.sh script.	System programmer	“Input for the core functions” on page 16
	Understand the considerations for using z/OSMF in a multi-sysplex environment.	System programmer	Chapter 9, “Using z/OSMF in a multi-system environment,” on page 135
	Create an override file, to be used as input when you run the izusetup.sh script.	System programmer	“Using an override file” on page 21
	Verify that your workstation meets the prerequisites for using z/OSMF.	System programmer	“Preparing your workstation for z/OSMF” on page 24
	Set up the z/OSMF started procedures.	System programmer	“Updating your system for the z/OSMF started procedures” on page 25

Table 1. Planning checklist for a first-time installation (continued)

✓	Task summary:	IT role / skills:	Where to find instructions:
	Understand the configuration implications of using z/OSMF in a multi-system environment.	System planners, installation managers, security administrators, and system programmers.	<ul style="list-style-type: none"> • “Configuring z/OSMF for high availability” on page 135 • “Configuring a primary z/OSMF for communicating with secondary instances” on page 144
	Follow a procedure to create a base z/OSMF configuration (core functions only).	Security administrator and system programmer	<ul style="list-style-type: none"> • “Creating a base z/OSMF configuration” on page 29 • “Step 1: Create the initial configuration” on page 33 • “Step 2: Run the security commands for the z/OSMF resources” on page 36 • “Step 3: Run the security commands for your user ID” on page 37 • “Step 4: Verify the RACF security setup” on page 38 • “Step 5: Complete the setup” on page 39.
	Activate z/OSMF by starting the z/OSMF server.	System programmer	“Step 6: Start the z/OSMF server” on page 41
	Open a web browser to the welcome page of a running instance of z/OSMF.	System programmer	“Step 7: Access the z/OSMF Welcome page” on page 44
	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 for “Adding a plug-in to your configuration” on page 9.

Migrating to the latest release

This configuration phase encompasses upgrading an existing (old) release of z/OSMF to the newest release.

Table 2. Planning checklist for a migration to a new release

✓	Task summary:	IT role / skills:	Where to find instructions:
	Learn about the migration process.	System planners, security administrators, and system programmers.	Chapter 4, “Migrating to a new release of z/OSMF,” on page 47
	Perform the pre-migration actions.	System programmer	“Pre-migration actions for z/OSMF V2R1” on page 47
	Perform the migration actions.	System programmer	<ul style="list-style-type: none"> • “Actions to perform before installing z/OSMF V2R1” on page 48 • “Actions to perform before configuring z/OSMF V2R1” on page 50 • “Actions to perform after activating z/OSMF V2R1” on page 58
	Configure the new release of z/OSMF, using migrated configuration and override files.	System programmer	“Configuring the new release of z/OSMF” on page 55

Table 2. Planning checklist for a migration to a new release (continued)

✓	Task summary:	IT role / skills:	Where to find instructions:
	Activate z/OSMF by starting the z/OSMF server.	System programmer	"Step 6: Start the z/OSMF server" on page 41
	When you are certain that you will not need to fallback to your current (old) release, you can perform the post-migration actions.	System programmer	"Clean-up actions to perform when satisfied with the new release" on page 58
	After you are satisfied with the base configuration, you can add function to z/OSMF through the addition of one or more optional plug-ins.	System programmer	See the steps for "Adding a plug-in to your configuration."

Adding a plug-in 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 one or more 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, "Planning for the optional z/OSMF plug-ins," on page 63
	Learn about the z/OSMF tasks.	System programmer	"Overview of z/OSMF system management tasks" on page 64
	Plan the security requirements for users of the z/OSMF tasks.	Security administrator and system programmer	"Planning security for the z/OSMF plug-ins" on page 79
	Gather information about your environment, to be used as input when you run the izusetup.sh script.	System programmer	"Planning worksheets for the z/OSMF plug-ins" on page 82
	Review and perform the z/OS system customization steps for each z/OSMF plug-in. These changes are required for enabling the various system management tasks in z/OSMF.	System programmer	Chapter 6, "Customizing your system for the z/OSMF plug-ins," on page 87
	Add optional plug-ins to z/OSMF using the supplied scripts.	System programmer	Chapter 7, "Adding plug-ins to a z/OSMF configuration," on page 127
	Authorize users or groups to access the z/OSMF tasks.	Security administrator and system programmer	Chapter 8, "Authorizing users to z/OSMF," on page 131

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 10, "Modifying the z/OSMF default keyring name," on page 151
- Chapter 11, "Customizing the Welcome page for guest users," on page 153
- Chapter 12, "Linking z/OSMF tasks and external applications," on page 155

- Chapter 13, "Configuring your system for asynchronous job notifications," on page 157
- Chapter 14, "Adding links to z/OSMF through the izusetup.sh script," on page 167
- Chapter 15, "Using the verify function as needed," on page 171
- Chapter 16, "Deleting incidents and diagnostic data," on page 173
- Chapter 17, "Troubleshooting problems," on page 177
- Chapter 18, "Configuration messages," on page 215.

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 47
- Chapter 5, “Planning for the optional z/OSMF plug-ins,” on page 63
- Chapter 6, “Customizing your system for the z/OSMF plug-ins,” on page 87
- Chapter 7, “Adding plug-ins to a z/OSMF configuration,” on page 127
- Chapter 8, “Authorizing users to z/OSMF,” on page 131
- Chapter 9, “Using z/OSMF in a multi-system environment,” on page 135.

Chapter 3. Configuring z/OSMF for the first time

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

Observe the following considerations:

- It is **strongly recommended** that you review all of the steps in this chapter before performing the configuration.
- If your installation is upgrading from a previous release of z/OSMF, skip this chapter. Instead, follow the instructions in Chapter 4, “Migrating to a new release of z/OSMF,” on page 47.

The configuration process

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

In z/OSMF V2R1, the default path is /usr/lpp/zosmf/V2R1. If this location is different on your system, you will need to set an environment variable, IZU_CODE_ROOT, in the shell before invoking the scripts. Because this variable represents a path, throughout this document, references to the path use the following convention: <IZU_CODE_ROOT>/bin refers to the path /usr/lpp/zosmf/V2R1/bin.

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

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

izusetup.sh

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

izudflt.cfg

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

izudflt.ovr

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

izu_env.sh

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

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

Stage 1 - Configuration

Stage 2 - Security setup

Stage 3 - Server instance creation.

This sequence is critical to a successful configuration. Earlier steps create resources, such as directories, that later steps must act upon, such as changing ownership of the directories. This document assumes that you will carry out the steps in the order in which they are presented.

Configuration stage

During this stage, you run the **izusetup.sh** script to create a file of configuration settings for your z/OS system. The script requires that you provide input about your environment. You can change any values as needed for your system environment. The script saves your information as variables in the configuration file, which is then used as input for subsequent steps in the configuration process.

Security setup stage

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

Server instance creation stage

The configuration process uses the configuration file from the configuration stage to create the z/OSMF server on your system. This stage of the process includes initializing or "priming" the data file, and performing some or all of the following types of system customization, as applicable:

- Allocating and mounting file systems
- Updating parmlib
- Creating z/OSMF directories
- Setting the ownership and permission of these directories.

Selecting a user ID for configuration

Select a user ID to use for running the z/OSMF scripts on your system. This user ID is referred to as the *installer user ID* in this document. Ensure that the installer user ID has superuser authority.

Superuser authority is required so that you can update your system by:

- Creating directories
- Allocating and mounting the z/OSMF data 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. As you proceed through the configuration process, z/OSMF adds more authorizations to your user ID. Specifically, the configuration process creates a RACF commands exec for your user ID with CONNECT statements to groups that are permitted to the required resources.

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 scripts, and the administration tasks that you perform, such as adding optional plug-ins and authorizing users.

If you inadvertently delete the user ID, you can create another one, as long as you assign it all of the necessary authorizations. For the authorizations to copy, see the generated REXX execs. If you inadvertently delete the execs, you can regenerate them by running the script **izusetup.sh** again with option **-config**.

In effect, the user ID that you use to configure z/OSMF becomes the administrator role for z/OSMF. If necessary, you can add more users to the administrator role as needed, through the **izuauthuser.sh** script. Information about the script is provided in Chapter 8, “Authorizing users to z/OSMF,” on page 131.

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 z/OSMF configuration scripts, 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.PFCTL
- 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*.

Security concepts in z/OSMF

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

Besides the ability to authenticate, a would-be z/OSMF user requires authorization to one or more z/OSMF resources (tasks and links), which is necessary before the user can do useful work in z/OSMF (Figure 3).

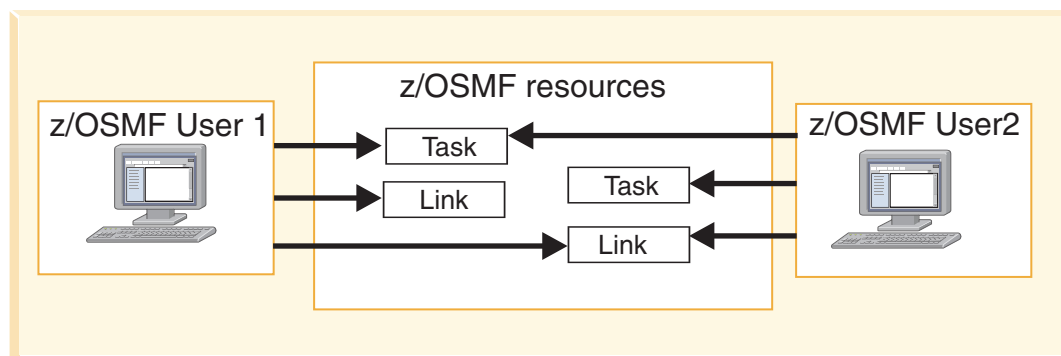


Figure 3. User authorizations in z/OSMF

Establishing security in z/OSMF will require 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.

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

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

Input for the core functions

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

Input for the script prompts and override file

Configuring the core functions requires that you have the following information available (Table 4). This table includes the variable names and defaults, if any, for these values. Gathering some of this information might require the assistance of your installation's security administrator.

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

Table 4. Worksheet for the core functions variables

Input	Description	Variable name	Default value	Your value
Mount point of the z/OSMF data file system.	Mount point (the fully-qualified path name) for the z/OSMF data file system.	IZU_DATA_DIR	/var/zosmf/data	
Name of the z/OSMF data file system.	Name of the z/OSMF data file system. If you pre-create the data file system, ensure that this variable is set to your file system name. The file system must be mounted at the IZU_DATA_DIR mount point (do this manually or allow the configuration script to mount it for you).	IZU_DATA_FS_NAME	IZU.SIZUDATA	
z/OSMF data file system type.	Type of file system (zFS or HFS) to be used for creating the z/OSMF data file system.	IZU_DATA_FS_TYPE	ZFS	

Table 4. Worksheet for the core functions variables (continued)

Input	Description	Variable name	Default value	Your value
Volume name for the z/OSMF data file system, or SMS-managed storage.	<p>Volume serial number (VOLSER) of the DASD to be used for creating the z/OSMF data file system. Specify the VOLSER (without single quotes) to specify a volume, or specify '*' (with single quotes) to let SMS select the volume. Using '*' requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle data set allocation automatically, list the volume explicitly.</p> <p>If you specify a volume, the volume must be online when you begin the configuration process described in this document.</p>	IZU_DATA_FS_VOLUME	'*'	
Allocation size (in cylinders) for the z/OSMF data file system.	<p>Initial space allocation, in cylinders, for the z/OSMF data file system data set. The script uses 90% of this value for the primary allocation and 10% for the secondary allocation.</p> <p>The minimum suggested size (and default) is 200 cylinders, which causes the script to use 180 cylinders for the primary allocation and 20 cylinders for the secondary allocation.</p> <p>For an additional consideration, see "Storage consideration for the Workflows task" on page 20.</p>	IZU_DATA_FS_SIZE	200	
AUTOUID override.	If you have AUTOUID enabled, this variable indicates whether (Y or N) RACF is to assign unused UIDs for all group IDs required during the configuration process. If this variable is set to Y, the other prompts for UID are suppressed.	IZU_AUTOUID_OVERRIDE	N	
AUTOGID override.	If you have AUTOGID enabled, this variable indicates whether (Y or N) RACF is to assign unused GIDs for all group IDs required during the configuration process. If this variable is set to Y, other prompts for GID are suppressed.	IZU_AUTOGID_OVERRIDE	N	
Group name for z/OSMF administrators.	Security group to be used for the z/OSMF administrator role. Any user IDs connected to this group are considered to be administrators.	IZU_ADMIN_GROUP_NAME	IZUADMIN	

Table 4. Worksheet for the core functions variables (continued)

Input	Description	Variable name	Default value	Your value
Group ID (GID) for the z/OSMF administrator or AUTOGID.	Group ID (GID) for the z/OSMF administrator group. Instead of specifying the GID value, you can enter AUTOGID to have RACF automatically generate a unique ID. For more information about the AUTOGID operand, see <i>z/OS Security Server RACF Security Administrator's Guide</i> .	IZU_ADMIN_GROUP_GID	9003	
Group name for z/OSMF users.	Security group to be used for the z/OSMF user role. Any user IDs connected to this group are considered to be users.	IZU_USERS_GROUP_NAME	IZUUSER	
Group ID (GID) for z/OSMF users.	Group ID (GID) for the z/OSMF user group. Instead of specifying the GID value, you can enter AUTOGID to have RACF automatically generate a unique ID. For more information about the AUTOGID operand, see <i>z/OS Security Server RACF Security Administrator's Guide</i> .	IZU_USERS_GROUP_GID	9004	
Group name for unauthenticated users.	Group to be used for unauthenticated users.	IZU_UNAUTHENTICATED_GROUP_NAME	IZUUNGRP	
Group ID for the unauthenticated users.	Group ID to be used for unauthenticated users.	IZU_UNAUTHENTICATED_GROUP_GID	9012	
Group name for the z/OS Security Administrator role.	Group name to be used for the z/OS Security Administrator role. The configuration process permits this group to the Workflows task.	IZU_ZOS_SECURITY_ADMIN_GROUP_NAME	IZUSECAD	
Group ID (GID) for the z/OS Security Administrator role.	Group GID to be used for the z/OS Security Administrator role.	IZU_ZOS_SECURITY_ADMIN_GROUP_GID	9006	
z/OSMF started task user ID.	User ID and credentials for running the z/OSMF started tasks, IZUANG1 and IZUSVR1.	IZU_STARTED_TASK_USERID_NAME	IZUSVR	
z/OSMF started task UID or AUTOUID.	UID for the z/OSMF started task user ID. Instead of specifying the UID value, you can enter AUTOUID to have RACF automatically generate a unique ID.	IZU_STARTED_TASK_USERID_UID	9010	

Table 4. Worksheet for the core functions variables (continued)

Input	Description	Variable name	Default value	Your value
z/OSMF started task home directory.	Home directory for the z/OSMF started task user ID. Some installations might require that this value be substituted with another directory. If so, specify a value that corresponds with the value you specify for the IZU_STARTED_TASK_USERID_NAME variable. For example, if you specify the value IZUSVR for IZU_STARTED_TASK_USERID_NAME, the z/OSMF started task home directory should be set to /var/zosmf/data/home/izusvr.	IZU_STARTED_TASK_USERID_HOME	/var/zosmf/data/home/izusvr	
z/OSMF started task shell program path.	Program path for the z/OSMF started task identity for z/OS UNIX system services. This value is used for the OMVS segment.	IZU_STARTED_TASK_USERID_PROGRAM	/bin/sh	
z/OSMF SAF profile prefix.	SAF profile prefix that will be prepended to the names of any resource profile names to be used for the z/OSMF core functions and optional plug-ins. The prefix is used as input for creating the sample RACF commands in the generated REXX exec programs.	IZU_SAF_PROFILE_PREFIX	IZUDFLT	
HTTP SSL port number.	Port number for SSL encrypted traffic from your z/OSMF configuration. In this release, the default port number is changed from 32208 (the WebSphere default), to 443, which follows the Internet Engineering Task Force (IETF) standard.	IZU_HTTP_SSL_PORT	443	
HTTP port number.	Port number for non-encrypted traffic, which is 80, by default. Note that if your installation is migrating from an earlier release of z/OSMF, you might have specified port number 32207 for this value, which is the WebSphere default.	IZU_HTTP_PORT	80	
z/OSMF server host name.	Host name for the z/OSMF server.	IZU_APPSERVER_HOSTNAME	@HOSTNAME	
Unauthenticated user name.	Provides an unknown user with basic privileges to access the Welcome page, but nothing more.	IZU_UNAUTHENTICATED_NAME	IZUGUEST	
Unauthenticated-user user ID.	Represents an unknown user for security purposes. This user ID is used by the z/OSMF server when no other user credentials are available for web container access. This is a restricted user ID; do not assign a password.	IZU_UNAUTHENTICATED_UID	9011	

Table 4. Worksheet for the core functions variables (continued)

Input	Description	Variable name	Default value	Your value
Do you want to create a Certificate Authority?	<p>Indicates 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.</p> <p>If you specify N, you must provide your own CA for enabling secure communications.</p>	IZU_DEFAULT_CERTAUTH	Y	
z/OS data set and file REST API procedure name.	<p>TSO logon procedure to be used for operations with the z/OS data set and file REST interface services.</p> <p>It is recommended that you accept the default procedure, IZUFPROC, which is supplied by IBM as a cataloged procedure in proclib. In most cases, this procedure should be sufficient for your installation. For instructions, see "Updating your system for the z/OS data set and file REST interface" on page 26.</p> <p>To use an alternative procedure name, specify a value of one to eight alphanumeric characters (A-Z, a-z, 0-9) or special characters (#, \$, or @).</p>	IZU_RESTAPI_FILE_TSOPROC	IZUFPROC	
z/OS data set and file REST API TSO account number.	<p>TSO account number to be used for the logon procedure for the z/OS data set and file REST interface services.</p> <p>Specify value of 1 to 40 alphanumeric characters (A-Z, a-z, 0-9) or special characters (#, \$, or @), or accept the default.</p>	IZU_RESTAPI_FILE_ACCTNUM	IZUACCT	
z/OS data set and file REST API TSO region size.	<p>Region size to be used for the logon procedure for the z/OS data set and file REST interface services.</p> <p>Specify a value from 32768 – 2096128 (kilobytes), or accept the default.</p>	IZU_RESTAPI_FILE_REGION	32768	

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 data 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 z/OSMF data 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 z/OSMF data file system. By default, the initial allocation is 200 cylinders. You can specify a larger allocation on the configuration variable `IZU_DATA_FS_SIZE`.

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.

Planning for additional instances of z/OSMF

You might want to create more instances of z/OSMF— on another system in the same sysplex or in another sysplex. For example, you might want to be able start z/OSMF on another system for high availability purposes. Or, you might want to replicate or clone an instance of z/OSMF to another system or sysplex.

If you plan to use z/OSMF in a multi-system environment, or across sysplexes, the decisions you make during the first-time setup can help to simplify the management of z/OSMF later. You can, for example, deploy the initial instance of z/OSMF in such a way that the product can be started from any system in the sysplex. Doing so can help to address z/OSMF high availability. This is an important consideration when deploying any application in a sysplex environment.

To learn more about these capabilities, see Chapter 9, “Using z/OSMF in a multi-system environment,” on page 135.

Using an override file

You can supply some of your configuration settings in an editable file called the *override file*. The values in this file override the IBM defaults for the z/OSMF configuration properties.

The override file does not need to contain the complete set of properties required for z/OSMF configuration. Rather, it should contain the properties that are most likely to be modified by your installation. With this approach, you can gather your installation values in one place (the override file) and have this file serve as input to the configuration process. You might find that having an override file provides you with a convenient means for gathering and reviewing configuration data at your installation before proceeding with the configuration process.

During the configuration process, specify the override file as input to the configuration script. In response, the configuration process presents your override file values as defaults for the script prompts for any properties specified in the override file. Press Enter to accept each value, or type an alternative value, as needed. If you provide an override file, you must ensure that the variables specified in the override file are set to valid values for your installation. As an added benefit, by specifying values in an override file, you can avoid inadvertently entering an invalid character in response to script prompts, which can cause the script to end in error.

IBM provides an override file with z/OSMF. For the contents of this file, see Appendix C, “Default configuration file and default override file,” on page 289.

Choosing a script mode: Interactive or fastpath

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

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

When used in fastpath mode, the **izusetup.sh** script runs without interactive prompting. Any values not found in the override file are taken from the configuration file. For any value not found in either location, the script ends with an error. Table 5 summarizes the considerations for each mode.

Table 5. Modes for running the izusetup.sh script

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

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

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

Reviewing the z/OSMF advanced settings

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

Table 6 on page 23 describes the advanced settings that are used during the z/OSMF configuration process.

Table 6. z/OSMF advanced settings

izuadmin.env variable	Description	Allowable range of values	Default value
ltpatimeout	Amount of time (in minutes) for LTPA credentials to be forwarded between servers. z/OSMF user sessions expire when this period of time has elapsed. For information, see “Re-authenticating in z/OSMF” on page 208.	25 – 35971	490
ltpacachetimeout	Amount of time (in seconds) for authentication settings to be held in cache.	1500 – 2158260 This value must be less than or equal to the ltpatimeout value multiplied by 60.	29400
sessiontimeout	Amount of time (in minutes) for the session management session timeout.	This value must be at least 5 greater than the ltpatimeout value.	495
izugwrkmanwlmclass	WLM transaction class to be used for managing the execution of long-running work. This setting is applicable if your z/OSMF configuration includes the Software Deployment plug-in.	One to eight alphanumeric characters (A-Z, a-z, 0-9) or special characters (#, \$, or @).	IZUGWORK
izuilunitvalue	Device to be used for storing data sets and z/OS UNIX files for the FTP jobs. This setting is applicable if your z/OSMF configuration includes the Incident Log plug-in.	N/A	SYSDA
izuiltempdirvalue	Temporary directory to be used for sending z/OS UNIX file attachments through FTP. This setting is applicable if your z/OSMF configuration includes the Software Deployment plug-in.	N/A	/tmp
izunotificationsmax	Maximum number of z/OSMF user notifications that can be created for your installation.	1 – 1000	500
izunotificationexpiration	Expiration (in days) for z/OSMF user notifications at your installation.	0 – 1825	30
izuworkflowsmax	Maximum number of z/OSMF workflows that can be created for your installation.	1 – 500	200

A sample **izuadmin.env** file is supplied with z/OSMF in the following directory:

<IZU_CODE_ROOT>/defaults/

where <IZU_CODE_ROOT> is the z/OSMF product file system. By default, this is /usr/lpp/zosmf/V2R1.

To override any of the current settings, use this procedure:

1. Copy the file **izuadmin.env** from the directory <IZU_CODE_ROOT>/defaults to the directory <IZU_CONFIG_DIR>.
2. Edit the <IZU_CONFIG_DIR>/izuadmin.env file using an editor of your choice, updating the settings as needed.

To have your changes take effect as soon as z/OSMF is configured, make the changes before running the script described in “Step 5: Complete the setup” on page 39. If you later decide to change a setting, you can do so through the procedure described in Appendix D, “Modifying the advanced settings for the z/OSMF configuration,” on page 293.

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 29 on page 180 or Table 30 on page 183, 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>.
- 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.

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 178.

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:** When you install the PTFs for APAR PM98630 and the corequisite APARs, z/OSMF requires that a TSO logon procedure be installed in your system proclib. The procedure is used internally by the z/OS data set and file REST interface services. IBM supplies a default procedure, IZUFPROC, which you must install prior to configuration. The default procedure should be sufficient for most z/OS installations. Review the procedure before installing it, however, to ensure that it is suitable for use in your environment.

If appropriate, you can use an alternative logon procedure, if it provides the same function as the shipped IZUFPROC procedure. Specifically, your logon procedure must contain, at a minimum, all of the DD statements from IZUFPROC; these must reference your system data sets that contain the z/OS UNIX REXX exec programs and ISPF libraries. Also, if your installation uses an actual (non-temporary) data set for ISPFPROF, the logon procedure must be configured to allow profile sharing.

IBM supplies the z/OSMF cataloged 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 cataloged 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.

Verify that the z/OSMF server has sufficient authorization

To ensure that the z/OSMF server can be started and stopped by your operations personnel, verify that the z/OSMF started task user ID has sufficient permissions for your environment. By default, this user ID is IZUSVR, but you might have specified another user ID during the configuration process; see Table 4 on page 16. For example, many installations choose to restrict access to the MVS **START** and **STOP** operator commands. If so, ensure that the IZUSVR user ID is authorized to the appropriate resource profiles.

By default, both of the z/OSMF started tasks (IZUANG1 and IZUSVR1) run under the started task user ID, IZUSVR.

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.”

Information about starting the started tasks, and optionally setting them up to start after every IPL, is provided in “Step 6: Start the z/OSMF server” on page 41.

Defining the z/OSMF started procedures to RACF

When you create the base z/OSMF configuration, as described in “Creating a base z/OSMF configuration” on page 29, the generated REXX exec **izuconfig1.cfg.rexx** contains RACF commands for defining the z/OSMF started procedures to the STARTED class. Figure 4 shows the commands that are provided in the exec.

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

Figure 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

When you install the PTFs for APAR PM98630 and the corequisite APARs, 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 24, 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 Chapter 3, “Configuring z/OSMF for the first time,” on page 13 describes the steps for creating a z/OSMF configuration. During this phase, you run a script, called **izusetup.sh**, that collects installation-specific data that is used in the configuration of z/OSMF.

When prompted, specify the TSO logon procedure, along with a corresponding TSO account number and address space region size. The configuration process supplies default values; you can accept the defaults or supply installation-supplied alternative values. Alternatively, you can specify these values in your override file.

The prompts are as follows:

- **IZUG274I: Enter the z/OS data set and file REST API TSO procedure name**
To accept the default value IZUFPROC, press Enter. Otherwise, specify the name of another TSO logon procedure to be used instead. Alternatively, you can specify the TSO logon procedure name on the variable IZU_RESTAPI_FILE_TSOPROC in your override file.
- **IZUG274I: Enter the z/OS data set and file REST API TSO account number**
To accept the default value IZUACCT, press Enter. Otherwise, specify an another TSO account number to be used instead. Alternatively, you can specify the TSO account number on the variable IZU_RESTAPI_FILE_ACCTNUM in your override file.
- **IZUG274I: Enter the z/OS data set and file REST API TSO region size**
To accept the default value 32768, press Enter. Otherwise, specify another valid region size from 32768 – 2096128 (kilobytes). Alternatively, you can specify the region size on the variable IZU_RESTAPI_FILE_REGION in your override file.

On completion of the configuration process, these values are saved in your configuration file.

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, and that the region size is at least 32768 (kilobytes).

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.

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

When you create the z/OSMF configuration, as described in “Creating a base z/OSMF configuration” on page 29, the generated REXX exec **izuconfig1.cfg.rexx** 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 7 describes the authorizations that are created by the generated REXX exec.

Table 7. Security authorizations created 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 26.
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	IZUPPROC	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 26.

For the contents of the generated REXX exec, **izuconfig1.cfg.rexx**, see Appendix F, “Contents of the RACF commands execs,” on page 301.

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 z/OSMF file systems are mounted at IPL time”
- “Using the automount facility” on page 28.

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

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

- **Product file system:** IZU.SIZUHFS is the default file system name for an HFS file system and IZU.SIZUZFS is the default file system name for a zFS file system. The z/OSMF product file system is mounted in read mode at the location specified on the IZU_CODE_ROOT environment variable.
- **Data file system:** The default name is IZU.SIZUDATA. The z/OSMF data file system is mounted in read/write mode at the location specified on the IZU_DATA_DIR configuration variable.

To have these file systems mounted automatically at IPL time, add MOUNT commands for the file systems to your currently active BPXPRMxx parmlib member. For your reference, Table 8 provides sample MOUNT commands.

Table 8. Sample MOUNT commands for z/OSMF file systems

z/OSMF file system to be mounted	MOUNT command example
Product file system	MOUNT FILESYSTEM('IZU.SIZUZFS') MOUNTPPOINT('/usr/lpp/zosmf/V2R1') TYPE(ZFS) MODE(READ)
Data file system	MOUNT FILESYSTEM('IZU.SIZUDATA') TYPE(ZFS) MODE(RDWR) MOUNTPPOINT('/var/zosmf/data') PARM('AGGRGROW') UNMOUNT

Note: The z/OSMF product file system is mounted READONLY, and therefore does not require an UNMOUNT specification on the MOUNT count.

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

```
BPXM048I BPX0INIT FILESYSTEM SHUTDOWN INCOMPLETE.
2 FILESYSTEMS(S) ARE STILL OWNED BY THIS SYSTEM.
```

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

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

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, note that you must pre-create the directory before running the script that configures z/OSMF.

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 running the script that configures z/OSMF, or perform the following steps manually before running the configuration script:

1. Configure your automount policy appropriately for the z/OSMF 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*.

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 *Program Directory for IBM z/OS Management Facility*, GI11-9847.
The examples in this document assume that your installation used the default product directories when installing z/OSMF.
2. Verify that you have completed the planning checklist for a first time installation in Chapter 2, “Project plans for configuring z/OSMF,” on page 7.
3. Print a copy of the worksheet in “Input for the core functions” on page 16, and verify you have collected the information for your environment. You will supply these values as input to the configuration script that you use to set up z/OSMF.
4. Optionally, you have created an override file to be used as input when you run the configuration script. To do so, make a copy of the IBM-supplied override file and update it with any changes to the defaults that you identified in “Input for the core functions” on page 16. For information, see “Using an override file” on page 21.

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 administrator 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 9 shows the performer for each step of the z/OSMF configuration process.

Table 9. Actions and performers for configuring z/OSMF on your z/OS system

Step to perform	Performed by
“Step 1: Create the initial configuration” on page 33.	z/OSMF installer
“Step 2: Run the security commands for the z/OSMF resources” on page 36.	Security administrator
“Step 3: Run the security commands for your user ID” on page 37.	Security administrator
“Step 4: Verify the RACF security setup” on page 38.	Security administrator
“Step 5: Complete the setup” on page 39.	z/OSMF installer
“Step 6: Start the z/OSMF server” on page 41.	z/OS operator
“Step 7: Access the z/OSMF Welcome page” on page 44.	Any authorized z/OSMF user or the z/OSMF installer

How to access and run the script

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

The **izusetup.sh** script resides in the /bin subdirectory of the z/OSMF product file system. By default, this is /usr/lpp/zosmf/V2R1/bin. To access the script, ensure that this directory is specified in your shell environment path.

Ensure that your PATH setting has the correct version of z/OSMF that you want to configure on your z/OS system. To check your path, run the following command from your shell session: `echo $PATH`

If your path does not contain the script directory, you can add it. To do so, enter the export command from z/OS UNIX. In the following example, the export command is used to add the default location for the script directory to the PATH setting:

```
export PATH=/usr/lpp/zosmf/V2R1/bin:$PATH
```

Or, you can ensure that your working directory is included in your PATH, and change to the script directory before running the script. To add your working directory to your search path, specify a period (.) in your search path. In the following example, the working directory is searched last in sequence:

```
PATH='/bin:/usr/local:.'
```

For more information about the z/OS UNIX shell, including how to switch between the shell and TSO/E, see *z/OS UNIX System Services User's Guide*.

Ensuring that your user ID has enough storage

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

For the below-the-bar storage allocation:

- If you plan to run the script in an OMVS session, ensure that the TSO/E region size (REGION) is at least 1G.
- If you plan to run the script in a telnet or rlogin session, ensure that ASSIZE in the OMVS segment for your user profile is at least 1G. This value can also be set through the BPXPRMxx parmlib member.

For the above-the-bar storage allocation, ensure that the MEMLIMIT value for your user ID is at least 1G (the default is 2G). This value can be set in a variety of ways, such as through the MEMLIMIT setting in your OMVS segment, or through the BPXPRMxx or SMFPRMxx parmlib members.

Figure 5 shows the format of the **RACF ALTUSER** command as it would be used to assign the storage allocations for a user. Here, the MEMLIMIT value is set in the OMVS segment for the user.

```
ALU user-name TSO(SIZE(1048576)) OMVS(ASSIZEMAX(1073741824) MEMLIMIT(1G))
```

Figure 5. Format of the RACF ALTUSER command

It is also possible to set the MEMLIMIT temporarily, through the **ulimit** shell command, if your z/OS UNIX system settings are configured to allow this action. Entering **ulimit -G 1** sets the storage limit to 1 gigabyte (1 GB) for the duration of your OMVS session.

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

Setting the z/OSMF environment variables for your shell session

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

Table 10 on page 31 shows the z/OSMF related environment variables that are used during your shell session.

Table 10. Worksheet for the z/OSMF environment variables

Environment Variable	Description	Variable name	Default value	Your value
z/OSMF configuration directory.	Specifies the directory (the fully-qualified path name) for the z/OSMF configuration.	IZU_CONFIG_DIR	/etc/zosmf	
z/OSMF log file directory.	Specifies the directory (the fully-qualified path name) to be used for storing log files created during the z/OSMF configuration process.	IZU_LOGFILE_ DIR	/var/zosmf/ configuration/logs	
z/OSMF root code directory path.	Specifies the mount point (the fully-qualified path name) for the z/OSMF product file system that was created earlier when you ran the jobs described in the <i>Program Directory for IBM z/OS Management Facility</i> , GI11-9847. This value is release-specific; ensure that it matches the installed release of z/OSMF.	IZU_CODE_ROOT	/usr/lpp/zosmf/V2R1	
Path statement for the z/OSMF binary files.	Specifies the /bin subdirectory of the z/OSMF product file system. This value is release-specific; ensure that it matches the installed release of z/OSMF.	PATH	/usr/lpp/zosmf/V2R1/ bin:\$PATH	
_BPX_SHAREAS setting	Specifies whether the child process is to be run in a separate address space from the login shell's address space.	_BPX_SHAREAS	NO This setting can help to avoid a potential out-of-memory error.	
Java home directory	Specifies the home directory (the fully-qualified path name) for IBM 64-bit SDK for z/OS, Java Technology Edition V7 on your system.	JAVA_HOME	/usr/lpp/java/ J7.0_64	
Path statement for the CIM WBEM root directory	Specifies the fully-qualified path name for the Common Information Model (CIM) server WBEM root directory.	PEGASUS_HOME	/usr/lpp/wbem	

To view the active environment values for your shell session, run the following command from your shell session: `env`

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

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

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

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

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

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

1. **Copy the IBM-supplied environment variables file to a read/write directory.** Copy the file to a location that will be accessible from your shell session, such as the z/OSMF configuration directory /etc/zosmf.

Choose a file name that is meaningful; the examples in this section use `izu_env.sh`. This name is case sensitive.

2. **Modify the existing export commands with new values, as needed.** As shown in Figure 6, the IBM supplied environment variables file contains the following export commands:

```
# Default value for the configuration directory
export IZU_CONFIG_DIR=/etc/zosmf
#
# Default value for the logfile directory
export IZU_LOGFILE_DIR=/var/zosmf/configuration/logs
#
# Default value for the product binaries
export IZU_CODE_ROOT=/usr/lpp/zosmf/V2R1
#
# Setup PATH so the zOSMF binaries are accessible.
export PATH=./usr/lpp/zosmf/V2R1/bin:$PATH
#
# For problems with out of memory starting jvms
export _BPX_SHAREAS=NO
#
# Default value for the Java product directory
export JAVA_HOME=/usr/lpp/java/J7.0_64
#
# Default value for the CIM WBEM root directory
export PEGASUS_HOME=/usr/lpp/wbem
```

Figure 6. Contents of the `izu_env.sh` file

Replace any of the exported values, as appropriate. You must ensure that the variables specified in the file are set to valid values for your session. Your values are used as supplied. Specify only the exported values that you want to replace. Any variables that you omit from the file are defaulted to the values shown in Table 10 on page 31.

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

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

Removing command aliases

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

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

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

Refreshing session status (for OMVS users)

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

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

For more information about the status indicators for an OMVS session, see *z/OS UNIX System Services User's Guide*.

Step 1: Create the initial configuration

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

About this step

When you run the **izusetup.sh** script, you specify a configuration file to be created as output, based on your input values. You gathered this input earlier in “Input for the core functions” on page 16. The examples in this document use the name `izuconfig1.cfg` to refer to this output file.

As described in “The configuration process” on page 13, you can use an optional override file to specify the settings for your environment; these values replace the settings found in the IBM-supplied configuration file, `izudflt.cfg`. Any changes that you make to the override file should be completed before you invoke the **izusetup.sh** script. A default copy of the override file is located in the `/usr/lpp/zosmf/V2R1/defaults` directory, which is read-only. To create an override file for your installation, copy the default `izudflt.ovr` file to a read/write directory, and edit the file with an editor of your choice. It is recommended that you use the same name for your override file: `izudflt.ovr`. For the contents of the override file that is supplied with z/OSMF, see Figure 65 on page 292.

As described in “Choosing a script mode: Interactive or fastpath” on page 21, you can run the **izusetup.sh** script either interactively or “quietly” through the fastpath mode. When used in interactive mode, the **izusetup.sh** script provides a prompt environment that makes it easy to modify the configuration settings needed to create a working instance of z/OSMF. However, in some cases, if you prefer to supply the configuration values in a file with no interactive prompting, use the fastpath mode. For more about these modes, see “Using the script interactively” on page 34 and “Using the script in fastpath mode” on page 34.

Regardless of which mode you use, the script does the following:

- Creates an updated configuration file that you will use to complete the configuration process.
- As an aid to your security administrator, the script creates two REXX execs with RACF commands for creating the security definitions for your installation. Information on running the execs is provided in “Step 2: Run the security commands for the z/OSMF resources” on page 36 and “Step 3: Run the security commands for your user ID” on page 37.

For descriptions of the variables provided in the default configuration file, see Appendix C, “Default configuration file and default override file,” on page 289.

Using the script interactively

By default, the script runs in interactive mode. Here, the script prompts you for a number of installation-specific values, such as the z/OSMF data file system, various security group names, and the other values you collected earlier in “Input for the core functions” on page 16. All prompts require a response; either an acceptance of the displayed value, or a value that you enter in response to the prompt. If you specify your installation-specific values in an optional override file, the displayed values will be taken from the override file. Otherwise, you will be presented with the IBM default values (or no value, when an installation-specific value is mandatory).

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

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

- To use an existing configuration file as input, specify the file name as input to the script. This file is expected to reside in the z/OSMF configuration directory `<IZU_CONFIG_DIR>`. Enter Y in response to the script prompt that asks whether to overwrite the existing configuration file. Your changes will be stored in that file (you might want to back up the contents of the file before invoking the configuration script in this manner). To create another configuration file, specify a new file name when prompted by the “save file” message.
- The script prompts you to select which plug-ins are to be configured. Specify N to bypass adding plug-ins; you will add them later, after you have completed an initial z/OSMF configuration. Instructions are provided in Chapter 7, “Adding plug-ins to a z/OSMF configuration,” on page 127.

Using the script in fastpath mode

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

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

Running the script

Authority

Run this script from a user ID with superuser authority (the installer user ID). For the specific authorizations required, see “Selecting a user ID for configuration” on page 14.

Environment

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

Storage allocation

Your user ID should have at least 1 gigabyte (1 GB) of storage allocated for its use. For information, see “Ensuring that your user ID has enough storage” on page 30.

Location

The script resides in the following directory:

`<IZU_CODE_ROOT>/bin`

where `<IZU_CODE_ROOT>` is the z/OSMF product file system. By default, this is `/usr/lpp/zosmf/V2R1`.

Invocation

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

```
izusetup.sh -file izuconfig1.cfg -config  
[-overridefile filename.ovr]
```

Where:

- *izuconfig1.cfg* identifies the configuration file to be created as output.
You can choose another name for the configuration file, but the .cfg file type is required. If you use a different name, choose one that will be easy to remember and make a note of it. You will need to specify this name several times during the z/OSMF configuration process.
- *izudflt.ovr* identifies an optional override file, which you can use to substitute values in place of the IBM defaults. You can choose another name for this file, but the .ovr file type is required.

For descriptions of the options that you can specify on the **izusetup.sh** script, see Appendix B, “izusetup.sh script,” on page 285.

Results

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

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

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

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

As an aid to your security administrator, the script creates two REXX exec programs, as follows:

- A program with sample RACF commands for creating the security definitions for your installation. If your installation uses another security management product, you can create equivalent SAF commands. Information about running the exec is provided in “Step 2: Run the security commands for the z/OSMF resources” on page 36.
- A program with sample RACF commands for authorizing your user ID (the installer user ID) to complete the configuration process. Information about running the exec is provided in “Step 3: Run the security commands for your user ID” on page 37.

This exec is not created if the installer user ID is already defined to the z/OSMF administrator security group (by default, IZUADMIN).

If the configuration directory already contains an exec from a previous configuration attempt, the script creates a backup copy of the original exec, using the exec name followed by a timestamp. Over time, you can review the directory for time-stamped files, and remove them, if desired.

If you need to repeat Step 1, use the -fastpath option

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

Step 2: Run the security commands for the z/OSMF resources

In this step, your security administrator runs a REXX exec program that was generated earlier when you ran the **izusetup.sh** script with option **-config**. This program contains sample RACF commands for creating profiles for z/OSMF resources (the tasks and core functions). It is strongly recommended that your security administrator review the contents of the exec before running it.

About this step

File **izuconfig1.cfg.rexx** contains sample RACF commands that your security administrator can use to secure the z/OSMF resources. The exec also contains commented sections for additional authorizations that might be applicable for your installation.

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

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 exec

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

For a RACF installation, ensure that the following security classes are active before you perform this step:

- 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 generated REXX exec, **izuconfig1.cfg.rexx**. To have the commands issued when the exec runs, uncomment the sections. Or, your security administrator can enter the commands directly, as shown in “Class activations that z/OSMF requires” on page 267.

Running the exec

Authority

This exec 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.

Environment

Run the exec from an OMVS or telnet/rlogin session. You cannot run it from ISHELL.

Location

The exec resides in the configuration file system (**IZU_CONFIG_DIR**). By default, this is **/etc/zosmf**.

Invocation

From your shell session, do the following:

1. Make the **IZU_CONFIG_DIR** directory your active directory. For example:
`cd /etc/zosmf`

2. Run the exec, as follows:

```
./izuconfig1.cfg.rexx
```

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

```
izuconfig1.cfg.rexx | tee  
/var/zosmf/configuration/logs/izuconfig1.cfg.rexx.output
```

For techniques, see *z/OS UNIX System Services User's Guide*.

Results

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

If the exec 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 3: Run the security commands for your user ID

In this step, your security administrator runs a REXX exec program that was generated earlier when you ran the **izusetup.sh** script with option **-config**. This program contains sample RACF commands for authorizing your user ID (the installer user ID) to complete the configuration process.

About this step

File **izuconfig1.cfg.<YOUR-USERID>.rexx** contains sample RACF commands for authorizing the installer user ID to:

- Complete the z/OSMF configuration process
- Log in to the Welcome page at the end of the configuration process
- Perform post-configuration tasks, as needed.

Instead of running this exec, you might prefer to enter the RACF commands directly. If so, examine the contents of the exec carefully to ensure that you create all of the necessary authorizations.

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

This exec is not created if the installer user ID is already defined to the z/OSMF administrator security group (by default, IZUADMIN). If so, you can skip this step, and proceed to “Step 4: Verify the RACF security setup” on page 38.

Before running the exec

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

Running the exec

Authority

This exec 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.

Environment

Run the exec from an OMVS or telnet/rlogin session. You cannot run it from ISHELL.

Location

The exec resides in the configuration file system (IZU_CONFIG_DIR). By default, this is /etc/zosmf.

Invocation

From your shell session, do the following:

1. Make the IZU_CONFIG_DIR directory your active directory. For example:

```
cd /etc/zosmf
```

2. Run the exec, as follows:

```
./izuconfig1.cfg.<YOUR-USERID>.rexx
```

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

```
izuconfig1.cfg.<YOUR-USERID>.rexx | tee  
/var/zosmf/configuration/logs/izuconfig1.cfg.<YOUR-USERID>.rexx.output
```

For techniques, see *z/OS UNIX System Services User's Guide*.

Results

On completion, the exec creates the required security definitions for the installer user ID.

Step 4: Verify the RACF security setup

In this step, your security administrator verifies the RACF security setup that was performed in the previous steps. To do so, your security administrator runs the **izusetup.sh** script with option **-verify racf**. If your installation uses a security management product other than RACF, you can skip this step.

About this step

The **izusetup.sh** script verifies the results of the RACF commands that were performed through the generated REXX execs, described in “Step 2: Run the security commands for the z/OSMF resources” on page 36 and “Step 3: Run the security commands for your user ID” on page 37.

If your security administrator modified the REXX execs before running them, such as changing an access level to a profile or class, the script might interpret the change as an error. If so, you can ignore the related error message.

Running the script

Authority

This script is run by your security administrator.

Environment

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

Location

The script resides in the following directory:

```
<IZU_CODE_ROOT>/bin
```

where **<IZU_CODE_ROOT>** is the z/OSMF product file system. By default, this is /usr/lpp/zosmf/V2R1.

Invocation

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

```
izusetup.sh -file izuconfig1.cfg -verify racf
```


where *izuconfig1.cfg* is the configuration file that was created earlier in “Step 1: Create the initial configuration” on page 33.

Results

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

```
<IZU_LOGFILE_DIR>/izuracverify.report
```

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

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

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

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

If the log file directory already contains a report file from a previous *-verify racf* invocation, the script saves the previous report file in a backup copy, with a timestamp added to the file name.

Step 5: Complete the setup

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

About the script

The **izusetup.sh** script creates an instance of z/OSMF, using the values you supplied earlier as input.

Specifically, the script:

- Initializes or "primes" the z/OSMF data file system and creates the necessary directories and files. This work includes:
 - Allocating the z/OSMF data file system and mounting it, by default, at */var/zosmf/data*.
The script mounts the filesystem with the option *UNMOUNT* to ensure that it is unmounted if the z/OS system becomes unavailable. Also, for a zFS filesystem, the script mounts the filesystem with the option *PARM('AGGREGROW')* to allow the filesystem to grow dynamically, as needed.
 - The script also sets the permissions and ownership of the directories and files in the z/OSMF data file system.
- Creates the home directory for the z/OSMF started task, if this directory does not exist already. By default, the directory is */var/zosmf/data/home/izusvr*.
- Changes ownership and permissions for the other directories that z/OSMF uses.
- Performs other data set allocations, as needed for z/OSMF processing.

Lastly, the script issues message IZUG349I, which provides the link (a URL) for accessing z/OSMF after it is started on your system, as described in “Step 7: Access the z/OSMF Welcome page” on page 44. z/OSMF will be available to users at the indicated URL.

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

Before running the script

Before running the script, observe the following considerations:

- By default, the z/OSMF started task user ID home directory is `/var/zosmf/data/home/izusvr`. If this directory is automount managed, you must pre-create it before running the script.
- Earlier, in “Step 1: Create the initial configuration” on page 33, you might have selected an interim or temporary parmlib data set to be used instead, perhaps because you did not want your system's active parmlib data set to be updated directly by the script. If so, your installation's system programmer must ensure that the temporary parmlib is accessible to z/OSMF by adding it to the list of active parmlib data sets.

Running the script

Authority

Run this script from a user ID with superuser authority (the installer user ID). For the specific authorizations required, see “Selecting a user ID for configuration” on page 14.

Environment

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

Location

The script resides in the following directory:

`<IZU_CODE_ROOT>/bin`

where `<IZU_CODE_ROOT>` is the z/OSMF product file system. By default, this is `/usr/lpp/zosmf/V2R1`.

Invocation

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

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

where `izuconfig1.cfg` is the configuration file that you created previously in “Step 1: Create the initial configuration” on page 33.

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

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

Results

On completion, the script displays message `IZUG349I`, which provides the link for accessing z/OSMF, as described in “Step 7: Access the z/OSMF Welcome page” on page 44. This message is also written to the script log file:

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

where `<IZU_LOGFILE_DIR>` is the log file directory for your installation. By default, this directory is `/var/zosmf/configuration/logs/`. If the script ends with errors, see the troubleshooting actions listed in “Problems during configuration” on page 192.

Step 6: Start the z/OSMF server

Before users can access z/OSMF, the z/OSMF server must be active. This topic describes the commands you can use to control the z/OSMF server and determine whether it is running.

Starting the z/OSMF server manually

To start the z/OSMF server manually, you can enter the MVS **START** command from the operator console. The **START** command specifies the member 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 logging in to the z/OSMF Welcome page.

On server start-up, 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.
```

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 25.

Consider having the server start automatically at system IPL time. For instructions, see “Ensuring that z/OSMF is started at IPL time” on page 43.

Specifying a job name and other parameters

On the **START** command, you can include additional program parameters to be passed to the started procedures, as appropriate for your environment. 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, for example: **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 the your security product, such as RACF. If you plan to run the z/OSMF started tasks under a job name, be sure that the job name is defined in a security profile for your installation.

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

Besides job name, you can also specify the following settings on the **START** command:

IZUMEM='maxmemlimit | NOLIMIT'

Specifies the 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 may be expressed in megabytes (M), gigabytes (G), terabytes (T), or petabytes (P). *nnnnn* can be a value from 0 to 99999, with a maximum value of 16384P. By default, the limit is four gigabytes (4G).

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

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

Observe the following considerations:

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

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, for example:

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

The value must be in quotation marks.

ROOT='directory-path'

z/OSMF root code directory path. By default, the procedures use directory path /usr/lpp/zosmf/V2R1. 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 in quotation marks, and mixed-case filesystem names are supported.

USERDIR='directory-path'

z/OSMF configuration 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 /etc/zosmf. If your installation configured z/OSMF to use another path for the configuration directory, specify that value here, for example: USERDIR='the/new/config/dir'.

The directory path must be in quotation marks, and mixed-case filesystem names are supported.

How to check if the z/OSMF server is running

To determine whether the z/OSMF server is running, you can enter **DISPLAY** commands for the z/OSMF started tasks, IZUANG1 and IZUSVR1, as shown in the examples that follow.

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

```
D A,IZUANG1
```

Figure 7 on page 43 shows an example of the expected results:

```

- 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 7. Expected results from the D A,IZUANG1 command

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

```
D A,IZUSVR1
```

Figure 8 shows an example of the expected results:

```

- 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 8. Expected results from the D A,IZUSVR1 command

Ensuring that z/OSMF is started at IPL time

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

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

Stopping the z/OSMF server

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

```

STOP IZUSVR1
STOP IZUANG1

```

Figure 9 on page 44 shows an example of the expected results:

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

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

Figure 9. Expected results from the STOP commands

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 7: 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 variable `IZU_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 log file that was created when you ran the **izusetup.sh** script, as described in “Step 5: Complete the setup” on page 39. This log file is in the format:

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

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

Figure 10 on page 45 shows the Welcome page prior to login. Because you have not yet authenticated with z/OSMF by logging in, the header displays *Welcome guest*.

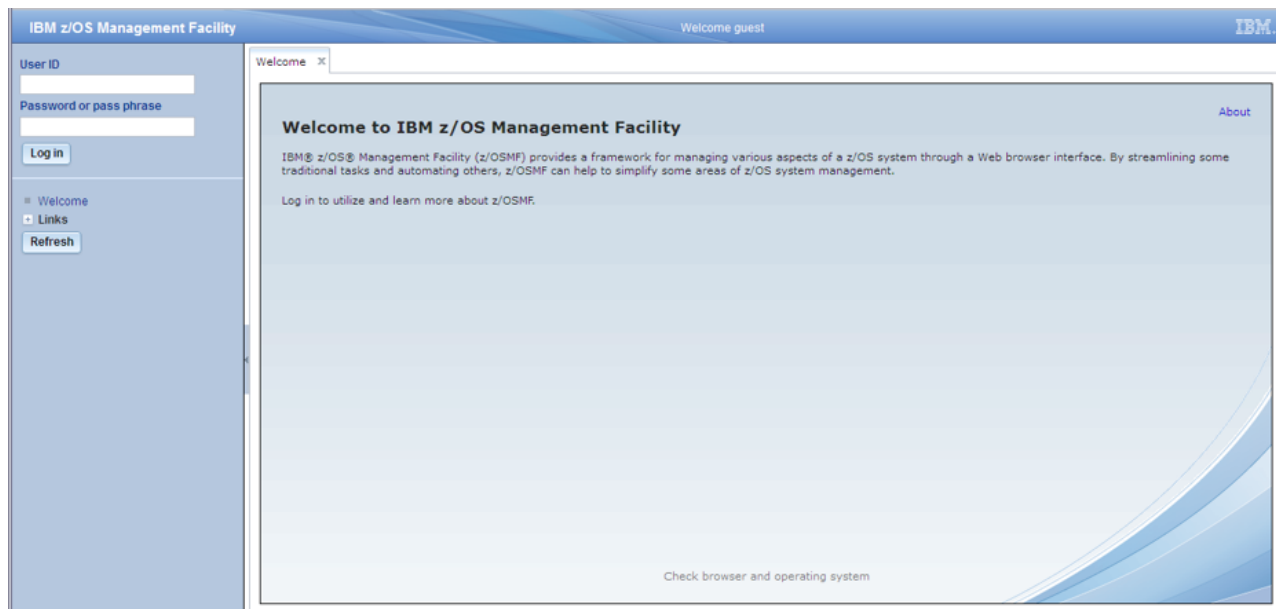


Figure 10. z/OSMF Welcome page (before login)

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 178.

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 205 for information.

Logging into z/OSMF

To log into z/OSMF, enter a valid z/OS user ID and password or pass phrase in the **Log in** 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 11 on page 46 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, Workflows, and the default links. In Figure 11 on page 46, the Links task, and the z/OSMF Administration and z/OSMF Settings categories are expanded to show the links and tasks.

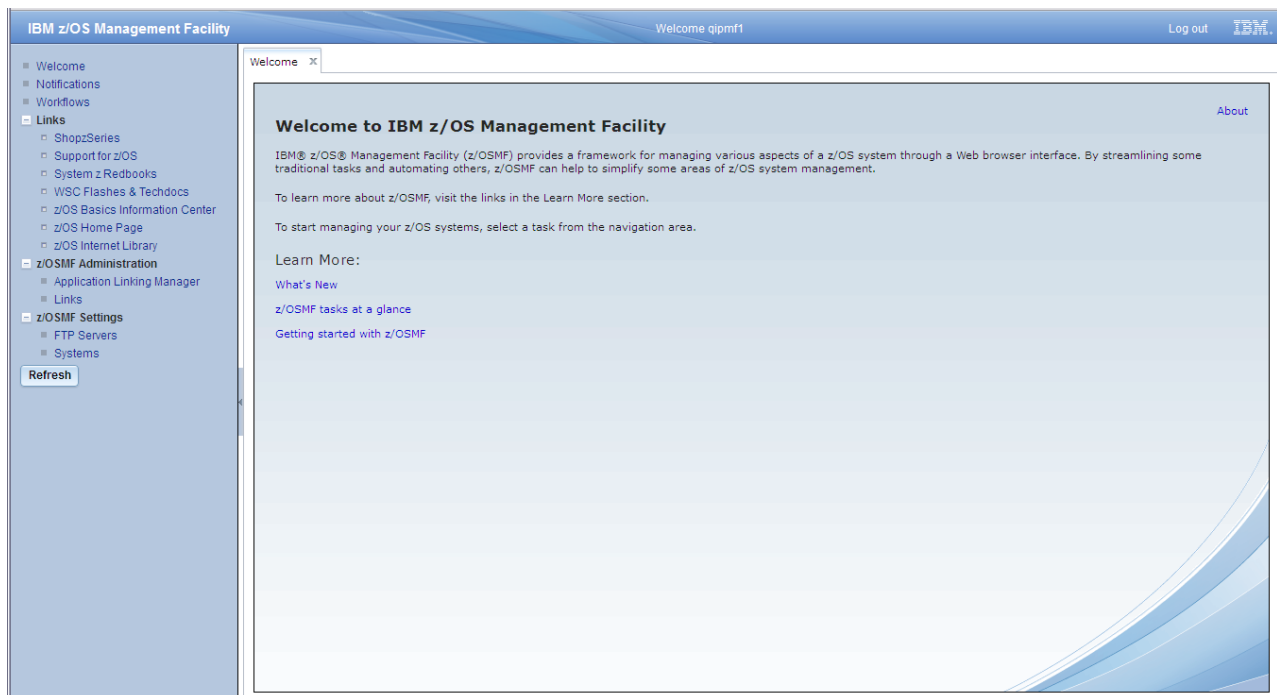


Figure 11. z/OSMF Welcome page (after login)

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.

Later, after 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 a plug-in to your configuration” on page 9.

Figure 11 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.

What to do next

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

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

This chapter describes how to migrate to z/OSMF V2R1 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 V2R1. 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 127.

Migrating to a new release of z/OSMF involves the following steps:

1. Perform the pre-migration actions, as described in “Pre-migration actions for z/OSMF V2R1.”
2. Perform the migration actions. To identify the timing of migration actions, this document groups the actions under the following headings:
 - “Actions to perform before installing z/OSMF V2R1” on page 48. These are migration actions that you perform on your current (old) system, either because they require the current system or because they are possible on the current system.
 - “Actions to perform before configuring z/OSMF V2R1” on page 50. These are migration actions that you perform after you have SMP/E installed z/OSMF V2R1 on a z/OS V2R1 system, but before you have configured the product.
Beginning with z/OSMF V2R1, processing is now 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.
 - “Actions to perform after activating z/OSMF V2R1” on page 58. These are migration actions that you can perform only after you have started the z/OSMF server.
3. Configure the new release of z/OSMF, using migrated configuration and override files. Follow the steps described in “Configuring the new release of z/OSMF” on page 55. Here, you will follow all of the phases of the configuration process to set up and verify the new release of z/OSMF on your system.
4. Generally, after migrating to a new release of z/OSMF, you should not attempt to return (fallback) to a previous release of the product. Doing so can result in configuration script errors or a configuration that is difficult to manage. Before attempting a fallback, see “Considerations for reverting to a previous release of z/OSMF” on page 57.
5. Activate z/OSMF V2R1 by starting the z/OSMF server.
6. When you are certain that you will not need to fallback to your current (old) release, you can perform the post-migration actions. See “Clean-up actions to perform when satisfied with the new release” on page 58.
7. When installing the September 2014 enhancements, you have an additional migration action to perform. See “Migration action for the September 2014 enhancements” on page 61.

Pre-migration actions for z/OSMF V2R1

Before migrating to the new release of z/OSMF, perform the pre-migration actions described in this topic.

z/OSMF V2R1 introduces a number of pre-migration actions, as follows:

- “Review the ServerPac process” on page 48
- “Actions to perform before installing z/OSMF V2R1” on page 48.

Review the ServerPac process

If your installation has used ServerPac in the past to install z/OSMF, see the information that follows for the changes in this release.

Observe the following considerations:

- If you select the **ServerPac full system replacement installation type**, the ServerPac process creates a default z/OSMF instance for you, using a ServerPac post-installation job. Unlike previous releases, the default instance does not include any of the optional plug-ins, such as Configuration Assistant, Incident Log, and so on. Instead, the instance uses a base z/OSMF configuration (core functions only). It is recommended that you use the base configuration to verify your initial setup, for example, by starting the z/OSMF server and logging in to the z/OSMF Welcome page. When you are satisfied with the base configuration, you can add plug-ins to the configuration later, after completing the ServerPac installation. For information, see Chapter 7, “Adding plug-ins to a z/OSMF configuration,” on page 127.
- If you select the **ServerPac software upgrade installation type**, you must create the initial instance of z/OSMF, using the planning and configuration information in this document. As in previous releases, you can use the provided shell scripts to manually configure z/OSMF on your system, and add plug-ins to it.

Actions to perform before installing z/OSMF V2R1

This topic describes z/OSMF migration actions that you can perform on your current (old) system. You do not need the z/OSMF V2R1 level of code to make these changes, and the changes do not require the z/OSMF V2R1 level of code to run after they are made.

Converting to SAF Authorization Mode

For z/OSMF V1R13 installations migrations only: If your current (old) system is currently running z/OSMF V1R13 in Repository Authorization Mode, you can optionally convert your existing security setup to SAF Authorization Mode before moving to z/OSMF V2R1. Doing so will require you to repeat the steps of the z/OSMF configuration process, supplying your current configuration file as input. The z/OSMF configuration process generates new REXX execs, which your security administrator can use to set up security for z/OSMF and authorize additional users to the product. If more than the default set of user authorizations is required, your security administrator is responsible for converting your existing z/OSMF user authorizations to SAF profiles and groups, for use under SAF authorization mode.

If your current (old) system is currently running z/OSMF V1R12, you must convert to SAF Authorization Mode when configuring the new release of z/OSMF on your system.

Procedure for converting to SAF Authorization Mode on a V1R13 system

This procedure assumes that:

- You have a valid z/OSMF configuration
- The z/OSMF data file system is mounted
- IBM WebSphere Application Server OEM Edition for z/OS has been started previously.

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

1. **Stop the WebSphere server.** Ensure that IBM WebSphere Application Server OEM Edition for z/OS is not running. If IBM WebSphere Application Server OEM Edition for z/OS is active, you must enter the appropriate STOP command to shut it down.
2. **Configure z/OSMF as you normally would, but specify SAF Authorization Mode for your configuration.** For example, if you use an override file when configuring z/OSMF, you can specify the authorization mode as a property in your override file, as shown in Figure 12 on page 49.


```
IZU_AUTHORIZATION_MODE=SAF
```

Figure 12. Override file updated for SAF Authorization Mode

Run the **izusetup.sh** script, as follows:

```
izusetup.sh -file izuconfig1.cfg -config  
-overridefile filename.ovr] [-fastpath]
```

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

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

For reference on the **izusetup.sh** script and the z/OSMF configuration process, see “Step 1: Create the initial configuration” on page 33.

3. **Have your security administrator run the security commands for the new authorization mode.**

When you convert an existing z/OSMF configuration to SAF Authorization Mode, the configuration process creates two security commands REXX execs for your use:

- `izuconfig1.cfg.rexx` contains the complete set of RACF commands for a new configuration.
- `izuconfig1.cfg.convertFromREptoSaf.rexx` contains only the delta of security commands of RACF commands that are required for setting up security under SAF Authorization Mode.

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

With the `IZU_CONFIG_DIR` directory as your active directory, run the REXX exec. For example:

```
./izuconfig1.cfg.convertFromREptoSaf.rexx
```

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

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

For reference, see “Step 2: Run the security commands for the z/OSMF resources” on page 36.

4. **Have your security administrator verify the security for the configuration.** Run the **izusetup.sh** script, as follows:

```
izusetup.sh -file izuconfig1.cfg -verify racf
```

For reference, see “Step 4: Verify the RACF security setup” on page 38.

5. **Prime the z/OSMF data file system.** Run the **izusetup.sh** script, as follows:

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

For reference, see the topic “Step 4. Prime the z/OSMF data file system” in your copy of the *z/OSMF Configuration Guide* for z/OSMF V1R13. (The `-prime` option is removed in z/OSMF V2R1.)

6. **Complete the setup.** From the administrator user ID (ZOSMFAD, by default), run the **izusetup.sh** script, as follows:

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

This script might take some time to complete. As it runs, the script writes messages to the script log file. For reference, see “Step 5: Complete the setup” on page 39.

7. **Restart the WebSphere server.**

Actions to perform before configuring z/OSMF V2R1

This topic describes z/OSMF migration actions that you can perform after you have installed z/OSMF V2R1, but before you create a new configuration. These actions might require the z/OSMF V2R1 level of code to be installed, but do not require it to be active.

The following migration actions are described:

- “Retaining the ZOSMFAD user ID from previous releases”
- “Migration considerations for the Software Management task”
- “Authorize the z/OSMF server to create PassTickets” on page 51
- “Installing the z/OSMF cataloged procedures” on page 51
- “Migrating your configuration file and override file” on page 53.

Retaining the ZOSMFAD user ID from previous releases

In previous releases of z/OSMF, the configuration process created a special user ID known as the z/OSMF administrator user ID. By default, the user ID was ZOSMFAD. You used this user ID for running configuration scripts and performing administration tasks, such as adding users and working with z/OSMF log files.

In z/OSMF V2R1, the configuration process no longer creates, or requires the use of, the administrator user ID. Though z/OSMF retains the concept of an administrator role, you can use any existing user ID for this purpose, as long as you define the user ID to the z/OSMF administrator security group (IZUADMIN).

If you want to continue using the ZOSMFAD in z/OSMF V2R1, you must ensure that it has superuser authority, which is needed for running the z/OSMF configuration scripts. At a minimum, ensure that ZOSMFAD has the following UNIXPRIV class profile privileges:

- CONTROL access to SUPERUSER.FILESYS
- UPDATE access to SUPERUSER.FILESYS.MOUNT
- READ access to SUPERUSER.FILESYS.CHOWN
- READ access to SUPERUSER.FILESYS.CHANGEPERMS
- READ access to SUPERUSER.FILESYS.PFSCTL

If you do not want to continue using the ZOSMFAD user ID (or whichever value you specified for IZU_ADMIN_NAME) for z/OSMF V2.1, then, after you stop using your existing z/OSMF release, you can remove this user ID and its associated authorizations. For information, see “Remove ZOSMFAD owned objects and authorizations from previous releases” on page 59.

Migration considerations for the Software Management task

In z/OSMF V1R13 (prior to APAR PM73833), the deployment functions were provided in the Deployment task. In z/OSMF V2R1, the name of this task is changed to Software Management to reflect the software management functions that are provided in addition to the deployment functions.

If your installation used SAF Authorization Mode in z/OSMF V1R13 and used the following default, generic profile to control access to the Deployment task, no migration actions are required:

```
<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.**
```

If your installation chose not to use the generic profile and instead created a discrete profile to control access to the Deployment task, a migration action is required. For example, suppose your installation created the following profile to control access to the Deployment task in z/OSMF V1R13:

```
<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DEPLOYMENT
```

Because the name changed in z/OSMF V2R1, your installation will need to create a generic profile like the default or a discrete profile like the following to control access to the Software Management task:

```
<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT
```

Authorize the z/OSMF server to create PassTickets

If your current (old) system includes the Capacity Provisioning plug-in or the Resource Monitoring plug-in, these functions might be using PassTickets for secure communication with a remote server. PassTickets provide an alternative to passwords. If so, you must ensure that the z/OSMF server user ID is authorized to create PassTickets in the same way that you did for the WebSphere servant user ID on previous systems. By default, this user ID is WSSRU1.

- For the Capacity Provisioning plug-in, determine whether your installation is using PassTickets to authenticate requests against the CIM server on a remote system. If so, you defined the profile IRRPTAUTH.CFZAPPL.* in the PTKTDATA class. To authorize the z/OSMF server to create PassTickets, grant the z/OSMF started task user ID at least UPDATE access authority to this resource. For example:

```
PERMIT IRRPTAUTH.CFZAPPL.* CLASS(PTKTDATA) ID(passticket_creator_userid)
ACCESS(UPDATE)
SETROPTS RACLIST(PTKTDATA) REFRESH
```

where *passticket_creator_userid* is the z/OSMF started task user ID. By default, this is IZUSVR.

- For the Resource Monitoring plug-in, determine whether your installation is using PassTickets to authenticate requests against the RMF Distributed Data Server (DDS) on a remote system. If so, you defined the profile IRRPTAUTH.GPMSEVER.* in the PTKTDATA class. To enable PassTicket creation for the z/OSMF server, give the z/OSMF started task user ID at least UPDATE access authority. For example:

```
PERMIT IRRPTAUTH.GPMSEVER.* CLASS(PTKTDATA) ID(passticket_creator_userid)
ACCESS(UPDATE)
SETROPTS RACLIST(PTKTDATA) REFRESH
```

where *passticket_creator_userid* is the z/OSMF started task user ID. By default, this is IZUSVR.

For more information about PassTickets, see *z/OS Security Server RACF Security Administrator's Guide*. For information about clean-up actions for IBM WebSphere Application Server OEM Edition for z/OS, see "Remove WebSphere constructs from previous releases" on page 60.

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:** When you install the PTFs for APAR PM98630 and the corequisite APARs, z/OSMF requires that a TSO logon procedure be installed in your system proclib. The procedure is used internally by the z/OS data set and file REST interface services. IBM supplies a default procedure, IZUFPROC, which you must install prior to configuration. The default procedure should be sufficient for most z/OS installations. Review the procedure before installing it, however, to ensure that it is suitable for use in your environment.

If appropriate, you can use an alternative logon procedure, if it provides the same function as the shipped IZUFPROC procedure. Specifically, your logon procedure must contain, at a minimum, all of the DD statements from IZUFPROC; these must reference your system data sets that contain the z/OS UNIX REXX exec programs and ISPF libraries. Also, if your installation uses an actual (non-temporary) data set for ISPFPROF, the logon procedure must be configured to allow profile sharing.

IBM supplies the catalogued procedures for z/OSMF 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.

Information about starting the started tasks, and optionally setting them up to start after every IPL, is provided in “Step 6: Start the z/OSMF server” on page 41.

Verify that the z/OSMF server has sufficient authorization

To ensure that the z/OSMF server can be started and stopped by your operations personnel, verify that the z/OSMF started task user ID has sufficient permissions for your environment. By default, this user ID is IZUSVR, but you might have specified another user ID during the configuration process; see Table 4 on page 16. For example, many installations choose to restrict access to the MVS **START** and **STOP** operator commands. If so, ensure that the IZUSVR user ID is authorized to the appropriate resource profiles.

By default, both of the z/OSMF started tasks (IZUANG1 and IZUSVR1) run under the started task user ID, IZUSVR.

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.”

Defining the z/OSMF started procedures to RACF

When you create the new z/OSMF configuration, as described in “Configuring the new release of z/OSMF” on page 55, the generated REXX exec **izuconfig1.cfg.rexx** contains RACF commands for defining the z/OSMF started procedures to the STARTED class. Figure 13 on page 53 shows the commands that are provided in the exec.

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

Figure 13. 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*.

Migrating your configuration file and override file

This section describes the steps for migrating your configuration file and override file to the latest format, using the IBM-supplied script **izumigrate.sh**.

About this script

This script migrates your configuration file, and, if specified, your override file from a previous release of z/OSMF to the latest format. Perform this step from your new (z/OS V2R1) system.

In updating the configuration file and override file, the script retains your current settings when possible. For any properties that are no longer valid for z/OSMF, the script omits the properties when creating the updated files.

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

If you migrate an existing override file, understand that:

- The script processes only the properties that are specified in the override file. The script does not add any new properties to the updated override file. To see which properties are added for the new release, see the report that the **izumigrate.sh** script creates. Then, you can edit the updated override file and add any new properties that are pertinent to your installation.
- The script determines the version of the override file by examining the override file property `IZU_OVERRIDE_FILE_VERSION`. This property, which was introduced in z/OSMF V1R12, should not be modified. If this property is missing from the override file, the script processes the override file as though it had originated from a z/OSMF V1R11 configuration. If this property is set incorrectly in the override file, the script fails with an error message.
- If your existing override file contains user comments, these sections are retained in the updated override file, though the placement of them might change as a result of the processing, which removes properties that no longer apply.

You can migrate the configuration file and override file together in one invocation of the script. Or, if you prefer, you can migrate these files individually through separate invocations of the script.

Other outputs from the script include the following:

- The script records the results of the migrate operation in the migration report file. You can review this file to see what settings were changed during the migrate operation, and what new properties are available.
- The script saves backup copies of your current configuration and override files, for historical purposes.

For the contents of the configuration file and override file that were supplied in this release of z/OSMF, see Appendix C, “Default configuration file and default override file,” on page 289.

After you have successfully migrated your configuration file, and, if specified, your override file, you can configure the new release of z/OSMF, as described in “Configuring the new release of z/OSMF” on page 55.

Running this script

Run the script from your new (z/OS V2R1) 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 file system. By default, this is /usr/lpp/zosmf/V2R1/bin.

Syntax

Run the script, as follows:

```

▶▶—izumigrate.sh— -file—izuconfig1.cfg—————▶▶
                  |— -overridefile—izudflt.ovr—————▶▶
                  |— -file—izuconfig1.cfg— -overridefile—izudflt.ovr—▶▶

```

Where:

- *izuconfig1.cfg* identifies the configuration file from a previous release of z/OSMF. This file is expected to reside in the z/OSMF configuration directory <IZU_CONFIG_DIR>.
- *izudflt.ovr* identifies an override file from a previous release of z/OSMF. This file is expected to reside in the z/OSMF configuration directory <IZU_CONFIG_DIR>.

The script saves the updated files, along with a backups of your current files, to the directory specified on the IZU_CONFIG_DIR configuration variable. By default, this is /etc/zosmf.

As the script runs, it writes log information to the z/OSMF log file directory, which is identified by the IZU_LOGFILE_DIR environment setting for the UNIX shell. By default, this directory is /var/zosmf/configuration/logs/.

Examples

You can migrate the configuration file and override file together in one invocation of this script. Or, if you prefer, you can migrate these files individually through separate invocations of the script.

- To migrate a configuration file, run the script as follows:
`izumigrate -file izuconfig1.cfg`
- To migrate an override file, run the script as follows:
`izumigrate -overridefile izudflt.ovr`
- To migrate a configuration file and an override file, run the script as follows:
`izumigrate -file izuconfig1.cfg -overridefile izudflt.ovr`

Results

On completion, the **izumigrate.sh** script migrates your configuration file to the correct format for the new release of z/OSMF. If you included an override file as input, the script migrates the override file in a similar manner.

As part of this processing, the script creates backups of your existing files, using a file name qualifier to help you correlate the backups with the particular release of z/OSMF. If your installation is migrating from z/OSMF V1R13, for example, the script creates backup files named `izuconfig1.cfg.V1R13` and `izudflt.ovr.V1R13`. If your installation is migrating from z/OSMF V1R12, the script creates backup files named `izuconfig1.cfg.V1R12` and `izudflt.ovr.V1R12`.

In the event that your installation needs to regress to an older level of z/OSMF, you can rename these files to their original names and use them again in the regressed configuration. For related information, see “Considerations for reverting to a previous release of z/OSMF” on page 57.

The script also creates a report file named **izumigration.report**. The report file records the actions that were taken to migrate your configuration and override files—the settings that have been modified, removed, or added between releases. The report file is divided into two sections, one for the configuration file and one for the override file, if applicable.

You can view the migration report file in the `<IZU_LOGFILE_DIR>` directory, which is the location identified by the `IZU_LOGFILE_DIR` environment setting for the UNIX shell. By default, this is `/var/zosmf/configuration/logs/`. The location of the migration report file is also provided in an informational message that is written to the script log file.

Sample migration report file

For your reference, a sample migration report is shown in Appendix H, “Example of the migration report,” on page 329. In this example, the report file records the results of updating the configuration file and the override file from the z/OSMF V1R13 format to the z/OSMF V2R1 format.

What to do next

After you have successfully migrated your configuration file, you must now configure the new release of z/OSMF, as described in “Configuring the new release of z/OSMF.”

Configuring the new release of z/OSMF

In this topic, you will configure the new release of z/OSMF, supplying the updated configuration and override files as input to the z/OSMF configuration process.

To configure the new release of z/OSMF, follow these steps:

1. **If you are using an override file:** If you use an override file when configuring z/OSMF, you can specify it as input to the **izusetup.sh** script. Use the latest format of the override file, which you created in “Migrating your configuration file and override file” on page 53. To this file, you can add any values that you want to specify for z/OSMF V2R1 to avoid having to enter the values later as responses to the script prompts. If you do not use an override file, you can skip this step. The script will prompt you for your configuration values as it runs.
2. **Run the `izusetup.sh` script, as follows:**

```
izusetup.sh -file izuconfig1.cfg -config  
[-overridefile filename.ovr]
```

where `izuconfig1.cfg` is the configuration file that was converted to the latest format in “Migrating your configuration file and override file” on page 53. You will overwrite this file.

If you omitted the override file, the script prompts you for any plug-ins to be added. You are prompted only for plug-ins that are not already included in your configuration. Specify N to bypass adding plug-ins; you can add them later.

On completion, the **izusetup.sh** script creates REXX exec programs with RACF commands for creating the security definitions for your installation. These programs contain sample RACF commands for creating profiles for securing z/OSMF resources (the tasks and core functions). The execs are stored in the IZU_CONFIG_DIR directory.

For reference on the **izusetup.sh** script and the z/OSMF configuration process, see “Step 1: Create the initial configuration” on page 33.

3. **Have your security administrator run security commands for the configuration.** Determine which generated exec is appropriate for your migration path, as follows:

- If you are migrating from a release of z/OSMF that used SAF Authorization Mode, run the exec **izuconfig1.cfg.rexx**. It contains the complete set of RACF commands needed for securing the z/OSMF functions and tasks. The exec also contains commented sections for additional authorizations that might be useful for your installation.
- If you are migrating from a release of z/OSMF that used Repository Authorization Mode, run the exec **izuconfig1.cfg.convertFromREPTtoSAF.rexx**. This file contains only the commands that are needed for creating SAF-based authorizations in your security product.

Have your security administrator review the contents of the exec before running it.

Then, with the IZU_CONFIG_DIR directory as your active directory, run the exec, as follows:

```
./izuconfig1.cfg.rexx
```

or

```
./izuconfig1.cfg.convertFromREPTtoSAF.rexx
```

Tip: If you want a log file, you can use a z/OS UNIX command, such as tee, to direct the output from this exec to a log file. For example, you could direct this output to the z/OSMF log file directory for your installation (IZU_LOGFILE_DIR). By default, this is /var/zosmf/configuration/logs/.

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

For reference, see “Step 2: Run the security commands for the z/OSMF resources” on page 36.

4. **Have your security administrator run security commands for the installer’s user ID.** Run the exec **izuconfig1.cfg.userid.exec**, where **userid** is the user ID that you are using to run the configuration script. This step authorizes you (the “z/OSMF installer”) to log in to the Welcome page at the end of the configuration process and perform other post-configuration tasks, as needed.

Have your security administrator review the contents of the exec before running it.

Then, with the IZU_CONFIG_DIR directory as your active directory, run the exec, as follows:

```
./izuconfig1.cfg.userid.exec
```

Tip: If you want a log file, you can use a z/OS UNIX command, such as tee, to direct the output from this exec to a log file. For example, you could direct this output to the z/OSMF log file directory for your installation (IZU_LOGFILE_DIR). By default, this is /var/zosmf/configuration/logs/.

On completion, this exec creates the security definitions needed for your user ID.

For reference, see “Step 3: Run the security commands for your user ID” on page 37.

5. **Have your security administrator verify the security for the new configuration.** If your installation uses RACF as its security management product, perform this step. Otherwise, skip this step and, instead, take the appropriate steps to verify your security setup.

Run the **izusetup.sh** script, as follows:

```
izusetup.sh -file izuconfig1.cfg -verify racf
```

For reference, see “Step 4: Verify the RACF security setup” on page 38.

6. **Complete the configuration.** Run the **izusetup.sh** script, as follows:

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


This script might take some time to complete. As it runs, the script writes messages to the script log file. For reference, see “Step 5: Complete the setup” on page 39.

7. **Start the z/OSMF server.** For information, see “Step 6: Start the z/OSMF server” on page 41.
8. **Verify the results:** 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. For information, see “Step 7: Access the z/OSMF Welcome page” on page 44.

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 205 for information.

Considerations for reverting to a previous release of z/OSMF

Generally, after your installation migrates to a new release of z/OSMF, it is not advisable to revert (fall back) to a previous release of the product. Before attempting a fallback, see this section for considerations.

Observe the following considerations:

- Each new release of z/OSMF adds functions and enhancements that might not be available on an older release, or might not operate in the expected manner.
- The configuration process is unique in each release of the product. It is not possible to run the latest configuration scripts on a downlevel release of z/OSMF.
- Attempting to fall back to an older release can result in configuration script errors or a configuration that is difficult to manage.

Though not recommended, reverting to an older release of z/OSMF can be made easier through preparation. Ensure that you create backup copies of the older release file systems before migrating to the new release. Specifically you must save copies of the following file systems:

- z/OSMF data file system. This is the directory mount point that was specified on the IZU_DATA_DIR variable during the configuration process. See Table 4 on page 16.
- IBM WebSphere Application Server OEM Edition for z/OS configuration file system. Usually, this file system is mounted at /zWebSphereOEM/V7R0/config1, but your installation might have specified another location for it. Check the WebSphere response file for variable zConfigHfsName.
- IBM WebSphere Application Server OEM Edition for z/OS product file system. Usually, this file system is mounted at /usr/lpp/zWebSphereOEM/V7R0, but your installation might have specified another location for it. Check the WebSphere response file for variable zSmpePath.

In a fallback scenario, you could rename the backup z/OSMF configuration file and, if applicable, override file to the original names to use these files as before (see “Results” on page 55).

As of z/OSMF V2R1, z/OSMF no longer includes IBM WebSphere Application Server OEM Edition for z/OS (FMID HBBN700). Thus, the WebSphere file systems are not available in V2R1. In the event that your installation wants to regress to an older level of z/OSMF, you need to have saved backups of the WebSphere file systems. If so, you can remount the saved file systems at their original mount points and begin using the older configuration. Understand that reverting to an older release in this manner means losing any functions or configuration changes specific to the new release.

If you have not retained the WebSphere file systems, you cannot fall back to an earlier release. Instead, you must SMP/E install the prior image and repeat the configuration steps for IBM WebSphere Application Server OEM Edition for z/OS and z/OSMF. For information, see the documentation for the earlier release.

Preservation of links through migration and fallback

Installing a new release of z/OSMF will preserve any installation-specific links that you have defined. If you fall back from your current level of z/OSMF to a previous level, such as V1R13, links always open in a z/OSMF window, even if you specified another launch behavior for the link.

Actions to perform after activating z/OSMF V2R1

This topic describes z/OSMF migration actions that you can perform after you have started the z/OSMF server on your system. These actions require the z/OSMF V2R1 level of code to be installed and active.

Notify users of the correct URL to use for z/OSMF V2R1

When you migrate to z/OSMF V2R1, the product URL is changed. Be sure to provide users with the new URL to use for accessing z/OSMF through a web browser. Users can add the URL to the browser bookmarks list. Similarly, when the prior z/OSMF release is no longer in use at your installation, ask users to remove the URL bookmark for the prior release.

To find the URL for z/OSMF on your system, see message IZUG349I, which was logged when you ran the **izusetup.sh** script with option **-finish** during the configuration process. This log file is in the format: `<IZU_LOGFILE_DIR>/izusetup_finish.mm.dd.yy.hh.mm.ss.tt.log`

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

The URL for the z/OSMF Welcome page has the following format:

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

where:

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

Clean-up actions to perform when satisfied with the new release

After you have verified that the new release of z/OSMF is operating as required, you can perform a number of post-migration clean-up actions. Perform these actions only when you are certain that you will not need to fallback to a previous release. These actions cannot be easily reversed.

The following post-migration clean-up actions are recommended:

- “Review the new z/OSMF service process”
- “Review the SAF profile prefix” on page 59
- “Check the security for ports 32207 and 32208” on page 59
- “Remove ZOSMFAD owned objects and authorizations from previous releases” on page 59
- “Remove WebSphere constructs from previous releases” on page 60
- “Remove the APF authorization for SYS1.MIGLIB(AMATERSE)” on page 60
- “Remove the most-generic profile for z/OSMF authorizations” on page 61
- “Remove the SURROGAT class profiles for z/OSMF V1R12” on page 60.

Review the new z/OSMF service process

In previous releases of z/OSMF, applying service sometimes required that you run the **izusetup.sh** script with the **-service** option. This action was needed to update the Enterprise Archive (EAR) files in z/OSMF.

As of z/OSMF V2R1, you are no longer required to perform this step. Instead, you need only restart the z/OSMF server. With this change, the **-service** option is deprecated and will likely be removed from z/OSMF in a future release. For instructions on applying z/OSMF service items, see the associated APAR cover letter.

Review the SAF profile prefix

Does your security product use the SAF profile prefix BBNBASE for z/OSMF resources? If so, be aware of the following changes, which occurred with z/OSMF V2R1.

- In previous releases, the configuration variable IZU_WAS_PROFILE_PREFIX was used to identify the WebSphere SAF profile prefix, which was BBNBASE by default. With the removal of IBM WebSphere Application Server OEM Edition for z/OS in z/OSMF V2R1, this variable is no longer specified.
- In z/OSMF V2R1, the configuration variable IZU_SAF_PROFILE_PREFIX is added. Use this value to specify the SAF profile prefix for a z/OSMF. By default, the prefix is IZUDFLT.

If your installation is migrating from an earlier release of z/OSMF, it is recommended that you review the use of the BBNBASE prefix and determine whether your security product definitions for z/OSMF should be revised to use the new prefix IZUDFLT.

Tip: To identify all of the affected profiles in a RACF database, you can use this RACF command: `SEARCH ALL CLASS(ZMFAPLA) FILTER(BBNBASE.**)`

Check the security for ports 32207 and 32208

With the removal of IBM WebSphere Application Server OEM Edition for z/OS in z/OSMF V2R1, the specification of HTTP port values is changed. You can use the z/OSMF supplied port settings, or specify new values during the z/OSMF configuration process.

The port values are specified through the following configuration variables:

- IZU_HTTP_SSL_PORT, which specifies the port number for SSL encrypted traffic from your z/OSMF configuration. In this release, the default port number is changed from 32208 (the WebSphere default), to 443, which follows the Internet Engineering Task Force (IETF) standard.
- IZU_HTTP_PORT, which is new in this release. This variable specifies the port number for non-encrypted traffic, which is 80, by default. Note that if your installation is migrating from an earlier release of z/OSMF, however, you might have specified port number 32207 for this value, which is the WebSphere default.

If your installation is migrating from an earlier release of z/OSMF you might have used port numbers 32207 and 32208 for z/OSMF web traffic. These earlier values are not persisted when you migrate to z/OSMF V2R1. Determine whether ports 32207 and 32208 should remain active on your system, and update the settings or close the ports, as required by your installation security policies.

Remove ZOSMFAD owned objects and authorizations from previous releases

In previous releases of z/OSMF, the configuration process created a special user ID known as the z/OSMF administrator user ID. By default, the user ID was ZOSMFAD. You used this user ID for running configuration scripts and performing administration tasks, such as adding users and working with z/OSMF log files.

In z/OSMF V2R1, the configuration process no longer creates, or requires the use of, the administrator user ID. Though z/OSMF retains the concept of an administrator role, you can use any existing user ID for this purpose, as long as you define the user ID to the z/OSMF administrator security group (IZUADMIN).

If you do not use the z/OSMF administrator user ID for any other purposes, you can remove it and its associated authorizations as part of the migration to z/OSMF V2R1. For a RACF installation, your security administrator can use a utility to identify the user ID objects and authorizations in the RACF database, including the following examples:

- z/OSMF administrator user ID. By default, this is ZOSMFAD.
- Directories and files that were created for the ZOSMFAD user ID, such as `/home/zosmfad`

- Administrator user ID authorizations to z/OSMF resources, as follows:
 - WebSphere Application Server administrators group (WSCFG1)
 - CIM server administrators group (CFZADMGP)
 - Capacity Provisioning Query Group (CPOQUERY)
 - Capacity Provisioning Control Group (CPOCTRL)
 - Workload Management group (WLMGRP)

Remove WebSphere constructs from previous releases

In previous releases of z/OSMF, your installation configured an instance of IBM WebSphere Application Server OEM Edition for z/OS for each instance of z/OSMF. This process produced a number of WebSphere constructs on your system, such as configuration files and log files, and the WebSphere servant region user ID. In z/OSMF V2R1, these constructs are no longer needed; you can remove them.

To find the residual constructs, check the directories and files under mount point /zWebSphereOEM/V7R0/config1. You can remove these constructs as part of your migration to z/OSMF V2R1.

Also, check for the WebSphere servant region user ID and any associated security authorizations in your security product. In previous releases, this user ID was defined on variable IZU_SERVANT_USERID in your configuration file or override file. By default, the user ID is WSSRU1.

Remove the APF authorization for SYS1.MIGLIB(AMATERSE)

Beginning in z/OSMF V2R1, the Incident Log task no longer requires that your SYS1.MIGLIB data set be APF-authorized. If no other programs or functions on your system require SYS1.MIGLIB to be APF-authorized, you can remove this authorization when you are satisfied with z/OSMF V2R1, and have no plans to fall back to an earlier release. Otherwise, leave this authorization in place.

APF authorizations are defined in the PROGxx member of SYS1.PARMLIB, if your site follows IBM recommendations. If you added SYS1.MIGLIB to the APF list for z/OSMF or the Incident Log task, it is recommended that you remove the explicit authorization. To do so, locate the appropriate PROGxx member and edit it to remove the APF ADD statement associated with SYS1.MIGLIB.

For more information about the PROGxx parmlib member, see *z/OS MVS Initialization and Tuning Reference*.

Remove the SURROGAT class profiles for z/OSMF V1R12

When your installation configured z/OSMF V1R12, the z/OSMF configuration process included RACF commands for creating the SURROGAT class profile BB0.SYNC.<user ID> for the administration user ID and for any other user IDs you might have authorized. You can remove these profiles as part of the migration to z/OSMF V2R1.

Migration action for the September 2014 enhancements

When you install the PTFs for APAR PI20091 and the corequisite APARs, a migration action is required, as described in this topic.

Remove the most-generic profile for z/OSMF authorizations

In previous releases, the generated program **izuconfig1.cfg.rexx** included RACF commands for defining the following generic profile in the ZMFAPLA class, and for creating permissions to it:

```
<SAF-prefix>.ZOSMF.**
```

where *<SAF-prefix>* is the SAF profile prefix that was defined for your configuration (by default, IZUDFLT). If you used **izuconfig1.cfg.rexx** in a previous release, this generic profile was created for your configuration.

With the installation of the PTFs for APAR PI20091 and the corequisite APARs, the generated program no longer creates authorizations based on this most-generic profile. Instead, the program is revised to create authorizations based on the following discrete profile:

```
<SAF-prefix>.ZOSMF
```

Specifically, the generated program **izuconfig1.cfg.rexx** creates the following profiles and permissions for your configuration:

```
RDEFINE ZMFAPLA IZUDFLT.ZOSMF UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SETTINGS.SYSTEMS UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS UACC(NONE)

PERMIT IZUDFLT.ZOSMF          CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.SYSTEMS CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF          CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.SYSTEMS CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF          CLASS(ZMFAPLA) ID(IZUSECAD) ACCESS(READ)
```

If your security management product currently uses the most-generic profile for z/OSMF authorizations, it is recommended that you replace it with authorizations based on the discrete profile.

In a RACF installation, you can use the following commands to remove the generic profile:

```
RDELETE ZMFAPLA IZUDFLT.ZOSMF.**
SETROPTS RACLIST(ZMFAPLA) REFRESH
```

For a list of the authorizations required in z/OSMF, see Appendix A, “Security configuration requirements for z/OSMF,” on page 267.

Chapter 5. Planning for the optional z/OSMF plug-ins

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 task
- 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 11 shows which optional plug-ins are available for configuration in z/OSMF V2R1. By default, z/OSMF does not include any of the optional plug-ins.

Table 11. Optional plug-ins and associated tasks in z/OSMF V2R1

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.

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 Chapter 6, "Customizing your system for the z/OSMF plug-ins," on page 87.

Usually, to add a plug-in, you will repeat most of the steps you follow to create the initial configuration. The procedure is described in Chapter 7, "Adding plug-ins to a z/OSMF configuration," on page 127. After a plug-in is configured, you can remove it from z/OSMF only by repeating the configuration process and not selecting the plug-in.

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 65
- "Configuration Assistant task overview" on page 66
- "Incident Log task overview" on page 67
- "ISPF task overview" on page 69
- "Notifications in z/OSMF" on page 70
- "Resource Monitoring task overview" on page 71
- "Software Management task overview" on page 73
- "System Status task overview" on page 75
- "Workflows task overview" on page 76
- "Workload Management task overview" on page 77.

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 "Planning security for the z/OSMF plug-ins" on page 79.

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 "Planning security for the z/OSMF plug-ins" on page 79.

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 14 shows the main page for the Capacity Provisioning task.

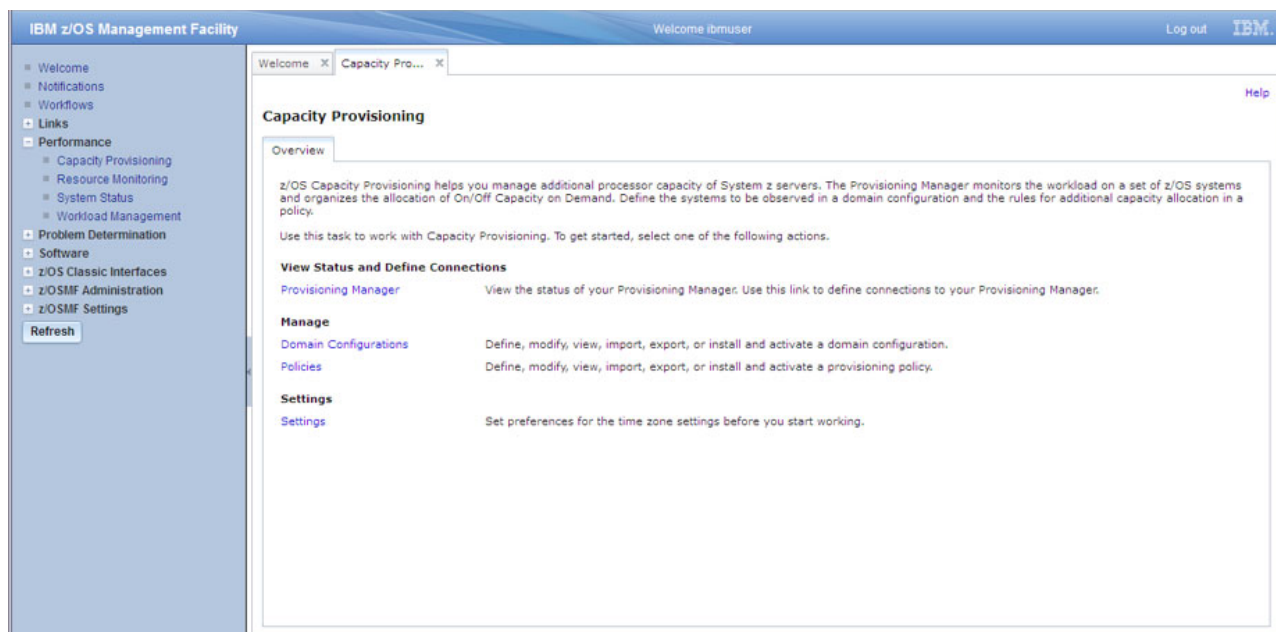


Figure 14. Capacity Provisioning task: Main page

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.

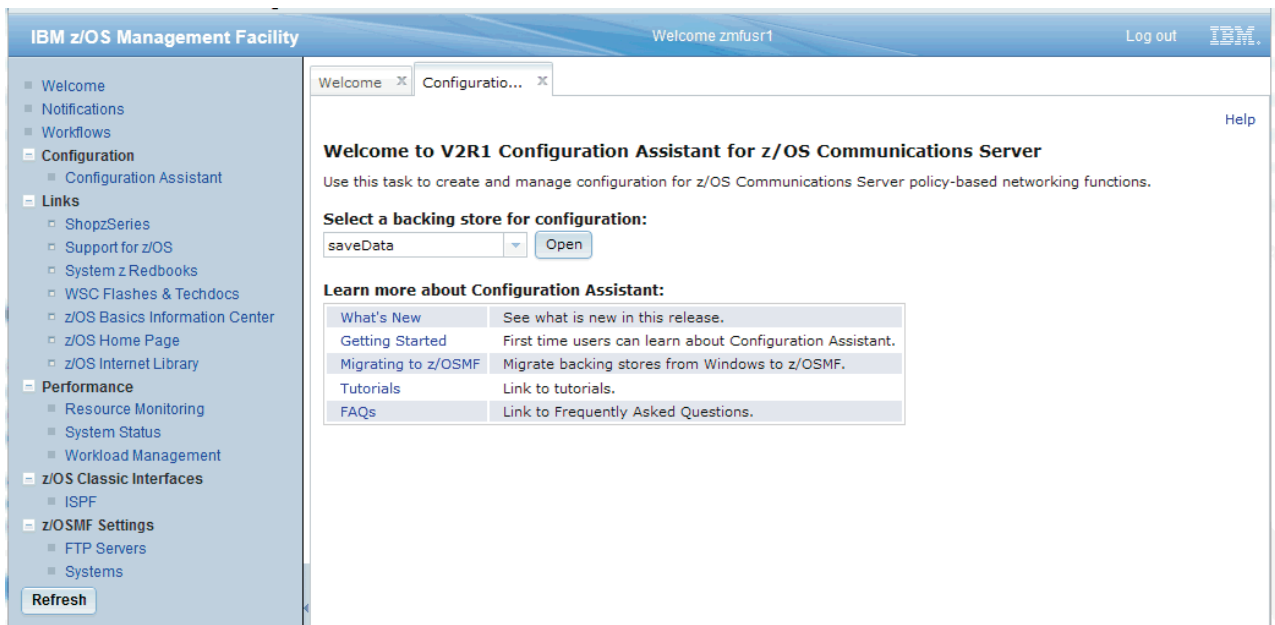


Figure 15. Configuration Assistant task main page

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 15 on page 66.

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 16 on page 68 shows a sample view from the Incident Log task.

IBM z/OS Management Facility

Welcome zmfusr3

Log out

IBM

Welcome

Incident Log

Help

Incident Log

Actions

Incident Type Filter	Description Filter	Date and Time (GMT) Dates from Oct 19, 2012 12:00:00 AM	Sysplex Filter	System Filter	Problem Number Filter	Tracking ID Filter	Notes Filter
<input type="checkbox"/> User Initiated	BUFFERUSAGE AFTER DELETION	Oct 22, 2012 5:04:52 PM	UTCPLXCB	CB86			
<input type="checkbox"/> User Initiated	BUFFERUSAGE AFTER DELETION	Oct 22, 2012 4:56:34 PM	UTCPLXCB	CB86			
<input type="checkbox"/> User Initiated	BUFFERUSAGE BEFORE DELETION	Oct 22, 2012 3:52:12 PM	UTCPLXCB	CB86			
<input type="checkbox"/> User Initiated	BUFFERUSAGE TEST	Oct 22, 2012 2:52:00 PM	UTCPLXCB	CB86			
<input checked="" type="checkbox"/> ABEND S00F4	COMPID=DF115,CSECT=IGVVDARD1+0D26,DATE=09/18/12,MAINTID=NONE ,ABND=0F4,RC=00000024,RSN=010E5AB8	Oct 22, 2012 5:05:46 AM	UTCPLXCB	CB88	12345,999,001		
<input type="checkbox"/> ABEND S0EC6	COMPON=BPX,COMPID=SCPX1,ISSUER=BPXMPCE,+157A,ABEND=S0EC6,REASON=0B010407	Oct 22, 2012 5:04:47 PM	UTCPLXCB	CB86			
<input type="checkbox"/> User Initiated	ALEX	Oct 22, 2012 5:04:47 PM	UTCPLXCB	CB86			
<input type="checkbox"/> ABEND S00C4	COMPON=HZR,COMPID=SCRTD,ISSUER=HZRMIREC,	Oct 22, 2012 5:04:47 PM	UTCPLXCB	CB86			
<input type="checkbox"/> User Initiated	ABEND=40D,RC=10,COMPON=RTM2,COMPID=SCRTD,UNRECOVERABLE ABEND FAILURE	Oct 22, 2012 5:04:47 PM	UTCPLXCB	CB86			
<input type="checkbox"/> ABEND	COMPON=CTT TC=WLJFSV29 ISSUER=CTTDE - TEST - CAT ADDRESS=226S2AD0, JOB#=04000077	Oct 22, 2012 5:04:47 PM	UTCPLXCB	CB88			
<input type="checkbox"/> ABEND S01FB	COMPON=JSS-REC,COMPID=SC1B8,ISSUER=EESB670,JOB SCHEDULING SUBROUTINE RECOVERY EXIT ROUTINE	Oct 19, 2012 8:06:54 PM	UTCPLXCB	CB89			
<input type="checkbox"/> ABEND S00C7	JES3 2.1.0 FLNO=020 ISDRVR FCT=2458DBC8 S0C7-40404040 IN IATISJL PSW=471C1000A49B439A 293/1604	Oct 19, 2012 8:04:26 PM	UTCPLXCB	CB86			
<input type="checkbox"/> ABEND S00C7	JES3 2.1.0 FLNO=019 ISDRVR FCT=2458D358 S0C7-40404040 IN IATISJL PSW=471C1000A49B439A 293/1604	Oct 19, 2012 8:04:24 PM	UTCPLXCB	CB86			
<input type="checkbox"/> ABEND S00C7	JES3 2.1.0 FLNO=018 ISDRVR FCT=2458C6B0 S0C7-40404040 IN IATISJL PSW=471C1000A49B439A 293/1604	Oct 19, 2012 8:04:22 PM	UTCPLXCB	CB86			
<input type="checkbox"/> ABEND S01FB	COMPON=JSS-REC,COMPID=SC1B8,ISSUER=EESB670,JOB	Oct 19, 2012 8:04:19 PM	UTCPLXCB	CB86			

Set Tracking ID...

Set Problem Number...

Add Notes...

Delete Incident...

Send Diagnostic Data...

View Diagnostic Details

FTP Job Status

Allow Next Dump...

Total: 42, Filtered: 42, Selected: 1

Refresh

Last refresh: Oct 22, 2012 5:22:48 PM local time (Oct 22, 2012 9:22:48 PM GMT)

Figure 16. Incident Log 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.

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 17.

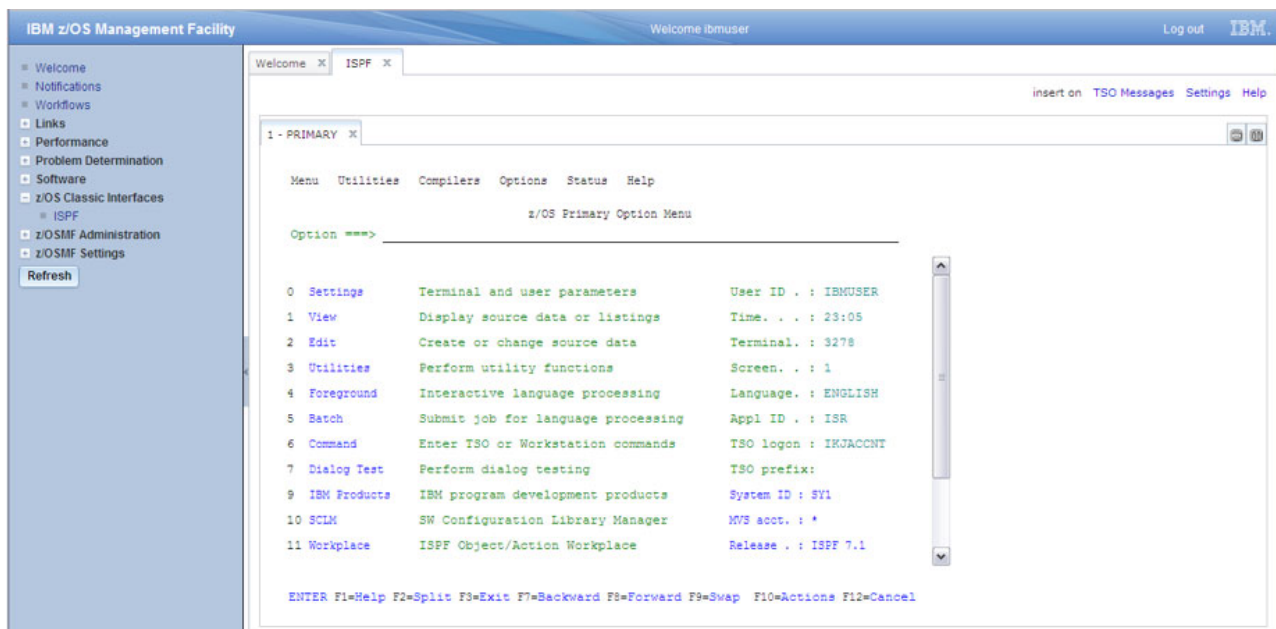


Figure 17. ISPF task main page

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 18. The Notifications task is displayed for all authenticated users. Unauthenticated guest users cannot access this task.

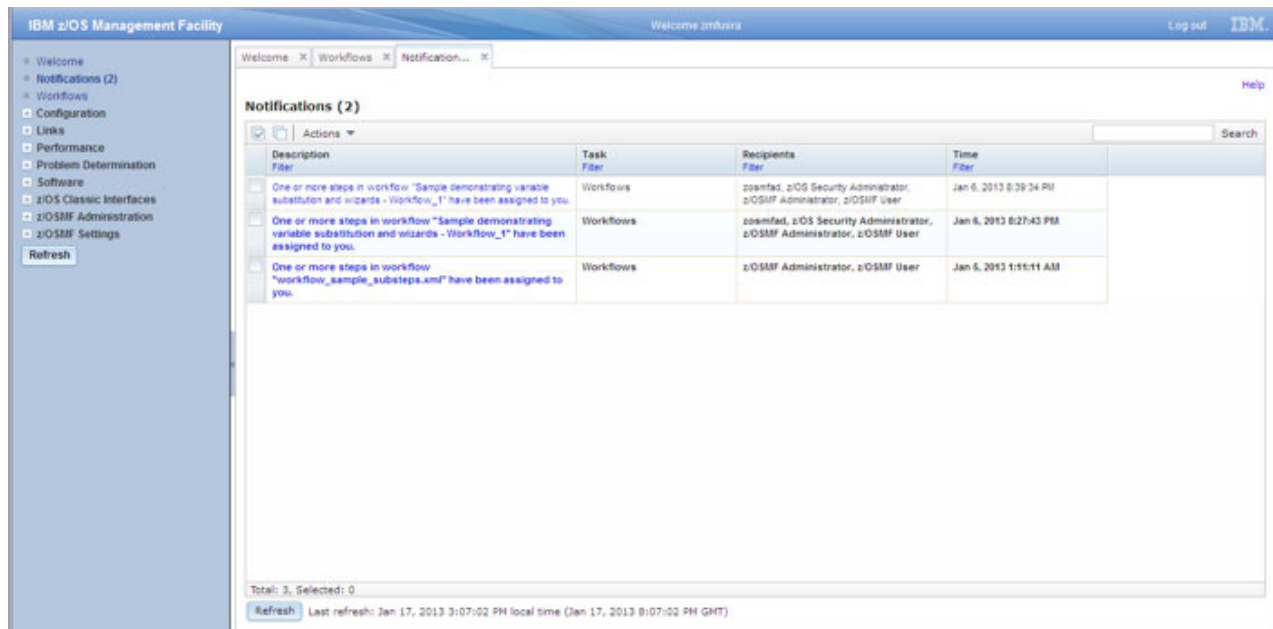


Figure 18. Notifications main page

z/OSMF includes settings that control the behavior of notifications, as follows:

Notification expiration

Notifications expire after a given period of time (by default, 30 days). When this limit is reached, z/OSMF deletes the expired notifications.

Notification maximum

You can retain a maximum number of notifications (by default, 500). When this limit is reached, new notifications cause the oldest to be deleted.

These settings are controlled by your installation, as described in “Reviewing the z/OSMF advanced settings” on page 22.

More information about the Notifications task is provided 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).

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 19 shows a sample view from the Resource Monitoring task.

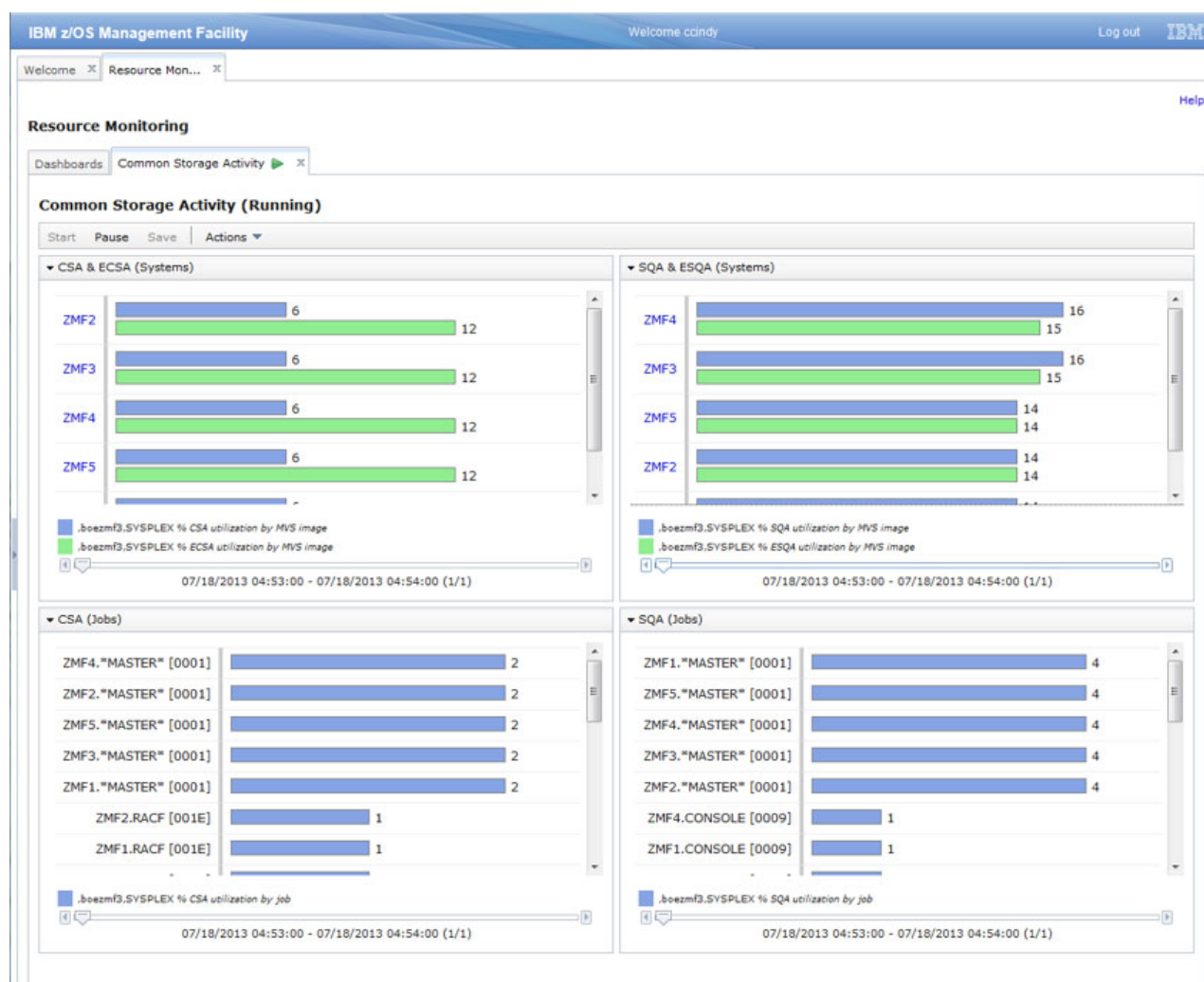


Figure 19. Resource Monitoring sample view

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 20 on page 74 depicts the main page in the Software Management task.

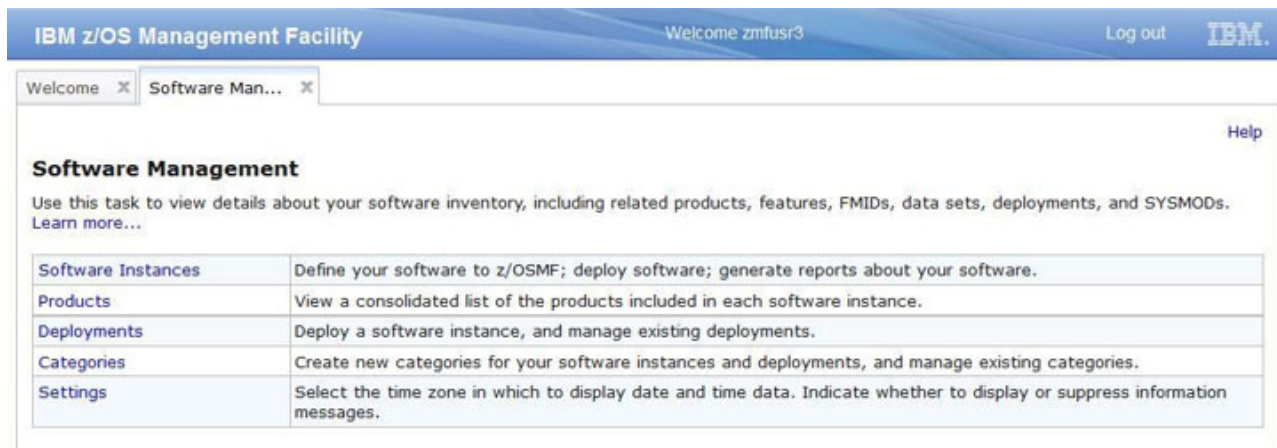


Figure 20. Software Management page

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.

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.

To display the System Status task, expand the Performance category in the navigation area and select **System Status**. Figure 21 on page 76 shows a sample view from the System Status.

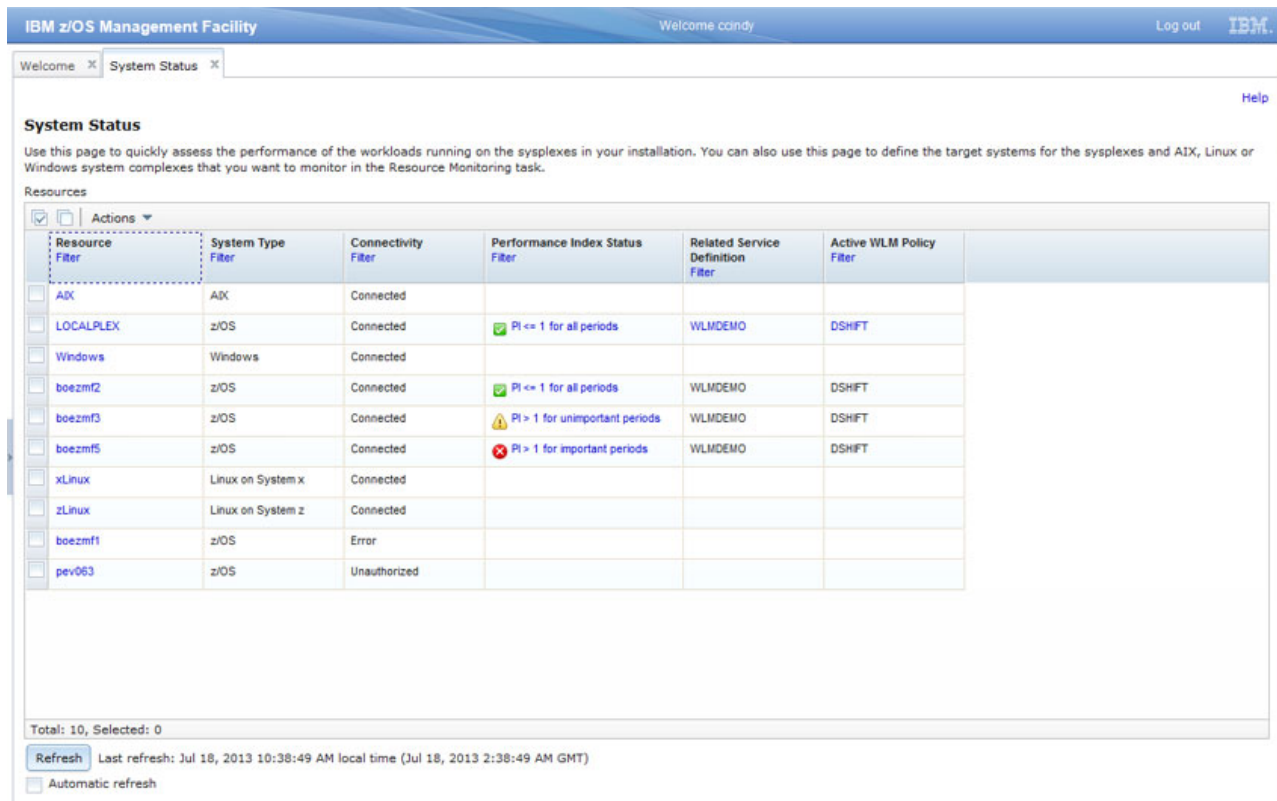


Figure 21. System Status sample view

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.

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 22 on page 77.

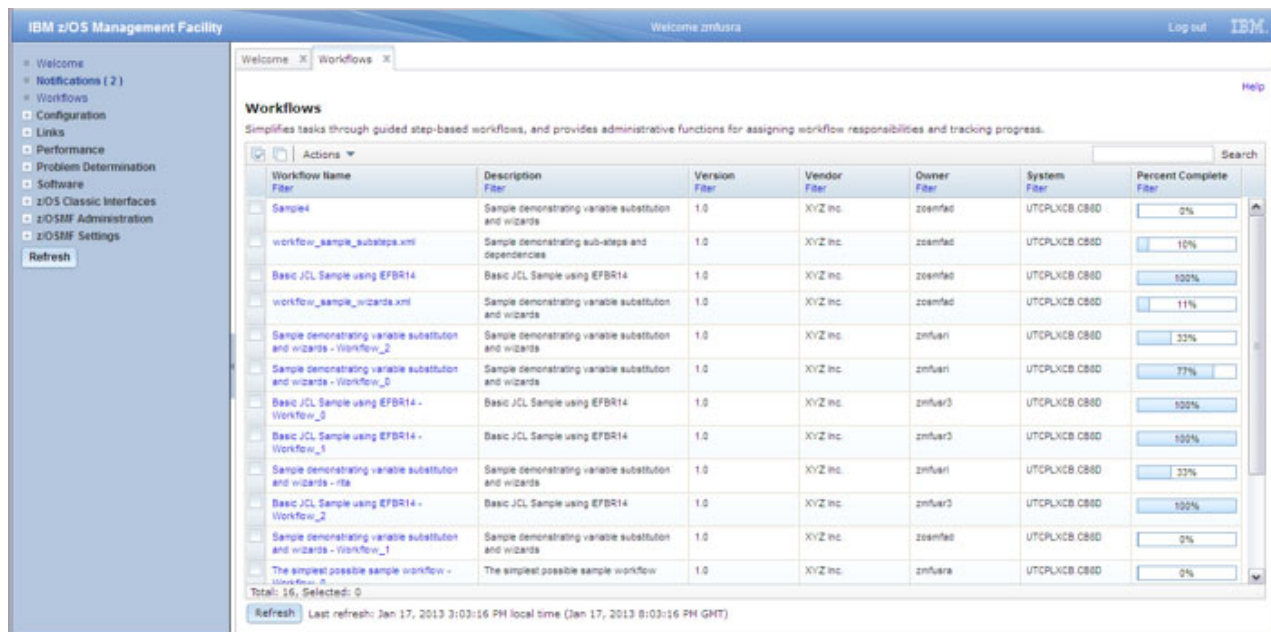


Figure 22. Workflows main page

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: <IZU_CODE_ROOT>/workflow/, where the default for <IZU_CODE_ROOT> is /usr/lpp/zosmf/V2R1. 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. The samples include a workflow that identifies the z/OS system customization steps for each of the plug-ins. See "Configuration workflow" on page 87.

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 Manager (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.

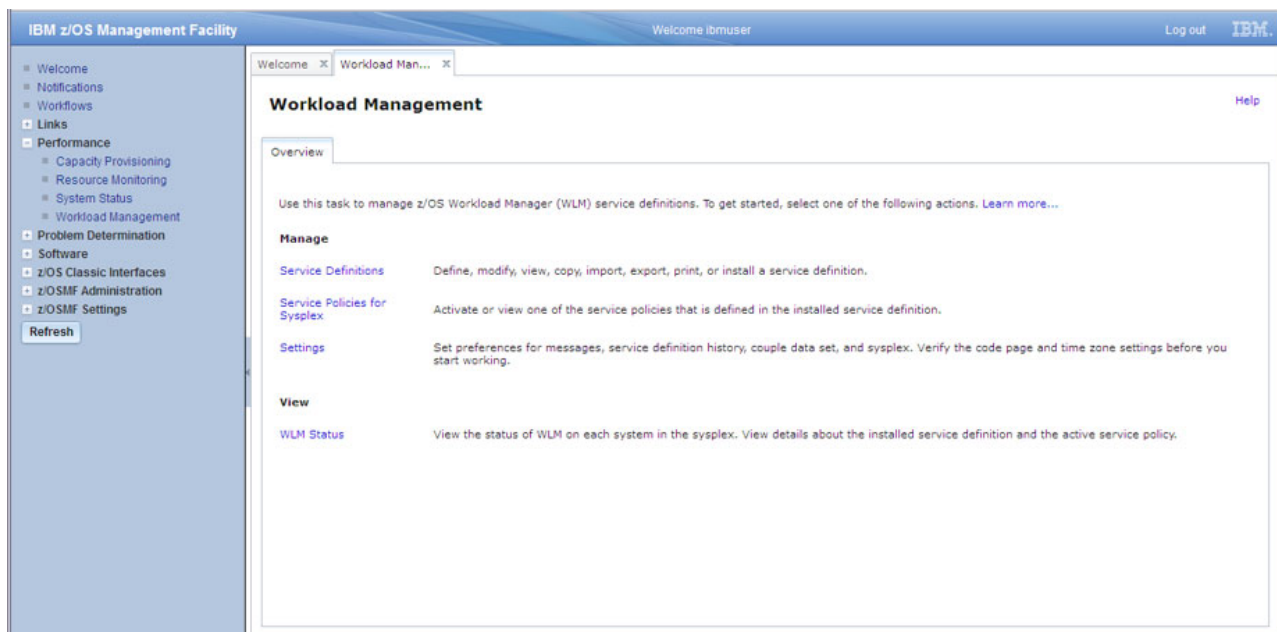


Figure 23. Workload Management task main page

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 23 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 data file system in which the data for the Workload Management task is stored.
- **Work with multiple service definitions.** In the Workload Management task, you can work with multiple service definitions simultaneously. To do so, open the service definitions with which you want to work in its own *View*, *Modify*, *Copy*, or *Print Preview* tab. You can also define multiple service definitions at the same time by opening several *New* tabs.
- **Install service definitions.** The Workload Management task provides features that you can use to install a service definition into the WLM couple data set for the z/OSMF host sysplex.
- **Extract the installed service definition.** The Workload Management task automatically extracts the service definition that is installed in the WLM couple data set for the z/OSMF host sysplex and stores it in the service definition repository so that you can view it, modify it, or activate one of its service policies.
- **Import and export service definitions.** The Workload Management task provides features that you can use to import a service definition from or export a service definition to your local workstation or a

sequential data set on the z/OSMF host system. The exported service definition is formatted so that it can be opened with the z/OS WLM Administrative Application (also called the WLM ISPF application).

- **Provide table view and print preview of the service definition.** The Workload Management task provides two views of a service definition.
 - **Table View.** The table view displays the parts of the service definition as tables. You can display the table view by opening the service definition in the *New*, *View*, *Modify*, or *Copy* tab. If you open the service definition in the *New*, *Modify*, or *Copy* tab, you can modify the service definition. In the *View* tab, you cannot modify the service definition.
 - **Print Preview.** The print preview presents the service definition in HTML format and allows you to select which parts of the service definition you want to preview or print. You can display the print preview by opening the service definition in the *Print Preview* tab.
- **Activate service policies.** In the Workload Management task, you can specify which policy to activate when you install a service definition or you can activate a service policy that is defined in the service definition currently installed in the WLM couple data set for the sysplex.
- **Preview service policies with overrides applied.** The Workload Management task allows you to preview an HTML formatted version of the service policy with overrides applied. The HTML formatted service policy contains the information that would be included in the policy if it were activated. To preview a service policy, open the policy in the *Print Preview* tab.
- **View the WLM status.** The Workload Management task provides an HTML formatted view (*WLM Status* tab) of the same data that is retrieved when you enter the `D WLM,SYSTEMS` command on the z/OS console. Specifically, the *WLM Status* tab displays the status of WLM on each system in the sysplex, and lists details about the installed service definition and the active service policy.
- **Define settings.** The Workload Management task provides a shared location (*Settings* tab) where you can specify how long to keep the service definition history and define the code page, time zone, and backup sequential data set for the sysplex. You can also enable consistency checking between z/OSMF and the WLM couple data set, and indicate whether you want the Workload Management task to display or suppress information messages, 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.

Planning security for the z/OSMF plug-ins

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 security controls are established on your system, a user can begin using z/OSMF to perform system management tasks.

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

Setting up security for the z/OSMF tasks and links

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

Figure 24 shows a typical security setup for z/OSMF. To conserve space, this figure includes only a subset of the available tasks.

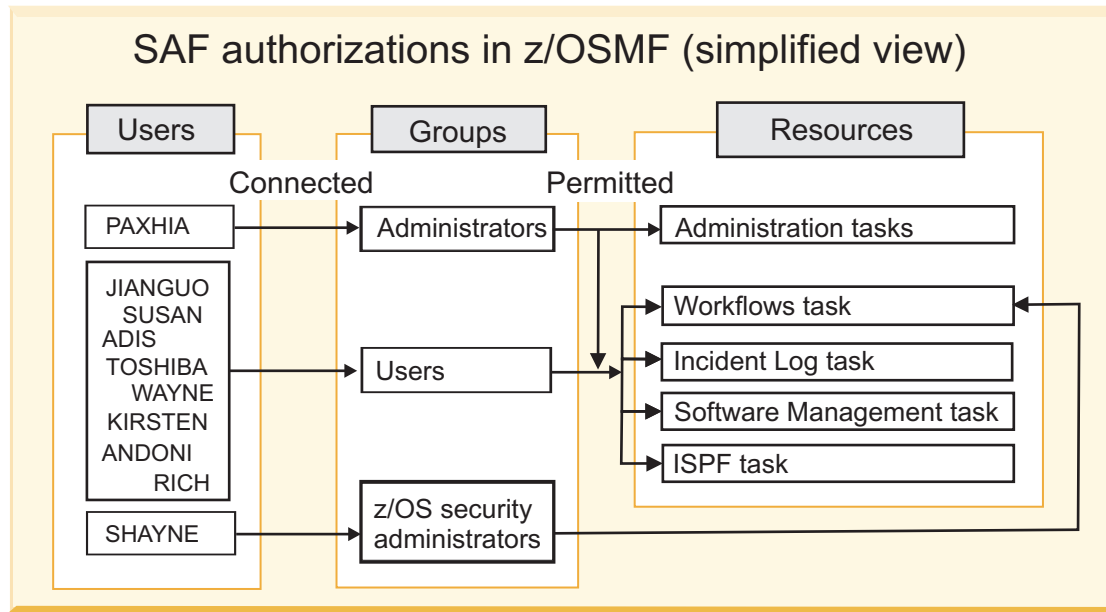


Figure 24. SAF authorizations in z/OSMF

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 a set of REXX execs with RACF commands that your security administrator can use to secure z/OSMF resources and users. These execs are created during the z/OSMF configuration process, and are customized for your installation, based on the plug-ins you have selected to configure.

The z/OSMF configuration process creates the security definitions, as follows:

- When adding plug-ins, your security administrator runs the REXX exec **izuconfig1.cfg.add.rexx**, which contains sample RACF commands for securing the plug-ins. The REXX exec includes 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, respectively. z/OSMF also creates the group IZUSECAD, to allow your z/OS security administrator to perform the security-related steps in the Workflows task.

For the security structures that are created during the z/OSMF configuration process, see Appendix A, “Security configuration requirements for z/OSMF,” on page 267.

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

- After the plug-ins are added, your security administrator can use the IBM supplied script, **izuauthuser.sh**, and the REXX exec it generates, to authorize users to z/OSMF and to the z/OS components used in z/OSMF operations. Your security administrator runs the REXX exec for each user to be authorized to z/OSMF.

When used as provided, the generated REXX exec connects the supplied user ID to the z/OSMF user group (IZUUSER). The exec also contains commented commands for connecting the user to the z/OSMF administrator group 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 46 on page 283.

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

- Depending on the plug-ins to be configured, your installation might need to create additional authorizations to various system resources. These requirements are described in this document. A change to your security setup will likely require an applicable refresh of your security product and a re-start of the z/OSMF server for the changes to take effect.

Figure 25 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 46 on page 283.

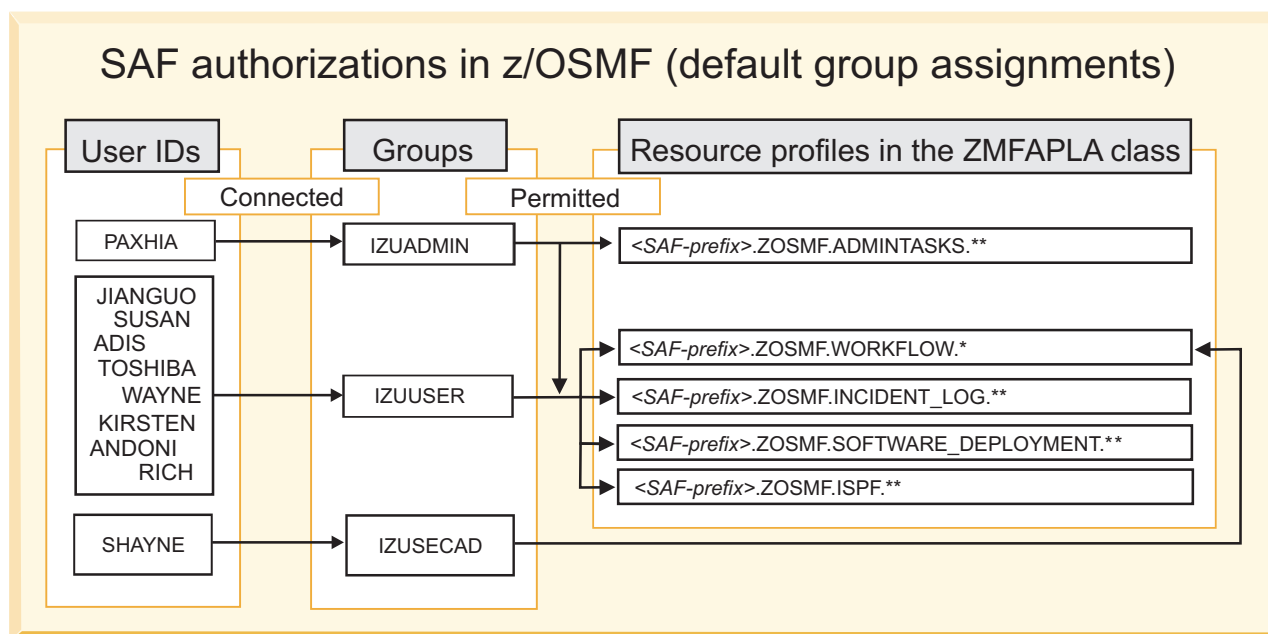


Figure 25. SAF authorizations in z/OSMF: The default setup

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

As shown in Figure 25, z/OSMF 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 additional 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 115.

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* task and access the default links. An authenticated guest can access everything a non-authenticated guest can, and also view the online help.

Sample RACF commands for z/OSMF plug-ins

Your security administrator can use the REXX exec **izuconfig1.cfg.add.rexx** to create authorizations for the z/OSMF plug-ins.

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

- “Commands for permitting z/OSMF tasks to the CIM server” on page 307
- “Commands for configuring the Capacity Provisioning plug-in” on page 308
- “Commands for configuring the Configuration Assistant plug-in” on page 310
- “Commands for configuring the Incident Log plug-in” on page 312
- “Commands for configuring the ISPF plug-in” on page 315
- “Commands for configuring the Resource Monitoring plug-in” on page 317
- “Commands for configuring the Software Deployment plug-in” on page 319
- “Commands for configuring the Workload Management plug-in” on page 321.

Planning worksheets for the z/OSMF plug-ins

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

To save time during the configuration process, have this information at hand when you perform the steps in Chapter 7, “Adding plug-ins to a z/OSMF configuration,” on page 127. The amount of information you need to gather depends on which plug-ins your installation plans to configure in addition to the core functions of z/OSMF.

The following planning worksheets are included:

- “Planning your plug-in selections”
- “Input for the Capacity Provisioning task” on page 83
- “Input for the Incident Log task” on page 84
- “Input for the Workload Management task” on page 86.

Planning your plug-in selections

Determine which plug-ins are needed for your installation and record your selections in the worksheet that follows.

Table 12 shows which value to specify for adding a plug-in, depending on the method you use to supply input to the script. You can add plug-ins interactively by specifying the plug-in ID in response to the script prompt. Or, you can add plug-ins through the override file by including the plug-in variable name and setting it to A. By default, none of the plug-ins are selected.

Table 12. Worksheet for planning your plug-in selections

✓	Plug-in	To add through the interactive script, specify the plug-in ID	To add through the override file, specify the variable name and set it to A	Default	Your value
	Incident Log	1	IZU_IL_CONFIGURE=A	N	
	Configuration Assistant	2	IZU_CA_CONFIGURE=A	N	
	Workload Management	3	IZU_WLM_CONFIGURE=A	N	
	Resource Monitoring	4	IZU_RMF_CONFIGURE=A	N	
	Capacity Provisioning	5	IZU_CP_CONFIGURE=A	N	
	Software Deployment	6	IZU_DM_CONFIGURE=A	N	
	ISPF	7	IZU_WISPF_CONFIGURE=A	N	

Input for the Capacity Provisioning task

If you choose to deploy the Capacity Provisioning plug-in, you must provide additional information to the **izusetup.sh** script.

For your planning purposes, Table 13 shows the information you should have at hand when running the configuration script. Here, you must supply the names of the security groups that your installation has created for authorizing users to the Provisioning Manager on your system. Table 13 includes the variable names and defaults for these values. For more information about the Capacity Provisioning security groups, see *z/OS MVS Capacity Provisioning User's Guide*.

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

Table 13. Worksheet for the Capacity Provisioning task variables

Input	Description	Variable name	Default value	Your value
Provisioning Manager query security group.	Group name to use for authorizing user access to the Capacity Provisioning task. The configuration process permits this group to the Capacity Provisioning task. Your installation must create this group outside of the z/OSMF configuration process.	IZU_CP_QUERY_GROUP_NAME	CPOQUERY	
Provisioning Manager control security group.	Group name to use for authorizing user access to the Capacity Provisioning task. The configuration process permits this group to the Capacity Provisioning task. Your installation must create this group outside of the z/OSMF configuration process.	IZU_CP_CONTROL_GROUP_NAME	CPOCTRL	
Group name for the CIM Administrator role.	Security group to be used for creating the CIM administrator user ID.	IZU_CIM_ADMIN_GROUP_NAME	CFZADMGP	
Group name for the CIM User role.	Security group to be used for defining CIM users.	IZU_CIM_USER_GROUP_NAME	CFZUSRGP	

Input for the Incident Log task

If you choose to deploy the Incident Log plug-in, you must provide additional information to the `izusetup.sh` script.

For your planning purposes, Table 14 shows the information you should have at hand when running the configuration script. Table 14 includes the variable names and defaults, if any, for these values. If you choose not to deploy the Incident Log plug-in, you can skip this planning worksheet.

Table 14. Worksheet for the Incident Log task variables

Input	Description	Variable name	Default value	Your value
Do you want to enable the common event adapter (CEA) component and update related parmlib options for using the Incident Log task?	<p>Indicates whether (Y or N) the script is to enable the common event adapter (CEA) component and update related parmlib options for using the Incident Log task.</p> <ul style="list-style-type: none"> If you reply Y, you are prompted for additional values for setting up your system for the Incident Log. The system changes include initializing a CEAPRMxx parmlib member with options set for Incident Log processing. If you reply N, you are responsible for performing this setup before users can begin using the Incident Log task. The script will not prompt you for the CEA related values that follow. 	IZU_IL_CEA_CONFIGURE	Y	
HLQ of the CEA data sets.	The high level qualifier to be used for CEA data sets, as defined in the CEAPRMxx parmlib member. This HLQ is used for the associated dump data sets. This value is one to eight characters.	IZU_CEA_HLQ	CEA	
Country code.	IBM-defined country code for your site (3-character alphanumeric).	IZU_COUNTRY_CODE	NO.DEFAULT.VALUE You must provide a value for this.	
Branch.	IBM-defined branch code (or branch office) for your site (3-character alphanumeric).	IZU_BRANCH_CODE	NO.DEFAULT.VALUE You must provide a value for this.	
What STORAGE option do you want to use?	<p>Indicates the volumes or a SMS STORAGE class to be used by CEA for storing diagnosis snapshots.</p> <ul style="list-style-type: none"> Enter V to specify one or more volumes. Enter S to specify an SMS storage class. <p>In response, the script prompts for each volume (up to seven) or a single storage class name. Specify each value on a separate line as prompted.</p>	IZU_STORAGE_VALUE	NO.DEFAULT.VALUE You must provide a value for this.	

Table 14. Worksheet for the Incident Log task variables (continued)

Input	Description	Variable name	Default value	Your value
Source data set for the CEAPRM00 member.	Source data set that contains the IBM-supplied member, CEAPRM00. Usually, this is your SMPE-installed SYS1.PARMLIB data set. Ensure that the data set exists and is cataloged.	IZU_CEAPRM_SOURCE_PARMLIB	SYS1.PARMLIB	
Target data set for saving the new CEAPRM _{mm} member.	Target data set to use for creating the new CEAPRM _{mm} member for Incident Log processing. This data set cannot be edited or allocated to a user or job when the izusetup.sh script is running. If you do not want your system's active parmlib data set to be updated directly by the configuration process, you can instead allow updates to be made to an interim or temporary parmlib data set. You can later manually copy from this interim place into the active parmlib data set.	IZU_CEAPRM_TARGET_PARMLIB	SYS1.PARMLIB	
Source data set for the IEADMCZM member.	Source data set for your existing IEADMCZM member. Usually, this is your SMPE-installed SYS1.SAMPLIB data set. Ensure that the data set exists and is cataloged.	IZU_IEADMC_SOURCE_PARMLIB	SYS1.SAMPLIB	
Target data set for saving the new IEADMC _{mm} member.	Target data set to use for creating the new IEADMC _{mm} member for Incident Log processing. This data set cannot be edited or allocated to a user or job when the izusetup.sh script is running. If you do not want your system's active parmlib data set to be updated directly by the configuration process, you can instead allow updates to be made to an interim or temporary parmlib data set. You can later manually copy from this interim place into the active parmlib data set.	IZU_IEADMC_TARGET_PARMLIB	SYS1.PARMLIB	
Suffix of the CEAPRM _{xx} parmlib member.	Two-character suffix of a new CEAPRM _{xx} parmlib member to be used for enabling captures or "snapshots" of the system logs. Two characters are required. If this member already exists, the script prompts you to choose whether to overwrite the existing member.	IZU_CEA_PARM_NAME	01	

Table 14. Worksheet for the Incident Log task variables (continued)

Input	Description	Variable name	Default value	Your value
Suffix of the IEADMCxx parmlib member.	Two-character suffix of a new IEADMCxx parmlib member to be used for setting dump options. Two characters are required. If this member already exists, the script prompts you to choose whether to overwrite the existing member. If the IZU_IL_CEA_CONFIGURE variable is set to N, it is assumed that the IEADMCnn member already exists and resides in a concatenated parmlib data set; specify the member suffix on this variable. If the IEADMCnn member does not reside in the parmlib data set, you must place it there manually before running the izusetup.sh -verify script.	IZU_IEA_PARM_NAME	ZM	
Group name for the CIM Administrator role.	Security group to be used for creating the CIM administrator user ID.	IZU_CIM_ADMIN_GROUP_NAME	CFZADMGP	
Group name for the CIM User role.	Security group to be used for defining CIM users.	IZU_CIM_USER_GROUP_NAME	CFZUSRGP	

Input for the Workload Management task

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

For your planning purposes, Table 15 shows the information you should have at hand when running the configuration script. Here, you must supply the name of the security group that your installation has created for authorizing users to workload manager (WLM) resources on your system, such as the WLM couple data set. Table 15 includes the variable name and default for this value.

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

Table 15. Worksheet for the Workload Management task variable

Input	Description	Variable name	Default value	Your value
Group for accessing workload manager (WLM) resources.	Group name to use for allowing the Workload Management task to access WLM resources on your system. This group requires UPDATE access to facility MVSADMIN.WLM.POLICY, as described in “Authorizing users to the MVSADMIN.WLM.POLICY profile” on page 123. Your installation must create this group outside of the z/OSMF configuration process.	IZU_WLM_GROUP_NAME	WLMGRP	
Group name for the CIM Administrator role.	Security group to be used for creating the CIM administrator user ID.	IZU_CIM_ADMIN_GROUP_NAME	CFZADMGP	
Group name for the CIM User role.	Security group to be used for defining CIM users.	IZU_CIM_USER_GROUP_NAME	CFZUSRGP	

Chapter 6. Customizing your system for the z/OSMF plug-ins

This topic 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” on page 88
- “Reviewing your CIM server setup” on page 88
- “Updating z/OS for the Capacity Provisioning plug-in” on page 90
- “Updating z/OS for the Configuration Assistant plug-in” on page 92
- “Updating z/OS for the Incident Log plug-in” on page 93
- “Updating z/OS for the ISPF plug-in” on page 111
- “Updating z/OS for the Resource Monitoring Plug-in” on page 112
- “Updating z/OS for the Software Deployment plug-in” on page 115
- “Updating z/OS for the Workload Management plug-in” on page 123.

In terms of security set-up, enabling a task will require that you perform some customization of the security management product on your host system (for example, make updates to the RACF database). The configuration process provides a REXX exec with RACF commands to help with performing these changes. An additional set of authorizations is needed whenever you add users to z/OSMF.

The z/OSMF configuration process creates a REXX exec with commands for your security administrator to use for authorizing users to the z/OSMF tasks. The steps for adding plug-ins to your configuration and authorizing users to plug-ins are described later in this document, in the following topics:

- Chapter 7, “Adding plug-ins to a z/OSMF configuration,” on page 127
- Chapter 8, “Authorizing users to z/OSMF,” on page 131.

Configuration workflow

z/OSMF includes the Workflows task to help with activities, such as configuring components or products in your installation. z/OSMF provides a sample configuration workflow that you can use to configure the z/OS system requisites for the z/OSMF plug-ins. To view the configuration workflow, import the following workflow definition file into the Workflows task:

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

where <IZU_CODE_ROOT> is the z/OSMF product file system. By default, this is /usr/lpp/zosmf/V2R1.

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:

```
<IZU_CONFIG_DIR>/workflow/izu.config.workflow.cfg
```

where <IZU_CONFIG_DIR> is the configuration file system. By default, this is /etc/zosmf.

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

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.

This section contains the following topics:

- “Ensure that the CIM server is started”
- “Advanced settings for the CIM server configuration.”

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*.

Advanced settings for the CIM server configuration

If the CIM server times out frequently during operations, you can increase the length of time that z/OSMF waits for a response from the CIM server. See Appendix D, “Modifying the advanced settings for the z/OSMF configuration,” on page 293.

Selecting a user ID for adding plug-ins

To add plug-ins to a z/OSMF configuration, you require a user ID with *superuser* authority. Also, depending on which plug-ins you choose to configure with z/OSMF, your user ID might require additional setup, as described in this topic.

See the sections that follow:

- “Requirements for user IDs connected to the administrator group”
- “Ensure that the administrator role is authorized to the CIM server”
- “Customizing the administrator role for running CIM commands” on page 90.

Requirements for user IDs connected to the administrator group

Besides having superuser authority, your user ID must be authorized to work with the directories, data sets, and file systems in the locations specified by the variables in the configuration file. Your user ID might require update authority to the parmlib data set for any members that are modified during the z/OSMF configuration process. For example, if you plan to configure the Incident Log plug-in, and you allow z/OSMF to configure the common event adapter (CEA) component of z/OS, the user ID that runs this script must be authorized on the z/OS system to activate the CEA parmlib member.

Also, ensure that the following is done for the user ID:

- Command aliasing is disabled, as described in “Removing command aliases” on page 32.
- If you selected one or more plug-ins that require the use of the CIM server on your z/OS system, verify that the z/OSMF administrator role is properly set up for the z/OS UNIX shell environment. By default, the file profile.add, which is shipped with the CIM server, provides the environment variables that you need to define for the administrator; see “Customizing the administrator role for running CIM commands” on page 90.

To find out which plug-ins require the CIM server, see “Reviewing your CIM server setup” on page 88.

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 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 ID to the CFZADMGP group.

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 “Logging into z/OSMF” on page 45.

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.

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” on page 91.

System customization for the Capacity Provisioning task

Table 16 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 16. z/OS setup actions for the Capacity Provisioning task

	z/OS setup action	Check when task is completed
<u>1</u>	Ensure that a Capacity Provisioning Domain is implemented in your enterprise. For information about setting up and implementing Capacity Provisioning, see <i>z/OS MVS Capacity Provisioning User's Guide</i> .	
<u>2</u>	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	

Table 16. z/OS setup actions for the Capacity Provisioning task (continued)

	z/OS setup action	Check when task is completed
<u>3</u>	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 <i>z/OS MVS Capacity Provisioning User's Guide</i> .	
<u>4</u>	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')
SETOPTS 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)
SETOPTS 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)
SETOPTS 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: SETOPTS 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 26, a number of base z/OS functions are involved when the Incident Log task is used to manage diagnostic data for your system.

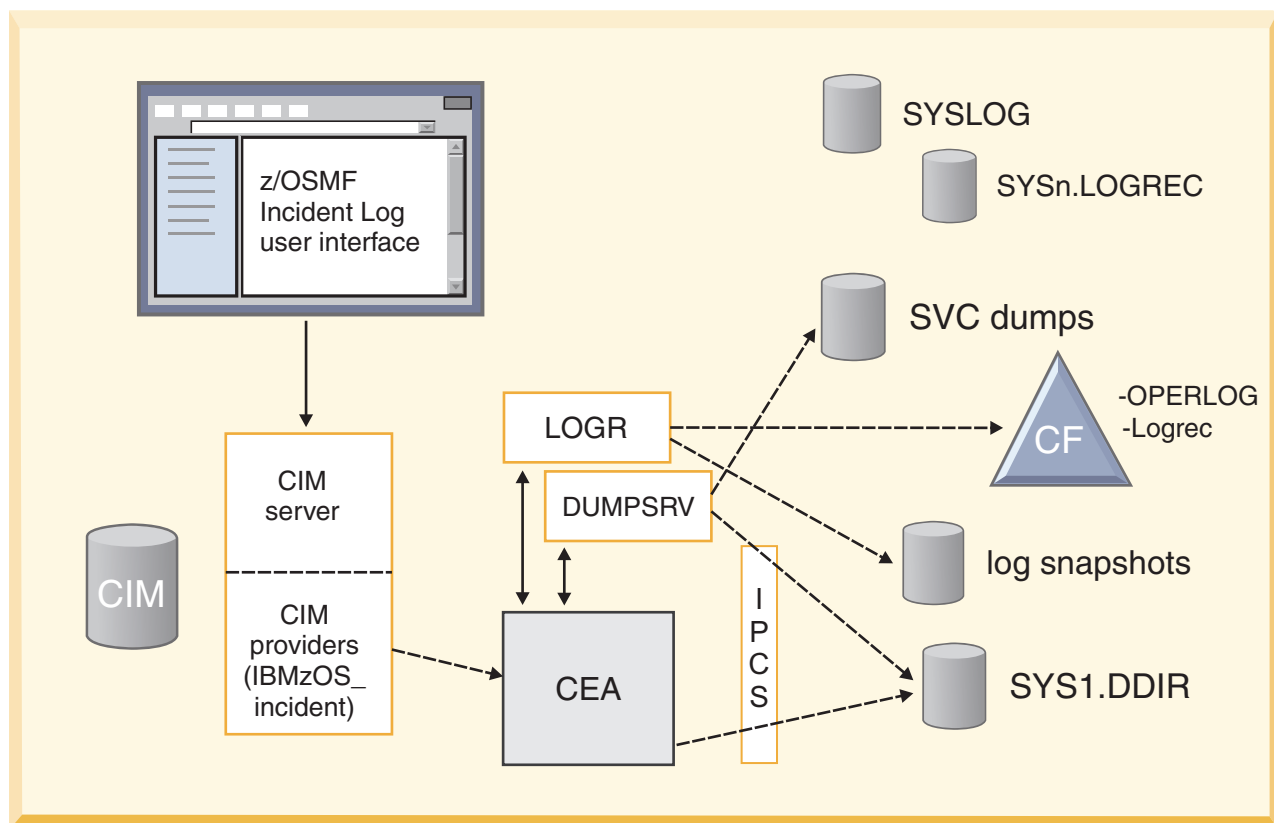


Figure 26. z/OS components used in Incident Log task processing

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 formatting the logrec data
- Common Event Adapter (CEA) for providing the data that is subsequently displayed in the Incident Log task user interface.

CEA helps to coordinate these system functions on behalf of z/OSMF incidents, in single system and sysplex environments.

Similar to other z/OS components, the CEA address space has the following attributes:

- Is started automatically during z/OS system initialization
- Supports a set of operator commands for interaction, such as MODIFY CEA
- Issues WTO messages (prefixed with CEA)
- Supports an abend code for handling incorrect actions (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 E, “Common event adapter (CEA) reason codes,” on page 297.

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 17 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 17.

Table 17. z/OS setup actions for the Incident Log task

	z/OS setup action	Where described	Check when task is completed
<u>1</u>	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 <i>z/OS Common Information Model User's Guide</i> .	
<u>2</u>	Define a couple data set for the system logger component of z/OS.	See "Defining a couple data set for system logger" on page 96.	
<u>3</u>	Enable message log snapshots on the host system, or, optionally, on a sysplex-wide basis.	See the following topics: <ul style="list-style-type: none"> • "Setup considerations for log snapshots" on page 98 • "Enabling the operations log (OPERLOG)" on page 98 • "Defining and activating the LOGREC log stream" on page 100 • "Defining diagnostic snapshot log streams" on page 102 • "Enabling SYSLOG for diagnostic snapshots" on page 102. 	
<u>4</u>	Enable error log snapshots on the host system, or, optionally, on a sysplex-wide basis.	See the following topics: <ul style="list-style-type: none"> • "Setup considerations for log snapshots" on page 98 • "Enabling the operations log (OPERLOG)" on page 98 • "Defining and activating the LOGREC log stream" on page 100 • "Defining diagnostic snapshot log streams" on page 102 • "Enabling SYSLOG for diagnostic snapshots" on page 102. 	
<u>5</u>	Set up and configure automatic dump data set allocation (auto-dump).	See "Configuring automatic dump data set allocation" on page 103.	
<u>6</u>	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 104.	
<u>7</u>	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 105.	

Table 17. z/OS setup actions for the Incident Log task (continued)

	z/OS setup action	Where described	Check when task is completed
<u>8</u>	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 107.	
<u>9</u>	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 109.	
<u>10</u>	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 110.	

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 27 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 27. Expected results from the D XCF,COUPLE,TYPE=LOGR operator 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:

```
//FMTLGCD S JOB MSGLEVEL=(1,1)
//          EXEC PGM=IXCL1DSU
//* S SUBMIT,JOB=LOGGER.ZOS17.JCL(FORMAT17)
//* SETXCF COUPLE,ACUPLE=(LOGGER.OSR13.LARGE.INVNTY,LOGR3),TYPE=LOGR
//* SETXCF COUPLE,PSWITCH,TYPE=LOGR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
  DEFINEDS SYSPLEX(PLEX1) DSN(LOGGER.OSR13.LARGE.INVNTY) 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).”
 - 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 102.
 - Defining a couple data set for sysplex-wide logging through system logger. See “Defining a couple data set for system logger” on page 96.

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 102.

- 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 100.

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” on page 99.

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 28 on page 99 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 28. 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” on page 101.

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 29 shows the expected results:

```
IFB090I  15.22.12  LOGREC DISPLAY 062
CURRENT MEDIUM = DATASET
MEDIUM NAME = SYS1.P02.LOGREC
```

Figure 29. 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 30 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 30. Expected results from the D LOGGER operator 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 31, 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 31. 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 110.

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:
`R0 *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"
```

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 through the **D GRS** command. Verify that no IPCS user is accessing the sysplex dump directory.

Establishing a larger sysplex dump directory

Over time, your sysplex dump directory might become full with the dumps you have saved. To create more space for dumps, you can delete old dumps from the directory. If you must retain the saved dumps, however, you can instead migrate your existing dumps to a larger sysplex dump directory.

To establish a larger sysplex dump directory, follow these steps:

1. Create a new sysplex dump directory data set through the **BLSCDDIR** CLIST, for example:

```
EXEC 'SYS1.SBLSCLI0(BLSCDDIR)'
'DSNAME(new.DDIR) VOLUME(volser) RECORDS(25000)'
```

If your existing dump directory was created with the default size of 15000 records, you might want to specify a larger size. Approximately 50 directory entries are used for each incident and more are used for multi-system dumps.

2. Use the IPCS COPYDDIR command to copy the old directory entries to the new directory data set, as follows:

```
COPYDDIR INDSNAME(SYS1.DDIR) DSNAME(new.DDIR)
```

3. Update BLSCUSER with the new dump directory name, but make note of the old dump directory name.
4. Recycle the DUMPSRV address space (CANCEL DUMPSRV; it restarts automatically). This action registers the new dump directory name to DUMPSRV.
5. Run BLSJPRMI (START BLSJPRMI). This action updates the in-storage copy of the dump directory name.

Your new sysplex dump directory now contains the old dumps and can be used to store new dumps.

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 276.

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 111.

How to check if CEA is active

To determine whether the CEA address space is active, enter the following command:

```
D A,CEA
```

Figure 32 on page 108 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*0    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 32. Expected results from the D A,CEA operator command

Starting the CEA address space

To start the CEA address space, enter the following command from the operator console: START CEA

It is recommended that you edit your active IEASYSxx parmlib member to identify the CEAPRMxx parmlib member to be used for the next IPL of the system. Specify the CEAPRMxx member suffix on the CEA=xx statement of IEASYSxx. The member specified in IEASYSxx will be in effect after the next system IPL.

To dynamically change the active CEA configuration, enter the MODIFY command, as follows: F CEA,CEA=xx, where xx is the suffix of the CEAPRMxx member to be used.

You can specify multiple CEAPRMxx members, for example:

```
F CEA,CEA=(01,02,03)
```

To check the resulting CEA configuration, enter the following command:

```
F CEA,D,PARMS
```

Identifying the CEAPRMxx member to use at IPL time

To ensure that common event adapter (CEA) is always active and using the correct settings, it is recommended that you edit your active IEASYSxx parmlib member to identify the CEAPRMxx parmlib member to use for the next IPL of the system. Specify the CEAPRMxx member suffix on the CEA=xx statement of IEASYSxx.

Modifying the common event adapter (CEA) settings

At any time during z/OSMF operations, you can modify CEA settings by selecting a new CEAPRMxx member. You can do so dynamically, that is, without having to restart CEA.

You might want to update the CEA settings to do the following:

- Add an eighth volume to CEA. Earlier, during the configuration prompts, if you provided VOLSER values to be used in the target CEAPRMxx member, you specified up to seven volumes as input. If you want to add an eighth volume, for example, to allow more space for diagnostic snapshots, you can update the CEAPRMxx member manually.
- Adjust the duration of OPERLOG or logrec that the system should capture for all future incidents.

If needed, you can restart CEA and specify a new CEAPRMxx member dynamically. To do so, enter the START command, as follows: START CEA. Then, enter the MODIFY command, as follows:

```
F CEA,CEA=xx
```

where xx represents the CEAPRMxx member suffix. You can specify multiple CEAPRMxx members, for example: F CEA,CEA=(01,02,03)

To check the results of these commands, enter the MODIFY command, as follows:

```
F CEA,D,PARMS
```

For information about how to configure CEA, see *z/OS Planning for Installation*.

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 110

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 IEFPSI 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. Also, the installation verification program (IVP) described in Chapter 7, “Adding plug-ins to a z/OSMF configuration,” on page 127 fails any tests that require an active SYSREXX component.

How to check if this step is done

If the AXR address space is active on the z/OS system, the System REXX component is active. To determine whether the AXR address space is active, enter the following command:

```
D A,AXR
```

Figure 33 on page 110 shows the expected results:

```

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 33. Expected results from the D A,AXR operator 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 the jobs described in *z/OS Program Directory*.

Ensuring that dump data set names are correct

If your installation has an automation program that copies an SVC dump data set to a different location using a different data set name, you must ensure that the dump data set name is changed accordingly in the sysplex dump directory. This action is necessary to allow the Incident Log task to locate the correct dump.

In your automation program, add a step to rename the dump data set in the sysplex dump directory; Figure 34 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 34. 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 3270 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 113
- "Browser consideration for the Resource Monitoring task" on page 114.

System customization for the Resource Monitoring and System Status tasks

Table 18 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 18. z/OS setup actions for the Resource Monitoring and System Status tasks

	z/OS setup action	Check when task is completed
<u>1</u>	Enable the optional priced feature, Resource Measurement Facility (RMF), on one of the systems in your enterprise. For information about enabling features, see <i>z/OS Planning for Installation</i> , GA22-7504.	
<u>2</u>	<p>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:</p> <pre>ROUTE *ALL,D A,GPMSERVE</pre> <p>If your installation uses RMF Cross Platform Monitoring (RMF XP), the RACF profile name for the RMF XP DDS is GPM4CIM, rather than GPMSERVE.</p> <p>For information about setting up the DDS and RMF XP, see <i>z/OS RMF User's Guide</i>, SC33-7990.</p>	

Table 18. z/OS setup actions for the Resource Monitoring and System Status tasks (continued)

	z/OS setup action	Check when task is completed
<u>3</u>	<p>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:</p> <pre>MODIFY GPMSERVE,OPTIONS</pre> <p>If your installation uses RMF XP, the RACF profile name for the RMF XP DDS is GPM4CIM, rather than GPMSERVE.</p> <p>In the command output, check for the HTTP_NOAUTH setting, which indicates the scope of authentication for the DDS, as follows:</p> <p>HTTP_NOAUTH() All hosts must authenticate</p> <p>HTTP_NOAUTH(*) No authentication is required</p> <p>HTTP_NOAUTH(<i>specific_host_or_mask</i>) All hosts except those matching the mask must authenticate.</p> <p>If DDS authentication is not required in your enterprise, you are done. Otherwise, proceed to Step 4.</p>	
<u>4</u>	<p>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:</p> <ul style="list-style-type: none"> • 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 <i>host_system_IP_address</i>: <pre>HTTP_NOAUTH(<i>host_system_IP_address</i>)</pre> <p>For more information about DDS authentication, see <i>z/OS RMF User's Guide</i>, SC33-7990.</p>	

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 GPMSEVER 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 GPMSEVER 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.GPMSEVER.* 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.GPMSEVER.* UACC(NONE)
```
 - Example (for a specific user ID):

```
RDEFINE PTKTDATA IRRPTAUTH.GPMSEVER.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.GPMSEVER.* CLASS(PTKTDATA) ID(passticket_creator_userid)  
ACCESS(UPDATE)
```
 - Example (for a specific user ID):

```
PERMIT IRRPTAUTH.GPMSEVER.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 185.

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 144.

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:

```
<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.**  
<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.**  
<safPrefix>.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 <safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.**. Otherwise, no actions can be performed because users will not have access to any objects.

To further restrict access to the objects and actions, define a SAF resource profile for each object and grant users the appropriate access authority. Regardless of where the physical resource described by an object resides, the SAF profiles for that object must be defined on the z/OS system that hosts the z/OSMF instance to which a user's web browser is connected. The 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 SMP/CSI data set that contains an SMP/E global zone. To control access to a specific global zone, define a SAF resource profile for that resource. The SAF resource name for a global zone object has the following format:

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

where:

- **GZN** indicates that the object associated with this SAF resource is a global zone.
- **systemName** is the name of the z/OSMF host system that has access to the global zone CSI data set. The system is defined 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.ZOS210.CSI that can be accessed by system AQFT, the SAF resource name for the global zone would be

```
<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.GZN.AQFT.MVSBUILD.ZOS210.CSI
```

Table 19 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 19. Actions users can take against global zones by access authority

Access Authority	Actions Allowed
READ	<ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• Modify the global zone properties that are <i>not</i> 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: <ul style="list-style-type: none">• Create new global zones explicitly using the Add action or implicitly as part of the Copy action.• Modify the global zone properties that are used to create the SAF resource name for the global zone and control access to the global zone. Note that, regardless of access level, the CSI data set name cannot be changed.• Remove the global zone.

Authorizing users to software instances

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

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

where:

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

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

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

For example, if you have a software instance named z/OSV2R1_Test that can be accessed by system AQFT and is assigned to categories z/OS and Test, its SAF resource names would be

```
<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.SWI.z/OS.AQFT.z/OSV2R1_Test
<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.SWI.Test.AQFT.z/OSV2R1_Test
```

Table 20 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 20. Actions users can take against software instances by access authority

Access Authority	Actions Allowed
READ	<ul style="list-style-type: none"> • 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	<p>In addition to the actions specified for READ access, users can perform the following actions:</p> <ul style="list-style-type: none"> • Modify the software instance properties that are <i>not</i> 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	<p>In addition to the actions specified for READ and UPDATE access, users can perform the following actions:</p> <ul style="list-style-type: none"> • 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:

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

where:

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

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

- **deploymentName** is the name of the deployment.

For example, if you have a deployment named z/OS_R21_Production that is not assigned to any category, its SAF resource name would be

```
<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.DEP.NOCATEGORY.z/OS_R21_Production
```

Table 21 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 21. Actions users can take against deployments by access authority

Access Authority	Actions Allowed
READ	<ul style="list-style-type: none">• View the properties of the deployment.• Copy the properties of the deployment.
UPDATE	<p>In addition to the actions specified for READ access, users can perform the following actions:</p> <ul style="list-style-type: none">• Modify the deployment properties that are <i>not</i> 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	<p>In addition to the actions specified for READ and UPDATE access, users can perform the following actions:</p> <ul style="list-style-type: none">• Create new deployments explicitly using the New action or implicitly as part of the Copy action.• Modify the deployment properties that are used to create the SAF resource name for the deployment and control access to the deployment.• Remove the deployment.

Authorizing users to categories

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

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

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

where:

- **CAT** indicates that the object associated with this SAF resource is a category.
- **categoryName** is the name of the category.

For example, if you have a category named z/OS, its SAF resource name would be

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

Table 22 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 22. Actions users can take against categories by access authority

Access Authority	Actions Allowed
READ	<ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• Modify the category properties that are <i>not</i> 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: <ul style="list-style-type: none">• Create new categories explicitly using the Add action or implicitly as part of the Copy action.• Modify the category properties that are used to create the SAF resource name for the category and control access to the category.• Remove the category.

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

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

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

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

```
RDEFINE ZMFAPLA +
(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:

```
<safPrefix>.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:

```
<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.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:

```
<safPrefix>.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 35.

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 35. Sample product information file

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 124
- “Using authorization levels for the Workload Management task” on page 124
- “Using a browser with WLM service definitions” on page 125.

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.
- During the z/OSMF configuration process, supply the name of the WLM user group in response to the following script prompt: Enter the Workload Manager group name, or press Enter to accept "WLMGRP". Alternatively, you can specify the group name on the variable IZU_WLM_GROUP_NAME in your override file.

As a result, the z/OSMF configuration script is updated to include commands to connect users to the WLM group.

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`

For an additional example, see “Commands for configuring the Workload Management plug-in” on page 321.

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, as defined on variable IZU_STARTED_TASK_USERID_NAME in your configuration or override file.

In RACF, you can use the following command:

```
PERMIT MVSADMIN.WLM.POLICY  
CLASS(FACILITY) ID(<IZU_STARTED_TASK_USERID_NAME>) ACCESS(READ)
```

2. Connect the z/OSMF started task user ID to the CIM user group. By default, the CIM user group is CFZUSRGP, as defined on variable IZU_CIM_USER_GROUP_NAME in your override file.

In RACF, you can use the following command:

```
CONNECT <IZU_STARTED_TASK_USERID_NAME> GROUP(<IZU_CIM_USER_GROUP_NAME>)
```

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.

For another example, see “Commands for configuring the Workload Management plug-in” on page 321.

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 23.

Table 23. 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 23.

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 z/OSMF configuration scripts do 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 185.

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

To add one or more plug-ins to z/OSMF, you can run the **izusetup.sh** script with a series of options, repeating some of the steps that you followed earlier to create a base z/OSMF configuration. The script uses your current configuration file as input. After a plug-in is added, you can remove it from z/OSMF only by running the **izusetup.sh** script again and not selecting that plug-in.

About the script

When used to add a plug-in, the **izusetup.sh** script 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, this script 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 script runs an installation verification program (IVP) that verifies the setup of the following z/OS system components:
 - Sysplex dump directory
 - System logger
 - Common event adapter (CEA)
 - System REXX.

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

The script resides in the `/bin` subdirectory of the z/OSMF product file system. This location is set through the `IZU_CODE_ROOT` variable in your global settings; the default is `/usr/lpp/zosmf/V2R1/bin`.

Run the script from the z/OSMF installer user ID. For the specific authorizations required, see “Selecting a user ID for adding plug-ins” on page 89.

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

Before running the script

Ensure that you collected the list of variables and other information that is described in “Planning worksheets for the z/OSMF plug-ins” on page 82. You supply these values as input to the script.

For the plug-ins to be added, ensure that you performed the appropriate z/OS system setup actions, as described in Chapter 6, “Customizing your system for the z/OSMF plug-ins,” on page 87. For example, if you plan to add the Incident Log plug-in, you completed the checklist in Table 17 on page 95 to verify that all of the setup actions were completed.

If you plan to add a plug-in that uses the CIM server (see “Reviewing your CIM server setup” on page 88), ensure that the CIM server is active on your system before you perform these steps. For information, see “Reviewing your CIM server setup” on page 88.

Steps for adding plug-ins to z/OSMF

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

1. **If you use an override file, edit it to indicate which plug-ins are to be added.** The example in Figure 36 on page 128 shows an override file that is edited to add the Capacity Provisioning plug-in to a z/OSMF configuration.

```

IZU_IL_CONFIGURE=N
IZU_CA_CONFIGURE=N
IZU_WLM_CONFIGURE=N
IZU_RMF_CONFIGURE=N
IZU_CP_CONFIGURE=A
IZU_DM_CONFIGURE=N
IZU_WISPF_CONFIGURE=N

```

Figure 36. Override file edited to add a plug-in

Configuring z/OSMF with the override file shown in Figure 36 would indicate that you want to add the Capacity Provisioning plug-in to your z/OSMF configuration. Use this same technique to add any of the z/OSMF plug-ins to your configuration.

After you complete the next steps to add the plug-in, the line will change to `IZU_CP_CONFIGURE=Y` to signify that, "yes," the Capacity Provisioning plug-in is added to your configuration.

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

2. Run the **izusetup.sh** script, as follows:

```

izusetup.sh -file izuconfig1.cfg -config
[-overridefile filename.ovr] [-fastpath] -add

```

where `izuconfig1.cfg` is the configuration file that was used during the initial configuration of z/OSMF. You overwrite this file. You can include the **-fastpath** option to have the **izusetup.sh** script run without any interactive prompting. Instead, the script uses the values from the configuration file and the override file. Omitted values cause the script to end with errors.

If you run the script in interactive mode, and specified "A" values in the override file for the plug-ins to be added, the script prompts you to either accept what was specified in the override file, or modify your plug-in selections.

If you omitted the override file in Step 1, the script prompts you to select which plug-ins are to be added. You are prompted only for plug-ins that are not already included in your configuration.

To select plug-ins, respond to this prompt, as follows:

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

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

If you run this script operation more than once, only your most recent plug-in selections are included in your configuration. Any non-selected plug-ins are removed. Therefore, specify the complete set of wanted plug-ins each time you run this script.

On completion, the **izusetup.sh** script creates a REXX exec with RACF commands for creating the security definitions for your installation. The exec name is a concatenation of your configuration file name, the plug-ins you selected, and ".rexx". If you use "izuconfig1.cfg" as your configuration file name, for example, and add two plug-ins, the exec is created as:

```

izuconfig1.cfg.add.<plug-in-1>.<plug-in-2>.rexx

```

The exec is stored in the `IZU_CONFIG_DIR` directory. The contents of the exec depend on which plug-ins you selected to configure with z/OSMF. For your reference, Appendix F, "Contents of the

RACF commands execs,” on page 301 contains the sample REXX output that would be created if all plug-ins were to be deployed in a z/OSMF configuration.

For reference, see “Step 1: Create the initial configuration” on page 33.

3. **Have your security administrator run security commands for the plug-ins.** The REXX exec **izuconfig1.cfg.add.rexx** contains sample RACF commands that your installation's security administrator can use to secure the plug-ins. Have your security administrator review the contents of the exec before running it.

With the IZU_CONFIG_DIR directory as your active directory, run the exec, as follows:

```
./izuconfig1.cfg.add.xxx.rexx
```

where *xxx* is the short name of the plug-in. If you are adding multiple plug-ins, the exec name includes the short name for each plug-in, for example: **izuconfig1.cfg.add.IL.CA.WLM.RMF.DM.rexx**

Tip: If you want a log file, you can use a z/OS UNIX command, such as **tee**, to direct the output from this exec to a log file. For example, you might direct this output to the z/OSMF log file directory for your installation (IZU_LOGFILE_DIR). By default, this directory is **/var/zosmf/configuration/logs/**.

On completion, this exec creates the security definitions that are needed for the plug-in configuration.

For reference, see “Step 2: Run the security commands for the z/OSMF resources” on page 36.

4. **Have your security administrator verify the security setup for the plug-ins.** If your installation uses RACF as its security management product, perform this step. Otherwise, skip this step and, instead, take the appropriate steps to verify your security setup.

Run the **izusetup.sh** script, as follows:

```
izusetup.sh -file izuconfig1.cfg -verify racf
```

For reference, see “Step 4: Verify the RACF security setup” on page 38.

The security setup requirements for each plug-in are described in Appendix A, “Security configuration requirements for z/OSMF,” on page 267.

5. **Deploy the plug-ins.** Run the **izusetup.sh** script, as follows:

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

This script might take some time to complete. As it runs, the script writes messages to the script log file. For reference, see “Step 5: Complete the setup” on page 39.

If you selected to configure the Incident Log task, the script runs an installation verification program (IVP) to verify the setup of z/OS system components. To see the results of the IVP, check the report file that is named **izuincidentlogverify.report**, which resides in the log file directory (IZU_LOGFILE_DIR). For more information, including corrective actions for problems that might be identified in the report, see “Using the installation verification program” on page 197. If the log file directory already contains a report file from a previous invocation, the script saves the previous report file in a backup copy, with a time stamp added to the file name.

6. **Start the z/OSMF server.** For information, see “Step 6: Start the z/OSMF server” on page 41.
7. 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. For information, see “Step 7: Access the z/OSMF Welcome page” on page 44.

Figure 37 on page 130 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 37 on page 130 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.

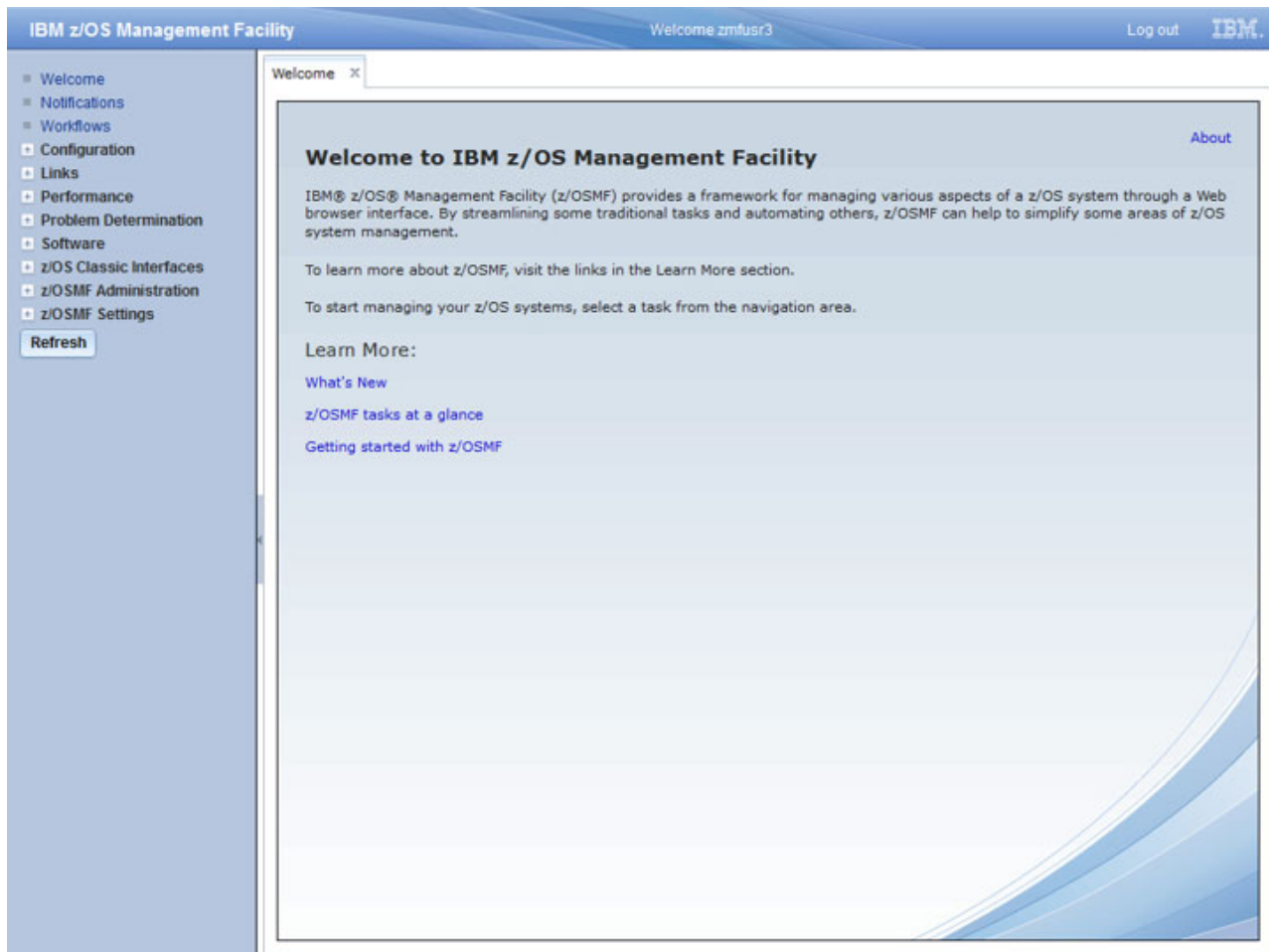


Figure 37. z/OSMF Welcome page (after you add the optional plug-ins)

What to do next

After you add an optional plug-in to z/OSMF, you can make its tasks available to users in the z/OSMF navigation area. To do so, you must authorize users to access the z/OSMF tasks, as described in Chapter 8, “Authorizing users to z/OSMF,” on page 131.

Chapter 8. Authorizing users to z/OSMF

This section describes the steps for authorizing an existing z/OS user ID to the z/OS components required for z/OSMF operations. This work includes running the **izuauthuser.sh** script to create a REXX exec with RACF commands for authorizing the user, and running that exec.

These programs are described in the following topics:

- “Creating the commands to authorize a user ID”
- “Authorizing a user ID” on page 133.

The resulting REXX exec is tailored for your z/OSMF configuration. By default, the REXX exec connects the user ID to the USER group, and includes commented commands for connecting the user ID to other groups. Examine the REXX exec and verify that the group is appropriate for the user.

If you add more plug-ins to your z/OSMF configuration later, you must re-run the **izuauthuser.sh** script and the generated rexx exec. Note that doing so can result in an “overlap” of RACF commands, for the previous set of plug-ins and the newly added plug-ins. Your security administrator should handle these situations accordingly.

The z/OSMF configuration process includes a resource called `<zSAFProfilePrefix>.izuNOUsers`, where `<zSAFProfilePrefix>` is the SAF profile prefix defined for the configuration (IZUDFLT by default). This resource is intended for z/OSMF internal use only; do not define this profile in the EJBROLE class, nor grant users access to it.

Creating the commands to authorize a user ID

You can use the script **izuauthuser.sh** to create a REXX exec with RACF commands for authorizing a user ID to one of the predefined z/OSMF roles. You can also use this script to display a list of the predefined z/OSMF roles.

About this script

This script creates a REXX exec with RACF commands for authorizing a user ID to one of the following predefined z/OSMF roles:

- z/OSMF User
- z/OSMF Administrator
- z/OS Security Administrator.

During the z/OSMF configuration process, your security administrator created security groups for the roles. Each group is permitted to a default set of z/OSMF resources (tasks and links) appropriate for the role. For the specific group permissions, see Table 46 on page 283. You can also use this script to display a list of the predefined z/OSMF roles.

Running this script

Authority

Run the script from the z/OSMF installer user ID. For the specific authorizations required, see “Selecting a user ID for configuration” on page 14.

Environment

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

Location

The script resides in the following directory:

<IZU_CODE_ROOT>/bin

where <IZU_CODE_ROOT> is the z/OSMF product file system. By default, this is /usr/lpp/zosmf/V2R1.

Invocation

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

```
izuauthuser.sh -file izuconfig1.cfg -userid userid -role role
```

Where:

- *izuconfig1.cfg* is the configuration file that you created previously in Chapter 7, “Adding plug-ins to a z/OSMF configuration,” on page 127.
- *userid* is the existing user ID for which the RACF commands are to be created.
- *role* is the z/OSMF role to which the user is to be assigned. The possible values for *role* are, as follows:
 - *user* authorizes the user ID to the role z/OSMF User
 - *admin* authorizes the user ID to the role z/OSMF Administrator
 - *security_admin* authorizes the user ID to the role z/OS Security Administrator.

In the following example, the **izuauthuser.sh** script is used to authorize the user PAXHIA to the role z/OSMF Administrator:

```
izuauthuser.sh -file izuconfig1.cfg -userid PAXHIA -role admin
```

To display a list of the available z/OSMF roles, by specifying the **-list roles** option, as follows:

```
izuauthuser.sh -list roles
```

Results

When used with the **-role** option, this script creates sample RACF commands in the following file:

<IZU_CONFIG_DIR>/izuconfig1.cfg.USERID.rexx

where <IZU_CONFIG_DIR> is the configuration file system. By default, this is /etc/zosmf.

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

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

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

When used with the **-list roles** option, this script displays a list of z/OSMF roles in your session. Figure 38 shows the output from the script when the **-list roles** option is specified.

```
# izuauthuser.sh -list roles

IZUG015I: In SAF authorization mode, the following aliases (and role files) can be specified when authorizing users.
IZUG016I: Specify "user" or "izu.user.role" to authorize the user id to this role.
IZUG016I: Specify "admin" or "izu.administrator.role" to authorize the user id to this role.
IZUG016I: Specify "security_admin" or "izu.zosSecurityAdministrator.role" to authorize the user id to this role.

IZUG210I: The script "./izuauthuser.sh" has completed.
```

Figure 38. Output from the *izuauthuser.sh* script when **-list roles** is specified

Authorizing a user ID

This section describes the REXX exec `izuconfig1.cfg.USERID.rexx`. In short, this exec contains sample RACF commands for authorizing a user ID to the z/OS components used in z/OSMF operations.

About this exec

This REXX exec contains sample RACF commands that your installation's security administrator can use to authorize a user ID to the z/OS components used in z/OSMF operations.

The content of this REXX exec is tailored based on your z/OSMF configuration. If you configured z/OSMF with the Incident Log task and the Workload Management task, for example, the resulting REXX exec will include the necessary RACF commands for authorizing a user ID to those tasks.

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

Before running the exec

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

Running this exec

Authority

This exec 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.

Environment

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

Location

The exec resides in the configuration file system (IZU_CONFIG_DIR). By default, this is `/etc/zosmf`.

Invocation

From an OMVS session, do the following:

1. Make the IZU_CONFIG_DIR directory your active directory. For example:
`cd /etc/zosmf`
2. Run the exec, as follows:
`./izuconfig1.cfg.USERID.rexx`

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

```
izuconfig1.cfg.USERID.rexx | tee
/var/zosmf/configuration/logs/izuconfig1.cfg.USERID.rexx.output
```

For techniques, see *z/OS UNIX System Services User's Guide*.

Results

On completion, this exec creates the required security definitions for the user ID on the z/OS system.

Chapter 9. Using z/OSMF in a multi-system environment

By default, the z/OSMF configuration process produces a configuration that is set up for a single-system environment. If you plan to use z/OSMF in a multi-system environment, or across sysplexes, the decisions you make during the first-time setup can help to simplify the management of z/OSMF later. You can, for example, deploy the initial instance of z/OSMF in such a way that the product can be started from any system in your sysplex. Doing so can help to address z/OSMF high availability. This is an important consideration when deploying any application in a sysplex environment.

The following terms are used in this topic:

- *High availability* refers to the ability to move workload processing from one system to another in the same sysplex without impacting workloads. A system with high availability characteristics should experience little or no disruption in service, even during planned outages or failures.
- *z/OSMF virtualization* refers to the way z/OSMF is configured so that one instance can be started on any system in the sysplex.
- *Cloning* means the ability to replicate an instance of an application to another system or sysplex. An application that supports cloning allows you to propagate its function throughout your enterprise, rather than having to rebuild the application fresh on each new system.

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

- “Configuring z/OSMF for high availability”
- “Cloning a primary instance of z/OSMF” on page 140
- “Modifying the z/OSMF host name” on page 141
- “Additional considerations for a multi-system environment” on page 143
- “Configuring a primary z/OSMF for communicating with secondary instances” on page 144
- “Enabling single sign-on between z/OSMF instances” on page 147.

Configuring z/OSMF for high availability

By default, the z/OSMF configuration process creates a system-specific configuration. For availability purposes, however, you might want to create a z/OSMF instance that can be restarted on another system in the same sysplex, or perhaps cloned to another sysplex. This topic describes how to configure z/OSMF for high availability in a sysplex environment. Some considerations described here are applicable to any application that you might want to deploy in a sysplex environment.

Generally, you should configure the initial instance of z/OSMF using a single, shared directory structure, so that one instance can be started on any system in the sysplex. When deployed in this way, z/OSMF is said to be *virtualized*, that is, system-independent.

For scenarios and examples of implementing z/OSMF in a multi-system sysplex environment, see the chapter on high availability in IBM Redbook *IBM z/OS Management Facility V2R1*, SG24-7851.

Mount points and file systems

By default, the z/OSMF configuration process creates product directories at the non-sharable mount points /etc and /var, as follows:

- The IZU_CONFIG_DIR variable specifies the path for the configuration directory, which is /etc/zosmf by default. This path contains the configuration file and optionally an override file that is used in the configuration process. Also, the configuration process creates additional directories and files, which are used by the z/OSMF started tasks.

- The IZU_LOGFILE_DIR variable specifies the path where logs are created during the configuration process. By default, this is /var/zosmf/configuration/logs.
- The IZU_DATA_DIR variable specifies the mount point for the z/OSMF data file system. By default, this is /var/zosmf/data.

To create a virtualized (or system-independent) instance of z/OSMF, you can specify a common, root directory for these mount points, such as /sharedapps. Doing so can help to simplify z/OSMF management later, for such operations as moving z/OSMF to another system, and cloning instances of z/OSMF.

Besides specifying a shared root directory mount point, several other configuration time settings are relevant for multi-system environments. See Table 24 for suggested settings.

Table 24. What variable settings are important for a multi-system environment?

Directory or structure	Variable name	Setting for a single-system environment (the default value)	Suggested setting for a virtualized z/OSMF instance	Notes
Mount point of the z/OSMF data file system.	IZU_DATA_DIR	/var/zosmf/data	/sharedapps/zosmf/data	
Name of the z/OSMF data file system.	IZU_DATA_FS_NAME	IZU.SIZUDATA	IZU.SIZUDATA	See Table Notes 1 and 2.
z/OSMF configuration directory.	IZU_CONFIG_DIR	/etc/zosmf	/sharedapps/zosmf/data/configuration	See Table Note 3.
z/OSMF log directory.	IZU_LOGFILE_DIR	/var/zosmf/configuration/logs	/sharedapps/zosmf/data/configuration/logs	
z/OSMF started task home directory.	IZU_STARTED_TASK_USERID_HOME	/var/zosmf/data/home/izusvr	/sharedapps/zosmf/data/home/izusvr	
z/OSMF server host name.	IZU_APPSERVER_HOSTNAME	@HOSTNAME. This value resolves to a specific host name fully-qualified domain name (FQDN).	Specify asterisk (*) to use the local host name. Alternatively, you can specify a dynamic VIPA (DVIPA) that resolves to the correct IP address.	See Table Note 4.

Table Notes:

1. Each active instance of z/OSMF requires its own data file system. When you use a virtualized z/OSMF instance, there is one data filesystem, which is accessible from any of the systems that are to run the virtualized z/OSMF instance. For your initial instance of z/OSMF, create a shared data file system (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.
2. If you plan to run more than one instance of z/OSMF in a sysplex, you require a unique data file system (and data file system name) for each instance. Consider using the system name to qualify the name of the data file system. For example: IZU.<system-name>.SIZUDATA. In contrast, if you plan to use a virtualized instance of z/OSMF, you need only one data file system; it will be shared by all participating systems. Consider using the name IZU.SIZUDATA, which is provided by default.
3. The z/OSMF data file system contains the configuration information for z/OSMF. If you plan to clone the z/OSMF instance, you should mount a separate file system at this directory, so that all

configuration information is contained in the separate file system. Only during the initial cloning process should you clone both the data file system and this configuration file system. If service is applied in the future, it might involve the configuration file system; if so, clone only the configuration file system after applying the service. More information is provided in “Cloning a primary instance of z/OSMF” on page 140.

4. A technique for using system symbols to create unique host names for z/OSMF instances is described in “Modifying the z/OSMF host name” on page 141.

Network connectivity

You can use the z/OS Communications Server TCP/IP sysplex networking dynamic VIPA (DVIPA) function to help ensure the availability of z/OSMF. If your installation has a primary z/OSMF instance and a backup instance, if the primary instance becomes unavailable, you can start the backup instance. With DVIPA, your installation can move z/OSMF to the backup system if a failure occurs on the primary system. This action allows z/OSMF to bind again to the same DVIPA address, and resume operation. z/OSMF remains available for workloads throughout the failover process.

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 80 443
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 at least one of the ports 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*.

Scenario for using a virtualized instance of z/OSMF

This topic presents an example scenario for using a virtualized instance of z/OSMF:

- “Create a virtualized instance of z/OSMF” on page 138. Here, you configure an instance of z/OSMF for high availability.
- “Restart z/OSMF processing on another system in the same sysplex” on page 140. Here, you start the virtualized instance on another system in the same sysplex.

This topic 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*.

The procedures assume that you followed the suggested values in Table 24 on page 136. For illustrative purposes, the examples refer to the fictional systems: "System A" and "System B."

Further considerations are provided in "Additional considerations for a multi-system environment" on page 143.

Create a virtualized instance of z/OSMF

You can create an instance of z/OSMF with characteristics that will allow it to be started from any system in the sysplex. In the example that follows, all of the configuration settings and data are created in the z/OSMF data file system, to be located at the following shared location: `/sharedapps/zosmf/data`.

Example: Follow these steps to configure z/OSMF on System A:

1. Create the root directory at a sysplex-wide, shared mount point. For example: `/sharedapps`.
2. Create the z/OSMF data file system directory: `/sharedapps/zosmf/data`.
3. Allocate the z/OSMF data file system, if it does not exist already.
4. Mount the z/OSMF data file system at the shared mount point:

```
/usr/sbin/mount -f 'IZU.SIZUDATA' /sharedapps/zosmf/data
```

where IZU.SIZUDATA is the default name of the z/OSMF data file system.

5. Create a configuration directory `/sharedapps/zosmf/data/configuration`. Allocate and mount a small ZFS file system at this mount point. For example:

```
zfsadm define -aggregate 'IZU.CONFDATA' -volumes PEVTS4 - cylinders 150 50
zfsadm format -aggregate 'IZU.CONFDATA' -compat
/usr/sbin/mount -f 'IZU.CONFDATA' /sharedapps/zosmf/data/configuration
```

Observe that a separate file system is created for the configuration data; this step allows for easier application of service to z/OSMF.

6. Copy the IBM-supplied environment variables file `/usr/lpp/zosmf/V2R1/defaults/izu_env.sh` to the newly created configuration directory:

```
/sharedapps/zosmf/data/configuration/izu_env.sh
```

For example:

```
cp /usr/lpp/zosmf/V2R1/defaults/izu_env.sh
/sharedapps/zosmf/data/configuration/izu_env.sh
```

If you rename the environment variables file, choose a name that is meaningful. The examples in this section use the name `izu_env.sh`. This name is case sensitive.

7. Modify the environment variables file with new values, as shown in Figure 39 on page 139.

```
# Default value for the configuration directory
export IZU_CONFIG_DIR=/sharedapps/zosmf/data/configuration
#
# Default value for the log file directory
export IZU_LOGFILE_DIR=/sharedapps/zosmf/data/configuration/logs
```

Figure 39. Updating the izu_env.sh file

8. Export the variable IZU_ENV_FILE, setting it to the location of the environment variables file. Or, add the export command to the .profile for the user ID that you use to run the scripts. The following export command example assumes that you have placed the environment variables file in the configuration directory and named it izu_env.sh:

```
export IZU_ENV_FILE=/sharedapps/zosmf/data/configuration/izu_env.sh
```

9. Copy the IBM-supplied override file /usr/lpp/zosmf/V2R1/defaults/izudflt.ovr to the z/OSMF configuration directory:

```
/sharedapps/zosmf/data/configuration/izudflt.ovr
```

For example:

```
cp /usr/lpp/zosmf/V2R1/defaults/izudflt.ovr
/sharedapps/zosmf/data/configuration/izudflt.ovr
```

10. Update the override file (izudflt.ovr) with your site specific values, including the values shown in Figure 40.

```
IZU_DATA_DIR=/sharedapps/zosmf/data
IZU_DATA_FS_NAME=IZU.SIZUDATA
IZU_STARTED_TASK_HOME=/sharedapps/zosmf/data/home/izusvr
```

Figure 40. Updating the override file

11. Run the **izusetup.sh** script to begin the configuration process:

```
izusetup.sh -config -file izuconfig1.cfg -overridefile izudflt.ovr
```

On the **izusetup.sh** script invocation, omit the path name from the configuration file that you specify on the -file parameter to use the configuration directory path that you set in Step 7. This is important because the IZU_CONFIG_DIR variable should refer to your shared directory structure (/sharedapps).

Complete the steps required to create a base z/OSMF configuration, as described in “Creating a base z/OSMF configuration” on page 29.

12. Start the z/OSMF server on System A:

```
START IZUANG1
START IZUSVR1,USERDIR='/sharedapps/zosmf/data/configuration'
```

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

If the z/OSMF directories are mounted at a shared mount point, as described in “Create a virtualized instance of z/OSMF” on page 138, moving z/OSMF processing to another system requires only that you restart the server on another system in the sysplex.

Example: Follow these steps:

1. Stop the z/OSMF server on System A
2. Start the z/OSMF server on System B.

When starting the server on the new system, specify the configuration directory on the start command. For example:

```
START IZUANG1
START IZUSVR1,USERDIR='/sharedapps/zosmf/data/configuration'
```

Cloning a primary instance of z/OSMF

This topic describes how to clone an existing instance of z/OSMF to another sysplex without having to run the configuration scripts to reinstall the product.

This topic 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*.

The procedure assumes that you followed the suggested values in Table 24 on page 136. For illustrative purposes, the procedure refers to the fictional system "System C."

Steps for cloning an instance of z/OSMF

This procedure allows you to clone z/OSMF to another sysplex without having to run the configuration scripts to create a new instance. To do so, you will clone the following z/OSMF file systems:

- z/OSMF data file system (IZU.SIZUDATA)
- z/OSMF configuration file system (IZU.CONFDATA).

Mount these file systems at the same mount points that are defined in the source system.

The z/OSMF data file system contains run-time information that will be updated with system or sysplex specific information. Therefore, you should clone this file system only the first time that you create another z/OSMF instance. The z/OSMF configuration file system contains configuration information that might be updated in the service stream, thus, this information would need to be propagated or cloned with the usual service levels. You can then clone this file system after applying the service.

You will also need to update the host name of the newly cloned instance, as described in “Modifying the z/OSMF host name” on page 141.

The following example summarizes the steps to follow:

1. Copy your z/OSMF related security definitions to the System C security database, or create an equivalent set of security definitions. Use RACF remote sharing, if applicable.
2. Create the root directory at a sysplex-wide, shared mount point. For example: /sharedapps.
3. Create the z/OSMF data file system directory: /sharedapps/zosmf/data
4. Clone the file system from the source sysplex and move it to the destination sysplex.
5. Mount the z/OSMF data file system at the shared mount point: /usr/sbin/mount -f 'IZU.SIZUDATA' /sharedapps/zosmf/data
where IZU.SIZUDATA is the default name of the cloned z/OSMF data file system.

6. Mount the configuration file system at the shared mount point: `/usr/sbin/mount -f 'IZU.CONFDATA' /sharedapps/zosmf/data/configuration`
7. Update the host name (or the system symbols that represent it) for the cloned z/OSMF configuration.
8. Start the z/OSMF server on System C.

When starting the server on the new system, specify the configuration directory on the start command. For example:

```
START IZUANG1
START IZUSVR1,USERDIR='/sharedapps/zosmf/data/configuration'
```

Modifying the z/OSMF host name

Your installation might want to create additional copies of an existing z/OSMF configuration, for cloning or high availability purposes. If so, a key requirement is that a unique host name must be associated with each instance of z/OSMF. This topic describes a technique for using system symbols to create unique host names for cloned z/OSMF configurations.

About the z/OSMF host name

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.

As part of the z/OSMF configuration process, you 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. z/OSMF saves the host name as variable IZU_APPSERVER_HOSTNAME in the configuration file.

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 “Network connectivity” on page 137.

Using a cloned z/OSMF configuration with a different host name

Suppose that you want to replicate z/OSMF throughout your enterprise, rather than having to rebuild the product fresh on each new system. You would do this, for example, when you want to clone a model z/OSMF instance and distribute it to another sysplex.

For the most part, z/OSMF supports cloning, but when you copy a z/OSMF configuration to another system, you copy its host name, too, which means that it is no longer unique. Therefore, you must take additional steps to ensure that a unique host name is associated with each cloned instance of z/OSMF. Here, you might find it convenient to use one or more z/OS system symbols to represent the z/OSMF host name on each z/OS system.

To create a unique host name for a cloned z/OSMF configuration, consider using the following technique:

1. When creating the initial z/OSMF configuration, accept the default host name value @HOSTNAME, which resolves to the hostname of the system that is used to configure z/OSMF. (To use a DVIPA address instead of system symbols, substitute the DVIPA address for the default host name value, then proceed to Step 7 in this procedure.)
2. Define a system symbol (or a series of system symbols) for the z/OSMF host name on each z/OS system that might run a cloned z/OSMF configuration. This step requires creating or updating an IEASYMxx parmlib member with one or more symbols that represent the host name that you want to change. If you already have a system symbol defined for host name, use the symbol.

You can represent part of the host name with a system symbol or the entire host name through a series of symbols.

In the following example, assume that symbols are used to resolve to either of the following host names, as needed:

STEAKS.TOGO.RESTAURANT.COM

SALADS.TOGO.RESTAURANT.COM

The variable portion of each host name is the first node (STEAKS or SALADS), followed by the static part of the host name (TOGO.RESTAURANT.COM).

The z/OSMF host name in this example consists of several symbols, using a common naming convention &IZUHNm.. Notice that the RESTAURANT node exceeds eight characters, thus, two symbols are used in combination to represent the node.

On System A, the host name is defined as follows:

```
SYSDEF SYMDEF(&IZUHN1.='COM')
SYSDEF SYMDEF(&IZUHN2.='URANT')
SYSDEF SYMDEF(&IZUHN3.='RESTA')
SYSDEF SYMDEF(&IZUHN4.='TOGO')
SYSDEF SYMDEF(&IZUHN5.='STEAKS')
```

3. On System B, the host name is defined as follows:

```
SYSDEF SYMDEF(&IZUHN1.='COM')
SYSDEF SYMDEF(&IZUHN2.='URANT')
SYSDEF SYMDEF(&IZUHN3.='RESTA')
SYSDEF SYMDEF(&IZUHN4.='TOGO')
SYSDEF SYMDEF(&IZUHN5.='SALADS')
```

For more information about creating system symbols and the IEASYMxx member, see *z/OS MVS Initialization and Tuning Reference*.

4. Define the IEASYMxx member in the LOADxx member for the system on which the cloned z/OSMF configuration will run.
5. Activate or refresh the IEASYMxx parmlib member so that the symbols are defined to the system and the z/OSMF server will use them. You can do this dynamically through the **SETLOAD** command.
6. In the initial z/OSMF configuration, update the bootstrap.template file to substitute the symbol for the host name value. For a procedure to use, see “Updating the bootstrap.template file.”
7. Clone the initial z/OSMF configuration and distribute it to another system or sysplex. For considerations, see “Configuring z/OSMF for high availability” on page 135.
8. Restart the z/OSMF server on each system to use the updated definitions and symbols.

When you change the host name, the product URL is changed. Be sure to provide users with the new URL to use for accessing z/OSMF through a web browser. Users can add the URL to the browser bookmarks list.

Updating the bootstrap.template file

To use a host name symbol for a cloned z/OSMF configuration, such as the one that was defined in “Using a cloned z/OSMF configuration with a different host name” on page 141, you must modify the bootstrap.template file. This step ensures that the cloned z/OSMF is started with a unique host name.

To modify the host name, do the following:

1. Locate the z/OSMF bootstrap.template file. By default, the location is: /etc/zosmf/servers/zosmfServers/bootstrap.templateok
2. Save a copy of the existing bootstrap.template file as a back-up.
3. In the bootstrap.template file, locate the izu.hostname property. The contents of the file are shown in Figure 41 on page 143.

```
# Licensed Materials - Property of IBM
#
# "Restricted Materials of IBM"
#
# Copyright IBM Corp. 2013 All Rights Reserved.
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with
# IBM Corp.
#
# -----
#

izu.hostname=*
izu.https.port=443
izu.http.port=80
```

Figure 41. Bootstrap properties for z/OSMF

Update the property `izu.hostname=` to use the system symbols that you have defined. You can replace part of the host name with a system symbol or the entire host name through a series of symbols.

In the following example, the host name from the previous example is substituted. Note that the host name is comprised of several symbols, with a “.” separating them. When resolved, these symbols (inclusive of the & and “.”) provide the host name.

```
izu.hostname=&IZUHNM5..&IZUHNM4..&IZUHNM3..&IZUHNM2..&IZUHNM1.
```

The value of the symbol cannot exceed the number of characters in the symbol name itself; the maximum number of characters for a symbol is eight.

4. Save the `bootstrap.template` file
 5. Restart the z/OSMF server and verify z/OSMF operations with the new host name.
-

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 data file system can be used by only a single instance of z/OSMF in a sysplex at a given time. To prevent the same z/OSMF data file system from being accessed by more than one instance of z/OSMF, z/OSMF locks the data file system through a global resource serialization ENQ with QNAME ZOSMF. If you start a second instance of z/OSMF using the same data file system, that z/OSMF will not be usable. Users who attempt to access the second instance of z/OSMF will encounter an error web page (message IZUG680E). Further, all log messages from the second instance of z/OSMF are routed to the z/OSMF server logs directory, rather than to the log in the z/OSMF data file system.
- Do not list the QNAME ZOSMF ENQ in the resource name list (RNL) in your installation's GRSRNLxx member.
- Running multiple instances of z/OSMF simultaneously in a sysplex, using different z/OSMF data file systems, is not recommended 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.IZU_SAF_PROFILE_PREFIX
- CA name is:

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

z/OSMF creates the CA if you specify Y for variable IZU_DEFAULT_CERTAUTH during the configuration process. If you specify N for this variable, z/OSMF does not create the CA, and, instead, signs the server certificate with CERTAUTH LABEL('zOSMFCA').

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 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 set the configuration variable `IZU_DEFAULT_CERTAUTH` to `N` on the secondary images, so that no CA is created and the imported CA is used, instead. Thus, 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.”

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 `IZU_SAF_PROFILE_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 146.

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 42 on page 146, both the primary z/OSMF and the secondary instances are identified by server certificates that were created using the same CA (Jupiter).

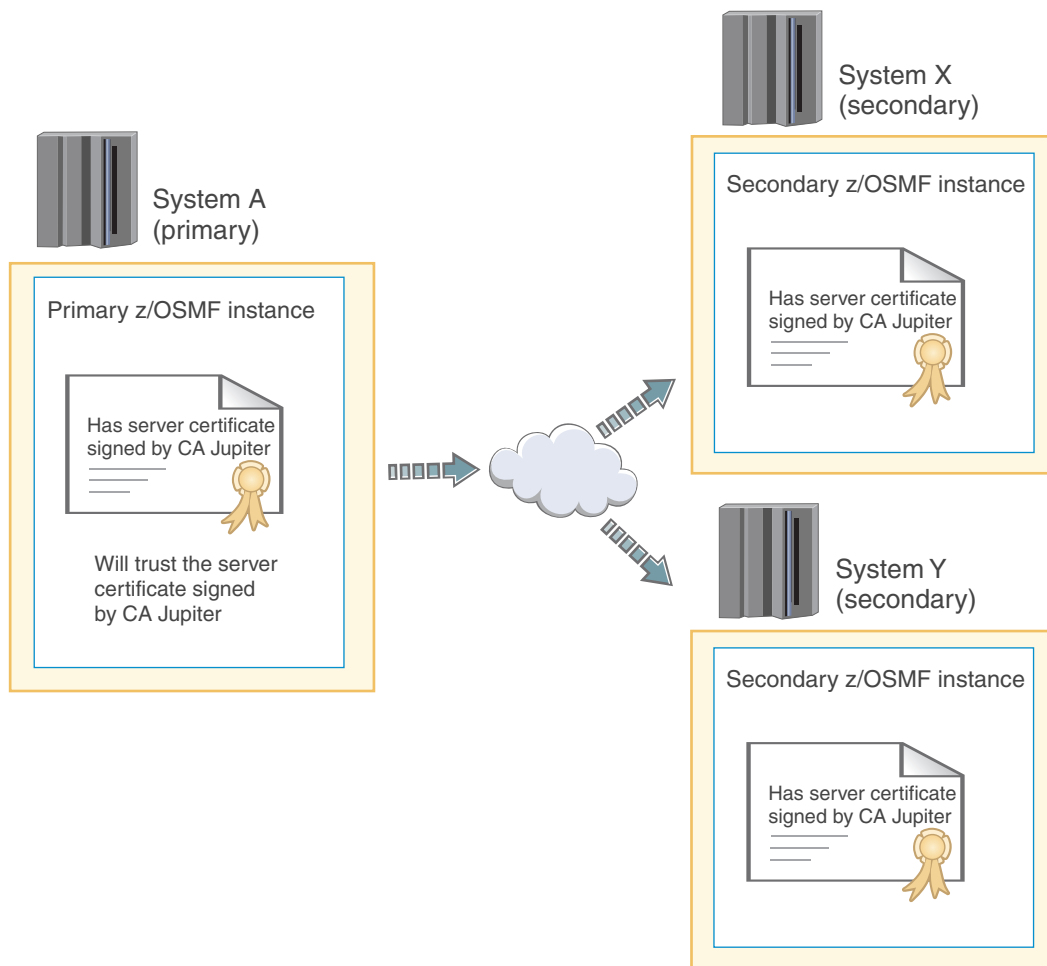


Figure 42. Trust relationship when server certificates are signed by the same CA certificate

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 43 on page 147, 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.

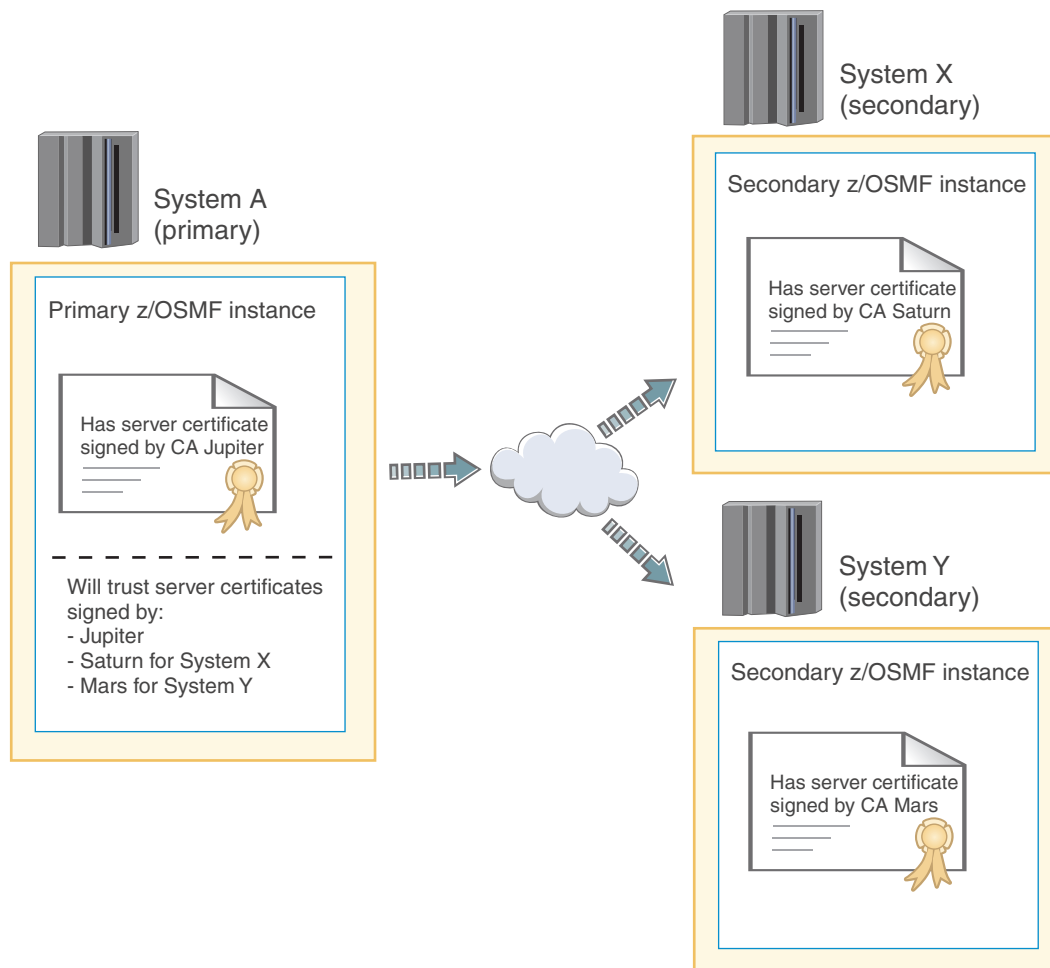


Figure 43. Trust relationship when the server certificates are signed by different CA certificates

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*.
- | • 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 IZU_SAF_PROFILE_PREFIX variable 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 profile 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 10, “Modifying the z/OSMF default keyring name,” on page 151
- Chapter 11, “Customizing the Welcome page for guest users,” on page 153
- Chapter 12, “Linking z/OSMF tasks and external applications,” on page 155
- Chapter 13, “Configuring your system for asynchronous job notifications,” on page 157
- Chapter 14, “Adding links to z/OSMF through the izusetup.sh script,” on page 167
- Chapter 15, “Using the verify function as needed,” on page 171
- Chapter 16, “Deleting incidents and diagnostic data,” on page 173
- Chapter 17, “Troubleshooting problems,” on page 177
- Chapter 18, “Configuration messages,” on page 215.

Chapter 10. Modifying the z/OSMF default keyring name

z/OSMF creates digital certificates that are used for secure communications between the user's web browser and the z/OSMF server, and between instances of z/OSMF servers.

The z/OSMF keyring name is generated during the configuration phase. The keyring name format is `IZUKeyring.<IZU_SAF_PROFILE_PREFIX>`. By default, the keyring name is `IZUKeyring.IZUDFLT`.

In most cases, the default z/OSMF keyring name should be sufficient for your installation. In some situations, however, your installation might require that another keyring name be used instead. Though it is possible to modify the z/OSMF keyring name, understand that doing so can affect secure communications. This modification should be attempted only by administrators who understand how digital certificates are used and stored by the security product.

The z/OSMF keyring name is not a user-selectable option during the configuration process. Thus, if you want to modify the z/OSMF keyring name, you should do so only after you have created a z/OSMF configuration. That is, you must complete and verify an initial z/OSMF configuration through all phases of set-up, that is:

1. Running the **izusetup.sh** script with the option `-config`
2. Performing the security set-up using the generated REXX exec
3. Running the **izusetup.sh** script with the option `-finish`.
4. Starting the z/OSMF server
5. Verifying connectivity between the browser and the z/OSMF application.

After the configuration is created, you can modify the z/OSMF keyring name. Note that the generated RACF REXX exec contains statements that include the generation of digital certificates and the keyring; you might want to refer to the exec as a reference when performing the steps that follow.

To modify the keyring name, do the following:

1. Locate the z/OSMF `bootstrap.template` file. By default, the location is: `/etc/zosmf/servers/zosmfServers/bootstrap.template`
2. Save a copy of the existing `bootstrap.template` file as a back-up.
3. In the `bootstrap.template` file, edit the keyring name property to specify the new keyring name. The property and default value is:

```
izu.ssl.key.store.saf.keyring=IZUKeyring.IZUDFLT
```

4. Save the `bootstrap.template` file
5. Restart the z/OSMF server and verify z/OSMF operations with the new keyring name.

Chapter 11. Customizing the Welcome page for guest users

Your installation can customize the content of the z/OSMF Welcome page for non-authenticated guest users. You might do so, for example, to provide users with information they should read before logging in to z/OSMF, such as instructions specific to your company. You can even add a small image or graphic, such as your company logo. After the guest user authenticates, the Welcome page is replaced with the standard z/OSMF Welcome page.

What can be customized

You can customize the following areas of the Welcome page:

Header area

Horizontal area above the main work area

Footer area

Horizontal area below the main work area

Image area

Small area at the right end of the footer.

Figure 44 shows the areas of the z/OSMF Welcome page that can be customized.



Figure 44. Customizable areas of the z/OSMF Welcome page

As shown in Figure 44, 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 44, the IBM logo is shown in this position.

Steps for customizing the Welcome page

A sample Welcome page properties file is supplied with z/OSMF:

```
<IZU_CODE_ROOT>/samples/customWelcome.properties
```

where `<IZU_CODE_ROOT>` is the z/OSMF product file system. By default, this is `/usr/lpp/zosmf/V2R1`.

To customize the Welcome page, follow these steps:

1. **Copy the sample Welcome properties file to the correct location.** Copy the sample Welcome properties file to the z/OSMF data file system directory. You specified this directory on the `IZU_DATA_DIR` configuration variable (by default, the directory is `/var/zosmf/data`).
It is recommended that you copy the file using the z/OSMF installer user ID that you created earlier; see “Selecting a user ID for configuration” on page 14. 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 45, the Welcome properties file contains the following input fields for the customizable areas:

```
header=  
footer=
```

Figure 45. 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 (`\uxxxx`) is treated as one character.

As an example, Figure 46 shows the Welcome page properties file that was used to customize the Welcome page in Figure 44 on page 153.

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

Figure 46. Example of a Welcome page properties file

3. **Add an image file, if required.** If you include an image file, such as your company logo, it must be named `customLogo` and have one of the following image formats: `.png`, `.jpeg`, `.jpg`, `.gif`, or `.bmp`. The required name and file type is case sensitive. Other names, if specified, are ignored. If you provide multiple image types, the priority order is: `.png`, `.jpeg`, `.jpg`, `.gif`, and `.bmp`.
The image size is limited to the area allotted on the Welcome page, which is about 120x40 pixels. A larger image will be scaled down to that size. A smaller image is not scaled up to that size.
Store the image file in the z/OSMF data file system directory, with the same ownership and permissions as done for the Welcome properties file in Step 1.
If the image file you supply is empty or corrupted, z/OSMF displays the following alternate text in place of the image:
Custom Company Logo
4. **View your changes.** Refresh your browser to display the customized Welcome page.

Chapter 12. 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 47 depicts the relationship of these components in the application linking process.

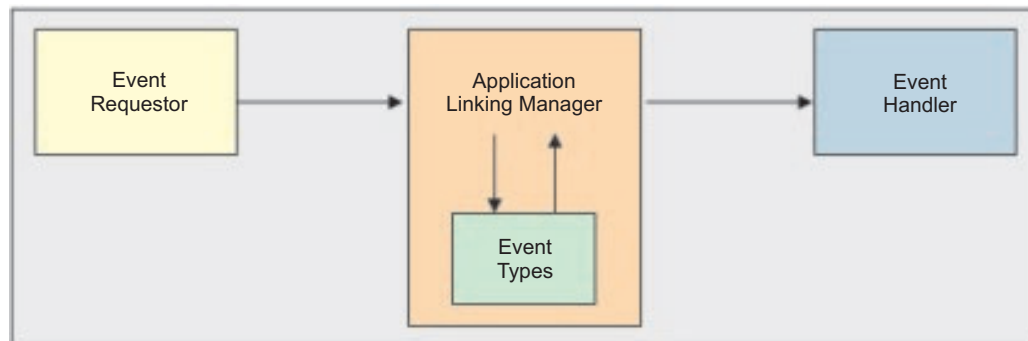


Figure 47. Key components in the application linking process

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.

- 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 13. 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 163.

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.

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 159
- 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 159.

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 89.

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 48 on page 159 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 48. 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 90.

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 49, 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 49. Subscription values for asynchronous job notification

In Figure 49, <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 49 on page 159, 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 160. 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 160.

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/;/\\\"~"

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 14. Adding links to z/OSMF through the `izusetup.sh` script

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 `izusetup.sh` script. If so, you can follow the steps in this section. You can add one link for each invocation of the `izusetup.sh` script.

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.

Before running the script

Ensure that z/OSMF is running. Otherwise, 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.

Steps for adding a link to z/OSMF

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

```
<IZU_CODE_ROOT>/samples/sampleLink.properties
```

where `<IZU_CODE_ROOT>` is the z/OSMF product file system. By default, this is `/usr/lpp/zosmf/V2R1`.

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

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

Figure 50. Content of the link properties file

In your link properties file, define the link using these input fields:

LinkName

Specify a name for the link, as it should be displayed in the z/OSMF navigation area. Specify a value of up to 30 characters, including alphanumeric characters (A-Z a-z 0-9), blanks, mathematical symbols (+ - = | ~ () { } \), punctuation marks (? , . ! ; : ' " / []), and the following special characters: %, \$, #, @, ^, *, and _. Any leading or trailing white space is ignored.

Specify your input in the form of the ASCII, EBCDIC or Unicode character sets. To use Japanese language characters, enter the characters in Unicode. Each Unicode character (`\uxxxx`) is treated as one character.

The name you select must be unique among the existing links defined in z/OSMF. It is recommended that you choose a name that will be easily understood by users. Avoid names that might be confused with other links or tasks in z/OSMF.

LinkURL

Specify the location for the link (a URL), which is a valid Internet or intranet address, for example:

`http://www.ibm.com`

The URL can be up to 4000 characters, including alphanumeric characters (A-Z a-z 0-9), blanks, mathematical symbols (+ - = | ~ () { } \), punctuation marks (? , . ! ; : ' " / []), and the following special characters: %, \$, #, @, ^, *, and _. Any leading or trailing white space is ignored.

z/OSMF performs limited syntax checking of the specified URL. Ensure that the link location is a syntactically correct URL. Generally, a URL includes a protocol (such as `http://`), a host name (`www.hostname.com`), and, often, a resource such as a directory path and file.

LinkNavigationCategory

Specify 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 script adds the link to the table displayed in the Links task with no roles assigned to it.

LinkSafSuffix

Specify the system authorization facility (SAF) resource name suffix to be used for managing user authorizations to the link. To create a unique resource name for the link, z/OSMF appends this value to the 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 51 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 51. Example of a link definition

3. **Add the link to z/OSMF.** From the z/OSMF installer user ID, run the **izusetup.sh** script, as follows:

```
izusetup.sh -file filename.cfg -addlink <pathname/link-properties-filename>
```

Figure 52. Syntax for adding a link to z/OSMF

where *link-properties-filename* is your link properties file.

This script might take some time to complete.

Processing your request

As it processes, the script writes messages to standard output and to the script log file:

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

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

Check the messages to determine whether a problem occurred during -addlink processing. If so, you must resolve the problem before the link can be added.

If z/OSMF is down, you must restart it to complete the processing of your request; see message IZU398I.

Results

On completion, the script issues message IZUG397I, which directs you to check the z/OSMF runtime log file (IZUGx.log) for an indication of whether the link was added. For more information, see “Working with z/OSMF runtime log files” on page 187.

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 53 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 53. 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 15. Using the verify function as needed

Whenever you make changes to your z/OSMF configuration, you can optionally verify your setup, as often as needed. To do so, you run the **izusetup.sh** script with option **-verify**.

To verify your configuration, run the **izusetup.sh** script with option **-verify**, as described in “Step 4: Verify the RACF security setup” on page 38. To select the scope of the verification, include one of the options shown in Table 25 with the **-verify** option.

Table 25. Script options for verification

Script option	Scope of verification
all	Verifies that all of the selected plug-ins were deployed. Also, if you selected to configure the Incident Log plug-in, this option runs the installation verification program (IVP) for verifying the z/OS system setup for the Incident Log task.
core	Verifies that the core functions were initialized.
log	Verifies that the Incident Log plug-in was deployed. This option also runs the installation verification program for verifying the z/OS system setup for the Incident Log task.
racf	Verifies the RACF security setup for all of the configured tasks and functions. This option should be used by your security administrator.

For example:

```
izusetup.sh -file izuconfig1.cfg -verify all
```

where **izuconfig1.cfg** is your current configuration file. If you omit the directory path, the script uses the z/OSMF configuration directory **<IZU_CONFIG_DIR>**, by default.

The script checks that all necessary configuration steps were carried out.

On completion, you can view the script output messages in the following log file:

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

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

If you run the script with the options **all**, **log**, or **racf**, the script creates a report indicating any areas that might require further action on your part. The report resides in the following location:

```
<IZU_LOGFILE_DIR>/izuincidentlogverify.report
```

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

For more information, see “Reviewing the results of the **izuincidentlogverify.report** file” on page 198.

Chapter 16. 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 107 and “Ensuring that System REXX is set up and active” on page 109.
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 increases 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.

Invoking the utility

The **ceatool** command-line interface must be invoked from the z/OS UNIX System Services shell or a BPXBATCH environment. Figure 54 shows the format of the **ceatool** command, which invokes the utility.

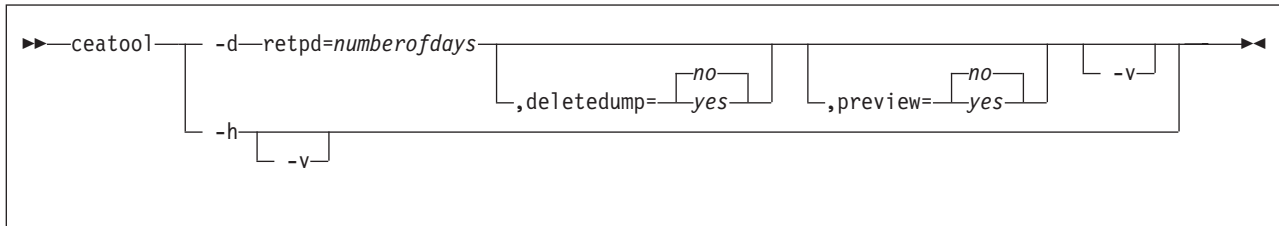


Figure 54. Format of the **ceatool** command.

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

Table 26. Sample ceatool commands

Sample Command	Results
<code>ceatool -d retpd=7,deletedump=no</code>	Deletes inactive incidents and the corresponding diagnostic data, excluding SVC dumps, that are older than seven days.
<code>ceatool -d retpd=7,deletedump=yes</code>	Deletes inactive incidents and the corresponding diagnostic data, including SVC dumps, that are older than seven days.
<code>ceatool -d retpd=7,deletedump=yes -v</code>	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.
<code>ceatool -d retpd=0</code>	Deletes all inactive incidents and the corresponding diagnostic data, excluding SVC dumps.
<code>ceatool -d retpd=7,preview=yes</code>	Displays the number of inactive incidents that are older than seven days. The incidents that satisfy the filter criteria are not deleted.
<code>ceatool -h</code>	Displays help for the ceatool command.
<code>ceatool -hv</code>	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 17. 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 178
- “Common problems and scenarios” on page 192.

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 27 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 27. 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 178.	N/A
z/OSMF core functions and system management tasks	<ul style="list-style-type: none">• The About page• z/OSMF log files and tracing.	<ul style="list-style-type: none">• “Finding information about z/OSMF” on page 186• “Working with z/OSMF runtime log files” on page 187.• “Problems when using Configuration Assistant” on page 210.	Messages encountered while configuring z/OSMF; see Chapter 18, “Configuration messages,” on page 215. 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.	“Enabling tracing and logging for z/OSMF” on page 188.	<ul style="list-style-type: none">• Chapter 18, “Configuration messages,” on page 215• 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/webervers/appserv/was/library/v85/was-zos/index.html .	Messages prefixed by CW.
CIM server and CIM providers	<ul style="list-style-type: none">• 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 <i>z/OS Common Information Model User's Guide</i> .	<i>z/OS Common Information Model User's Guide</i> .
Common event adapter (CEA)	System commands: <ul style="list-style-type: none">• MODIFY CEA• MODIFY AXR• TRACE CT.	z/OS MVS System Commands.	<i>z/OS MVS System Messages</i> for information about: <ul style="list-style-type: none">• WTO messages• CTRACE• Reason codes.

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 24.

Ensure that your browser is enabled for JavaScript. For instructions, see Table 29 on page 180 or Table 30 on page 183, as appropriate.

Running the tool

To run the tool, do the following:

1. Open a web browser to the environment checker tool:

`https://hostname:port/zosmf/IzuUICommon/environment.jsp`

where:

- *hostname* is the hostname or IP address of the system on which z/OSMF is installed
- *port* is the secure application port.

To find the hostname and port, see the link for z/OSMF in message IZUG349I. This message was written to the log file that was created when you ran the **izusetup.sh** script with the -finish option, as described in “Step 5: Complete the setup” on page 39. This log file is in the format:

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

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

2. Follow the instructions for your particular browser in the online help for the tool.

Understanding the results of the tool

Table 28 describes the layout of the environment checker report.

Table 28. Columns in the environment checker tool results page

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

Table 28. Columns in the environment checker tool results page (continued)

Column	Description
Settings as of <i>date-time</i>	<p>Findings from the most recent invocation of the tool. This column indicates potential problems with your browser.</p> <p>In the column heading, the date and time (<i>date-time</i>) is represented in ISO 8601 format, a standard provided by the International Organization for Standardization (ISO). In this format:</p> <ul style="list-style-type: none"> Calendar date is represented in year-month-day format (<i>yyyy-mm-dd</i>) . Time of day (<i>T</i>) is based on the 24-hour clock: <i>hh:mm:ss:mmm</i>. <i>Z</i> indicates zero offset from coordinated universal time (UTC). <p>In the report, the status of each setting is indicated, as follows:</p> <p>Items marked with a critical icon X Setting is not correct for z/OSMF. You must fix this problem before continuing with z/OSMF.</p> <p>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.</p> <p>No error indication Setting is correct for z/OSMF.</p>
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 55 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 2014-05-29T19:58:45.154Z	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	1344 by 840	Minimum screen resolution of 1024 by 768		
Browser Content Dimensions	1187 by 631	Minimum browser content dimensions of 800 by 600		
Browser Name and Version Browser User-Agent value	Firefox 24.0 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0	Supported browsers by operating system:		
		Browser	Microsoft Windows 7 Professional (32-bit)	Microsoft Windows 7 Professional (64-bit)
			Microsoft Windows 8, Pro, Enterprise (32-bit)	Microsoft Windows 8, Pro, Enterprise (64-bit)
		Firefox ESR 17.0.x	Yes	Yes
		Firefox ESR 24	Yes	Yes
		Internet Explorer 8 (32-bit)	Yes	No
		Internet Explorer 8 (64-bit) ¹	No	No
		Internet Explorer 9 (32-bit)	Yes	No
		Internet Explorer 9 (64-bit) ¹	No	No
		Internet Explorer 10 (32-bit)	Yes	Yes
		Internet Explorer 10 (64-bit) ²	No	Yes
		¹ Requires Microsoft Windows 7 Professional (64-bit).		
		² Requires Microsoft Windows 7 Professional (64-bit) or Microsoft Windows 8, Pro, Enterprise (64-bit).		
Operating System	Microsoft Windows 7	Microsoft Windows 7 Professional (32-bit and 64-bit) and Microsoft Windows 8, Pro, Enterprise (32-bit and 64-bit)		
Add-ons	No problem add-ons detected	The Firebug add-on can affect browser performance.		

Figure 55. 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 185.
- 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 185.
- 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 29 shows the recommended settings for the Mozilla Firefox browser.

Table 29. Recommended settings for Firefox

Environment Option	Response
JavaScript	<p>To work with z/OSMF, your browser must have JavaScript enabled.</p> <p>To enable JavaScript, do the following:</p> <ol style="list-style-type: none"> 1. From the <i>Tools</i> menu, click Options > Content tab. 2. Ensure that the JavaScript check box is selected. 3. Click OK.
Cookies	<p>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.</p> <p>To enable cookies for use by any site, do the following:</p> <ol style="list-style-type: none"> 1. From the <i>Tools</i> menu, click Options > Privacy tab. 2. Ensure that the Accept cookies from sites check box is selected. 3. Click OK. <p>To enable cookies for only the z/OSMF site, clear the Accept cookies from sites check box. Then, do the following:</p> <ol style="list-style-type: none"> 1. Click Exceptions. 2. Enter the URL for the z/OSMF site at your installation. 3. Click Enable > Close > OK.

Table 29. Recommended settings for Firefox (continued)

Environment Option	Response
Pop-up Windows	<p>For proper functioning with z/OSMF, your browser must be enabled for pop-up windows.</p> <p>To enable your browser for pop-up windows, do the following:</p> <ol style="list-style-type: none"> 1. From the <i>Tools</i> menu, click Options > Content tab. 2. Clear the Block pop-up windows check box. 3. Click OK. <p>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:</p> <ol style="list-style-type: none"> 1. Click Exceptions. 2. Enter the URL for the z/OSMF site at your installation. 3. Click Allow > Close > OK.
Frames	<p>To work with z/OSMF, your browser must have frames enabled. By default, the Firefox browser is enabled for frames.</p> <p>If you need to enable your browser for frames, do the following:</p> <ol style="list-style-type: none"> 1. In the browser input area, enter the following URL: <code>about:config</code>. 2. If a warranty warning message appears, click the I'll be careful, I promise! button to continue. 3. In the Filter field, enter <code>frames</code>. 4. Click <code>browser.frames.enabled</code> to set the Value field to <code>true</code>. 5. Close the browser to save the changes.
Screen Resolution	<p>For optimal viewing with z/OSMF, your workstation requires a minimum screen resolution of 1024 by 768 pixels.</p> <p>To increase the screen resolution, do the following:</p> <ol style="list-style-type: none"> 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.

Table 29. Recommended settings for Firefox (continued)

Environment Option	Response
Browser Content Dimensions	<p>For optimal viewing with z/OSMF, your browser requires a usable content display area of at least 800 by 600 pixels.</p> <p>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.</p> <p>To check the desktop appearance settings, do the following:</p> <ol style="list-style-type: none"> 1. Right-click on the desktop and select Properties to open the <i>Display Properties</i> 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. <p>To remove unnecessary toolbars, do the following:</p> <ol style="list-style-type: none"> 1. From the <i>View</i> menu in Firefox, click Toolbars. 2. For any unnecessary toolbars, clear the associated check box. <p>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.</p>
Add-ons	<p>For optimal performance with z/OSMF, disable the Firebug add-on in your browser settings.</p> <p>To disable the Firebug add-on, do the following:</p> <ol style="list-style-type: none"> 1. From the <i>Tools</i> 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.
Plug-ins	<p>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.</p> <p>In the environment checker report, the Settings column shows the installed plug-ins for your browser. To verify this list, do the following:</p> <ol style="list-style-type: none"> 1. In the browser input area, enter the following URL: <code>about:plugins</code>. 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. <p>To disable a plug-in, do the following:</p> <ol style="list-style-type: none"> 1. From the <i>Tools</i> 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 30 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 185.

Table 30. Recommended settings for Internet Explorer

Environment Option	Response
JavaScript	<p>To work with z/OSMF, your browser must have JavaScript enabled.</p> <p>To enable JavaScript, do the following:</p> <ol style="list-style-type: none">1. From the <i>Tools</i> menu, click Internet Options > Security tab.2. Click Custom Level.3. Scroll down to <i>Scripting</i>, then <i>Active Scripting</i>.4. Click Enable.5. Click OK > OK.
Cookies	<p>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.</p> <p>To enable cookies for use by any site, do the following:</p> <ol style="list-style-type: none">1. From the <i>Tools</i> menu, click Internet Options > Privacy tab.2. Click Advanced.3. Select the Override automatic cookie handling check box.4. Select Accept for <i>First-party Cookies</i> and <i>Third-party Cookies</i>.5. Click OK > OK. <p>To enable cookies for only the z/OSMF site, clear the Override automatic cookie handling check box and select Block for <i>First-party Cookies</i> and <i>Third-party Cookies</i>. Then, do the following:</p> <ol style="list-style-type: none">1. From the <i>Tools</i> 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	<p>For proper functioning with z/OSMF, your browser must be enabled for pop-up windows.</p> <p>To enable your browser for pop-up windows, do the following:</p> <ol style="list-style-type: none">1. From the <i>Tools</i> menu, click Internet Options > Privacy tab.2. Clear the Turn on Pop-up Blocker check box.3. Click OK. <p>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:</p> <ol style="list-style-type: none">1. Select Settings2. Enter the URL for the z/OSMF site at your installation.3. Click Add.4. Click Close > OK.

Table 30. Recommended settings for Internet Explorer (continued)

Environment Option	Response
Frames	<p>To work with z/OSMF, your browser must have frames enabled.</p> <p>To enable your browser for frames, do the following:</p> <ol style="list-style-type: none"> 1. From the <i>Tools</i> menu, click Internet Options > Security tab. 2. Click Custom Level. 3. Scroll down to <i>Miscellaneous</i>, then <i>Launching programs and files in an IFRAME</i>. 4. Click Enable. 5. Click OK.
Screen Resolution	<p>For optimal viewing with z/OSMF, your workstation requires a minimum screen resolution of 1024 by 768 pixels.</p> <p>To increase the screen resolution, do the following:</p> <ol style="list-style-type: none"> 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	<p>For optimal viewing with z/OSMF, your browser requires a usable content display area of at least 800 by 600 pixels.</p> <p>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.</p> <p>To check the desktop appearance settings, do the following:</p> <ol style="list-style-type: none"> 1. Right-click on the desktop and select Properties to open the <i>Display Properties</i> 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. <p>To remove unnecessary toolbars, do the following:</p> <ol style="list-style-type: none"> 1. From the <i>View</i> menu, click Toolbars. 2. For any unnecessary toolbars, clear the associated check box. <p>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.</p>
Add-ons	<p>For optimal performance with z/OSMF, it is recommended that you include only required add-ons with your browser.</p> <p>To disable an add-on, do the following:</p> <ol style="list-style-type: none"> 1. From the <i>Tools</i> 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 30. Recommended settings for Internet Explorer (continued)

Environment Option	Response
Plug-ins	<p>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.</p> <p>In the environment checker report, the Settings column shows the installed plug-ins for your browser. To verify this list, do the following:</p> <ol style="list-style-type: none"> 1. From the <i>Tools</i> 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 `IZUGn.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.zosmf.navigation.listener.Bootstrap|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 187.

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 IZUGn.log, where *n* is a numeral from 0 to 9.

z/OSMF creates log files in a "cascading" manner. The most current log file is always named IZUG0.log. When this log file reaches its predefined limit, z/OSMF saves it as IZUG1.log and begins writing to a new IZUG0.log file. When the IZUG0.log file is again full, z/OSMF saves it as IZUG1.log after renaming the existing IZUG1.log file to IZUG2.log. z/OSMF continues this process, saving each log file under the next available name, up to a maximum of ten log files. Thereafter, z/OSMF discards the oldest log file (IZUG9.log) whenever a new log file is to be created.

The z/OSMF runtime log files are written in English only, and are tagged as ASCII, using the ISO8859-1 code page. You can view the log files in ASCII format through ISPF option 3.17, using the VA action (View an ASCII file). Other viewing options, such as OBROWSE, or tools such as vi, emacs, or grep, might require that you first convert the files to EBCDIC. To have ASCII files converted to EBCDIC automatically prior to browsing, set the z/OS UNIX System Services environment variable _BPXK_AUTOCVT to "ON".

To work with the logs, you require 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 same operation. For the steps, see "Enabling tracing and logging for z/OSMF" on page 188.

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 190.

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 script 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 configuration file system, which is, by default /etc/zosmf. If a problem occurs with the configuration log file, the log data is written instead to the directory specified by \$TMPDIR, if this environment variable is set. Otherwise, the configuration log data is written to the /tmp directory.

Enabling tracing and logging for z/OSMF

For diagnostic purposes, you might be asked by IBM Support to enable tracing and logging for z/OSMF. You can configure the z/OSMF server to start in a trace-enabled state, or you can enable tracing and logging dynamically for the running server. The trace output is written to files in the z/OSMF logs directory.

Activating tracing and changing the level of logging are performed through the same operation.

This section contains the following topics:

- “Enabling tracing and logging at server start-up”
- “Enabling tracing and logging on a running server” on page 189.

Understand that tracing carries a performance cost. Do not activate tracing for z/OSMF unless directed to do so by IBM Support.

| Enabling tracing and logging at server start-up

| The z/OSMF server configuration settings are used to configure tracing and logging for z/OSMF. These settings, which are read when the server is started, determine the initial trace state for the server.

| If there is a problem with starting the server, you might be asked by IBM Support to configure the server to start in a trace-enabled state. If so, you are asked to add the appropriate trace specifications to the z/OSMF bootstrap.template file. Doing so ensures that the server is started with the proper traces enabled. z/OSMF writes the trace output to files in the z/OSMF logs directory.

| To start this type of tracing, do the following steps:

- | 1. Locate the z/OSMF bootstrap.template file. By default, the file resides at this location:
| /etc/zosmf/servers/zosmfServers/bootstrap.template.
- | 2. Save a copy of the existing bootstrap.template file as a back-up.
- | 3. Edit the bootstrap.template file, and locate the current trace settings. It looks similar to the following line:
| com.ibm.ws.logging.trace.specification=com.ibm.zosmf.*=info

- | 4. Modify the line to include the appropriate trace specifications. Ensure that each specification is separated by a colon (':').
| For the valid trace settings, see the following IBM technote for WebSphere Application Server V8.5 Liberty profile: <http://www.ibm.com/support/docview.wss?uid=swg21596714>.
| For example, to add tracing of all messages that are related to the z/OSMF configuration, modify the preceding line, as shown:
| `com.ibm.ws.logging.trace.specification=com.ibm.zosmf.*=info:com.ibm.ws.config.*=all`
 - | 5. Save the `bootstrap.template` file.
 - | 6. Restart the z/OSMF server and resume z/OSMF operations.
- | Your changes take effect immediately and are maintained across z/OSMF server restarts.
- | To work with the z/OSMF log files, you require a user ID with z/OSMF administrator authority (that is, a user ID defined to the z/OSMF administrator security group).

Enabling tracing and logging on a running server

You might be asked by IBM Support to enable tracing and logging for z/OSMF dynamically. If so, use the command `MODIFY` with the `LOGGING` option to set the appropriate tracing specification. To run this command, your user ID must be permitted to enter operator commands.

The command has the following syntax:

```
f server-name,logging='trace_specification'
```

where:

server-name

Is the server for your z/OSMF configuration. Set this value to the job name of the z/OSMF server, which is `IZUSVR1`, by default.

trace_specification

Is the level of tracing to be used. This value is provided by IBM Support. To reset the trace specification to the previous setting, specify `"reset"` as the trace specification.

Enter the command from the operator console. The command output is displayed in the operator console and in the z/OS system log.

Your changes take effect immediately and remain in effect while the server is running. Your changes are discarded when the server is restarted, and the previous settings are used. To have your changes be saved across server restarts, you must enable tracing and logging at server start-up, as described in “Enabling tracing and logging at server start-up” on page 188.

The following `MODIFY` command sets the trace specification to all:

```
f izusvr1,logging='*=warning:com.ibm.zosmf.util.data.*=all'
```

Figure 56 on page 190 shows an example of the command output.

```

00- SY1 f izusvr1,logging='*=warning:com.ibm.zosmf.util.data.*=all'
SY1 +CWVKB0005I: COMMAND RESPONSES COMPLETED SUCCESSFULLY FROM Logging
Command Handler.
SY1 +CWVKB0002I: MODIFY COMMAND
LOGGING='*=warning:com.ibm.zosmf.util.data.*=all' COMPLETED
SUCCESSFULLY.

```

Figure 56. Sample results from the MODIFY LOGGING operator command

The following MODIFY command resets the trace specification:

```
f izusvr1,logging='reset'
```

Figure 57 shows an example of the command output.

```

00- SY1 f izusvr1,logging='reset'
SY1 +CWVKB0005I: COMMAND RESPONSES COMPLETED SUCCESSFULLY FROM Logging
Command Handler.
SY1 +CWVKB0002I: MODIFY COMMAND LOGGING='reset' COMPLETED SUCCESSFULLY.

```

Figure 57. Sample results from the MODIFY LOGGING RESET operator command

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 58 shows portions of an example of z/OSMF server side log data.

```

2009-04-29T18:38:51.285Z|00000012|com.ibm.zosmf.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.zosmf.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.zosmf.util.eis.EisException.getEisException(EisException.java:145)
com.ibm.zosmf.util.eis.EisException.diagnoseAndThrow(EisException.java:221)
com.ibm.zosmf.util.eis.cim.ccp.CimClientPool.getWBEMClient(CimClientPool.java:279)

    0
    0
    0

+> 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)

    0
    0
    0

[tx000000000000000017:pegadm@IBM-FF0E8EC4FCB.xxx.yyy.com (GET) /zosmf/pdw/PdwServiceServlet/
Incidents?filters=IncidentTime(FROM1240704000000)&dojo.preventCache=1241030163470]

```

Figure 58. Portion of a z/OSMF server side log data

As shown in Figure 58, 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.zosmf.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 59.

```
[tx00000000000000ED5:debug2@9.10.83.13 (POST) /zosmf/IzuUICommon/UILoggerServlet?preventCache=1243956783360]
2009-06-02T15:37:51.933Z|0000001A|com.ibm.zosmf.util.log.servlet.UILoggerServlet|UILoggerServlet::doPost()
SEVERE: [2009-06-02T15:36:47.047Z] IZUG802E: An error occurred. Error: "makeTree error: Error: timeout exceeded"
[tx00000000000000ED8:debug2@9.10.83.13 (POST) /zosmf/IzuUICommon/UILoggerServlet?preventCache=1243956783360]
2009-06-02T15:37:52.020Z|0000001A|com.ibm.zosmf.util.log.servlet.UILoggerServlet|UILoggerServlet::doPost()
SEVERE: [2009-06-02T15:36:47.203Z] IZUG802E: An error occurred. Error: "makeTree error: Error: timeout exceeded"
[tx00000000000000ED9:debug2@9.10.83.13 (POST) /zosmf/IzuUICommon/UILoggerServlet?preventCache=1243956783360]
```

Figure 59. 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 identified by the Incident Log installation verification program (IVP)” on page 197
- “Problems when accessing the user interface” on page 204
- “Problems when using Configuration Assistant” on page 210
- “Problems when using the Incident Log task” on page 212
- “Problems when using the ISPF task” on page 210
- “Problems when attempting to send data” on page 213.

Problems during configuration

This topic provides troubleshooting tips for resolving problems related to the configuration and setup of z/OSMF.

Troubleshooting topics are included for the following problems and scenarios:

- “izusetup.sh script cannot locate CEA parmlib member”
- “izusetup.sh script cannot activate CEA parmlib member” on page 193
- “izusetup.sh script fails or CIM server abends” on page 194
- “izusetup.sh script fails when issuing an operator command, such as DUMP” on page 194
- “izusetup.sh script fails with an authorization failure for the z/OSMF installer” on page 194
- “izusetup.sh script fails with incomplete details in the log file” on page 195
- “izusetup.sh script fails because cimivp times out” on page 195
- “A z/OSMF script fails because no z/OS UNIX processes are available” on page 196
- “You receive message EDC5134I: Function not implemented” on page 196
- “RACDCERT or another RACF command abends during configuration” on page 197.

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 E, “Common event adapter (CEA) reason codes,” on page 297.

izusetup.sh script cannot locate CEA parmlib member

Symptom: The script `izusetup.sh -finish` fails with the following message:

IZUG207E: File <source parmlib>(CEAPRM00) does not exist.

Possible Causes: The script searches for the IBM-supplied member, CEAPRM00 in the source data set (*source parmlib*) that you specified earlier as input (see Chapter 7, “Adding plug-ins to a z/OSMF configuration,” on page 127). However, the source data set is:

1. Missing or is not cataloged
2. Missing the CEAPRM00 member

3. Protected through a RACF data set profile (for example, SYS1.*) and the issuer of the script (the installer user ID) is not permitted to the profile.

By default, the source data set is SYS1.PARMLIB.

Corrective Actions: Ensure that the parmlib data set:

1. Exists and is cataloged
2. Contains the IBM-supplied member CEAPRM00
3. If protected through a RACF data set profile, the z/OSMF installer user ID is permitted to the data set profile. To grant this permission, use the following command, where *USER-ID* is the user ID to be authorized to the data set profile SYS1.*:

```
PERMIT SYS1.* ID(USER-ID) ACCESS(READ)
```

izusetup.sh script cannot activate CEA parmlib member

Symptom: The script `izusetup.sh -finish` fails. The z/OSMF log contains messages like the following:

```
IZUG124I: The Common Event Adapter (CEA) parmlib member "CEAPRMWW" is
being activated. /u/pegasus/wbem/bin/cimcli CIMException:
Cmd= im Object= IBMzOS_PDW_IVP.ivp_id="IBMzOS_PDW_IVP"
CIM_ERR_FAILED: MODIFY CEA,CEA=WW

IEE538I CEAPRMWW MEMBER NOT FOUND IN PARMLIB

IZUG123E: An error occurred. The Common Event Adapter (CEA) parmlib member
was not activated.
```

Possible Cause: z/OSMF cannot activate the newly created CEAPRM_{nnn} parmlib member (by default, CEAPRM01). This error can occur if the configuration script copied the CEAPRM_{xx} member to a target parmlib data set that is not in your installation's parmlib concatenation. You specified the target parmlib data set earlier when you ran the script described in Chapter 7, “Adding plug-ins to a z/OSMF configuration,” on page 127. By default, this is data set SYS1.PARMLIB.

Corrective Action: To resolve the problem, copy the CEAPRM_{xx} member to your parmlib concatenation. Then, enter the following command to activate the new CEAPRM_{xx} member, where *xx* represents the member suffix:

```
MODIFY CEA,CEA=xx
```

To verify that the new CEAPRM_{xx} parmlib member is in effect, enter the MODIFY command, as follows:

```
MODIFY CEA,DISPLAY,PARMS
```

Ensure that the new member:

- Defines a high level qualifier for CEA, such as HLQ(CEA), and sets the SNAPSHOTS parameter to Y to allow CEA to create diagnostic snapshots of the system logs
- Sets the IBM branch and country code values for your installation
- Defines the storage value for parmlib (an SMS class or a string of volume names).

It is recommended that you edit your active IEASYS_{xx} parmlib member to identify the CEAPRM_{xx} parmlib member to use for the next IPL of the system. Specify the CEAPRM_{xx} member suffix on the CEA=*xx* statement of IEASYS_{xx}.

For more information about the CEAPRMxx parmlib member, see *z/OS MVS Initialization and Tuning Reference*.

izusetup.sh script fails or CIM server abends

Symptoms: The script `izusetup.sh -finish` fails. Or, the CIM server abends when attempting to use CEA.

Possible Cause: LIBPATH is not set up correctly

Corrective Action: Add the path in which the CEA DLLs are installed to LIBPATH. Usually, this is `/usr/lib`.

izusetup.sh script fails when issuing an operator command, such as DUMP

Symptom: The script `izusetup.sh -finish` fails. SYSLOG contains messages related to authorization errors.

Possible Cause: The z/OSMF installer user ID lacks OPERCMDS access.

Corrective Action: If your installation protects MVS commands with the RACF class OPERCMDS, you must grant the proper authority to the installer user ID.

- To grant DUMP command access to the z/OSMF installer user ID, enter the PERMIT command as follows. This authorization is required for the `izusetup.sh -verify` step to complete.

```
PERMIT MVS.DUMP CLASS(OPERCMDS) ID(USER-ID) ACCESS(CONTROL)
```

- To allow the z/OSMF installer to use all operator commands, enter the PERMIT command, as follows:

```
PERMIT MVS.** CLASS(OPERCMDS) ID(USER-ID) ACCESS(CONTROL)
```

- To grant the z/OSMF installer access to particular operator commands, enter the PERMIT command with one or more of the profiles shown in Table 31, as appropriate for your installation.

Table 31. Authorizing the z/OSMF installer user ID for operator commands

Resource profile	Access required
MVS.DISPLAY.LOGGER	READ
MVS.SETLOGR.LOGR	UPDATE
MVS.DISPLAY.SYMBOLS	ALTER
MVS.DISPLAY.XCF	READ
MVS.DUMP	CONTROL

izusetup.sh script fails with an authorization failure for the z/OSMF installer

Symptom: The script `izusetup.sh -finish` fails with an authorization failure message for the z/OSMF installer 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)
```

izusetup.sh script fails with incomplete details in the log file

Symptom: The script `izusetup.sh -finish` fails with the following message:

```
IZUG305E The script <script-name> failed with reason code nnn;  
see log file <log-file-path-and-name>.
```

In this message, the reason code `nnn` indicates that an internal script encountered an error while processing. On examining the indicated log file, `izusetup_finish<timestamp>.log`, you find little additional information about the error.

Corrective Action: For more information about this error, check the contents of `z/OSMF` server log file. This log file is located in the `z/OSMF` server logs directory. 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`

Depending on the source of the error, more information might be available in the reason code documentation for `z/OS UNIX System Services` or `Java`.

izusetup.sh script fails with "garbage characters" in the display or log file

Symptom: The script `izusetup.sh -finish` fails with message `IZUG295E` indicating that the verification process has failed. This message is accompanied by unrecognized or "garbage" characters written to the `z/OSMF` log, the user's screen, or both. Figure 60 shows an example:

```
AN_Ni0-(/N>-EE/EEAA-----ä?>ÄÄEN>Ä-È?-%?Ä/%-än(-eÄEIAE-----EIAÄÄEE---ä?I>Ä-ä? 0  
IEÄE-è-EEÄ ---(|+|è&-&ä-&|.-nä(-ä|(---ä&inä--- --ä-----<& e+/ Ä--ÿääè&-----ä?I>  
Ä-|øÄE/EN>Ä-è-EEÄ ---è&---ÿÄEEN?>-----è-Èø%ÄI--(|+|è&---äEÄÄ(Ä -----  
+I_ÄÄE-?Ä-/ÄE NIA-i+nî-è-EEÄ -eÄEINAAE-øE?ÄÄEEÄE-----+I_ÄÄE-?Ä-/ÄENIÄ-/ÄÄEÄEE-Èø/ÄÄ  
È-----+I_ÄÄE-?Ä-ää-ø?ÈÈÈ-----+I_ÄÄE-?Ä-?>%N>Ä-øE?ÄÄEE?ÈÈ- -ä&-----&-----:nn&---  
---+I_ÄÄE-?Ä-?>%N>Ä-ÄNE,-I?%I_ÄE-----AN_Ni0--- %%-EÄEEE-Ä?_ø%ÄEÄÄ-EIAÄÄEEÄI%`  
  
--IZUG295E: Verification proce ss "/usr/lpp/wbem/bin/cimivp" has failed.  
IZUG211E: Script "./izusetup.sh" encountered errors: exiting script.
```

Figure 60. Example of the "garbage characters" problem

Corrective Action: Verify that the `z/OSMF` installer's profile is properly set up for the `z/OS UNIX` shell environment. By default, the file `profile.add`, which is shipped with the CIM server, provides the environment variables that you need to define for the installer; see `/usr/lpp/wbem/install/profile.add`. If you are not using the defaults, you should modify the appropriate settings. Copy the contents of the `profile.add` file to the `.profile` file in the home directory of the `z/OSMF` installer user ID. The `.profile` file should be owned by the `z/OSMF` installer, and have read-write-execute access for the owner.

Then, run the `izusetup.sh -finish` script again.

izusetup.sh script fails because cimivp times out

Symptom: The script `izusetup.sh -finish` fails with a message indicating that the `cimivp` program has timed out.

Corrective Action: As part of its processing, the script `izusetup.sh -finish` runs the CIM installation verification program, `cimivp`. If the execution of `cimivp` times out, the problem might be a slow IP

hostname resolution or a large number of managed resources to be queried, such as logical disks. The default timeout for cimivp is two minutes. To override this default, you can export the following variable in your z/OS UNIX shell environment:

```
CIM_IVP_TIMEOUT=nnn
```

where *nnn* is the number of seconds that cimivp is to wait for a response from the CIM server before it fails with a timeout. For example, to set the cimivp timeout to five minutes, enter the following export command:

```
export CIM_IVP_TIMEOUT="300"
```

Then, run the **izusetup.sh -finish** script again.

For more information about the cimivp program, see *z/OS Common Information Model User's Guide*.

A z/OSMF script fails because no z/OS UNIX processes are available

Symptom: A script fails with a message indicating that no z/OS UNIX processes are available for the user ID that was used to run the script.

Possible Cause: The user ID 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 identified by the Incident Log installation verification program (IVP)

This topic provides troubleshooting tips for system setup problems identified by the Incident Log task installation verification program (IVP). Included are procedures and methods for performing problem determination and for troubleshooting the status of the different system components.

Using the installation verification program

The Incident Log task installation verification program (IVP) checks the z/OS system setup to determine actions that might have been missed during z/OSMF configuration.

About the installation verification program

The IVP checks for the following conditions, all of which are required for successful operation of the Incident Log task:

- CEA component is available
- System REXX component is available
- User is authorized for the Incident Log task resources associated with CEA and CIM
- Sysplex dump directory is available and accessible
- System REXX execs are available and operational
- System Logger is available
- Operations log (OPERLOG) and logrec snapshots are accessible
- Dump analysis and elimination (DAE) is active and its symptom data set is available.

“Updating z/OS for the Incident Log plug-in” on page 93 contains sections on how to perform each of these z/OS setup tasks manually.

Running the installation verification program

To run the Incident Log task IVP, your user ID must be permitted to enter operator commands. To add this authority, enter the RACF PERMIT command, as follows:

```
PERMIT MVS.** CLASS(OPERCMDS) ID(userid) ACCESS(CONTROL)
```

You can invoke the IVP program as a batch job using the following JCL:

```
//PDWIVP EXEC PGM=BPXBATCH,TIME=1440,REGION=0M,
//  PARM='PGM /usr/lpp/wbem/bin/cimcli ei IBMzOS_PDW_IVP -niq',
//      COND=(0,NE,CIMIVP)
//STDENV  DD  PATH='&ENVPATH/cimserver.env'
//STDOUT  DD  PATH='&RPTFILE',
//      PATHOPTS=(OAPPEND),
//      PATHMODE=(SIRUSR,SIWUSR,SIRGRP)
//STDERR  DD  PATH='&EFILE',
//      PATHOPTS=(OAPPEND),
//      PATHMODE=(SIRUSR,SIWUSR,SIRGRP)
//CEEDUMP DD  SYSOUT=*
//SYSPRINT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
//SYSMDUMP DD  SYSOUT=*
```

Figure 61. Invoking the Incident Log task IVP as a batch job

Reviewing the results of the `izuincidentlogverify.report` file

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

<IZU_LOGFILE_DIR>/izuincidentlogverify.report

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

To verify the configuration of the Incident Log task, z/OSMF creates a test SVC dump on the system and performs a series of tests on the dump. For each test, the **izuincidentlogverify.report** file shows either SUCCESS or an error message. Each error message corresponds to a possible cause and one or more corrective actions for the problems described by this report.

For your reference, the format of the IVP report is shown in Appendix G, “Format of the installation verification program report,” on page 325.

For information about the errors and corrective actions you can take, see “Problems identified by the Incident Log installation verification program (IVP)” on page 197. Table 32 summarizes the potential problems and the recommended corrective actions.

Table 32. Responding to system setup errors indicated in the `izuincidentlogverify.report` file

Problem indicated by the IVP	Corrective action
CEA address space is not running.	Start the CEA address space; see “Ensure that common event adapter (CEA) is configured and active” on page 107.
System REXX address space is not running.	Start the System REXX address space; see “Ensuring that System REXX is set up and active” on page 109.
User is not authorized.	Authorize the user to the indicated security class <i>profile-class</i> ; see “User is not authorized” on page 200
Unable to locate an incident in the sysplex dump directory.	Check the sysplex dump directory setup; see “Unable to locate an incident in the sysplex dump directory” on page 200.
Unable to open the sysplex dump directory.	Check the sysplex dump directory setup; see “Unable to open the sysplex dump directory” on page 201.
Another resource is using the sysplex dump directory.	Check the sysplex dump directory usage; see “Another resource is using the sysplex dump directory” on page 201.

Table 32. Responding to system setup errors indicated in the *izuincidentlogverify.report* file (continued)

Problem indicated by the IVP	Corrective action
Unable to generate the prepared data set.	Verify that the System REXX exec library is accessible, the SYSREXX address space is active, and that the compiled REXX exec CEACDMPP exists and is accessible to System REXX. See “Ensuring that System REXX is set up and active” on page 109.
User is not SAF authorized.	Grant the user the system authority to view the log files; see “User is not SAF authorized” on page 202.
System logger is not available.	Check the system logger setup; see “System logger not available” on page 202.
Unable to find the active DAE data set name.	Check the dump analysis and elimination (DAE) setup; see “Configuring dump analysis and elimination” on page 104.
System REXX environment cannot process the request.	Ensure that runtime support for compiled REXX is set up properly; see “System REXX cannot process the request” on page 202.
Unable to allocate the prepared data set to be tersed.	The function that prepares the incident materials to be sent through FTP could not allocate the data set to be tersed; see “Unable to allocate the prepared data set to be tersed” on page 202.
Unable to find the OPERLOG snapshot.	Check the system logger setup for the operations log (OPERLOG); see “Unable to find the OPERLOG snapshot” on page 203.
Sysplex dump directory has no space allocated.	Allow more space for incidents; see “Sysplex dump directory has no space allocated” on page 203.
No diagnostic data available.	Specify a larger time interval for error log snapshots; see “No diagnostic data available” on page 203.
Unable to allocate new data set.	When preparing incident materials to be sent through FTP, z/OSMF could not allocate a new data set to contain the tersed diagnostic snapshot. See “Unable to allocate new data set” on page 203.
Internal error encountered. CEA return code: <i>return-code</i> CEA reason code: <i>reason-code</i>	Look for system messages indicating why the failure occurred in the CIM trace associated with the failed return code; see “Internal error encountered. CEA return code: CEA reason code:” on page 204.

Resolving problems identified by the installation verification program

This topic provides corrective actions for system setup problems identified by the Incident Log task installation verification program (IVP).

Troubleshooting topics are included for the following problems and scenarios:

- “CEA address space is not running” on page 200
- “System REXX address space is not running” on page 200
- “User is not authorized” on page 200
- “Unable to locate an incident in the sysplex dump directory” on page 200
- “Unable to open the sysplex dump directory” on page 201
- “Another resource is using the sysplex dump directory” on page 201
- “Unable to generate prepared data set” on page 202
- “User is not SAF authorized” on page 202
- “System logger not available” on page 202
- “Unable to find the active DAE data set name” on page 202
- “System REXX cannot process the request” on page 202
- “Unable to allocate the prepared data set to be tersed” on page 202
- “Unable to find the OPERLOG snapshot” on page 203
- “Sysplex dump directory has no space allocated” on page 203

- “No diagnostic data available” on page 203
- “Unable to allocate new data set” on page 203
- “Internal error encountered. CEA return code: CEA reason code:” on page 204

CEA address space is not running

Possible Cause: The common event adapter (CEA) address space is not active.

Corrective Action: Start the CEA address space. For information, see “Ensure that common event adapter (CEA) is configured and active” on page 107.

System REXX address space is not running

Possible Cause: The System REXX address space (AXR) is not active.

Corrective Action: Start the System REXX address space. For information, see “Ensuring that System REXX is set up and active” on page 109

User is not authorized

Possible Cause: Most likely, a problem occurred when running the script to define a z/OSMF user.

Corrective Action: Authorize the user to the indicated security class *profile-class*. Check the `izuauthuser.sh` script, which is used to authorize the user; see “Creating the commands to authorize a user ID” on page 131. Ensure that the user has the appropriate permission to the CEA classes required for using the Incident Log task; see Table 45 on page 278.

Unable to locate an incident in the sysplex dump directory

Possible Cause: IPCS could not locate the sysplex dump directory data set. The dump directory is a shared VSAM data set with a default name of SYS1.DDIR. The installation can rename the data set and communicate that name through the BLSCUSER parmlib member.

Corrective Action: Check the sysplex dump directory setup:

1. Try locating the sysplex dump directory through ISPF 3.4
2. Verify that the name of the sysplex dump directory is the same as specified in the BLSCUSER member
3. Try rerunning BLSCDDIR to create the SYS1.DDIR data set.
4. Run a job to check the contents of the sysplex dump directory.

Figure 62 on page 201 shows an example of a job that you can use to create an IPCS report of the contents of the sysplex dump directory.

```
//IPCSJOB JOB 'D10.JOBS','IPCSU1 OUTPUT',MSGLEVEL=(1,1),
//          MSGCLASS=A,CLASS=J
//* -----
//*
//* INPUT: DUMP DIRECTORY IN DATA SET 'SYS1.DDIR'
//* OUTPUT:
//*   - IPCS DUMP DIRECTORY DATA SET FOR THE INPUT DUMP
//*     (IPCSDDIR DD)
//*   - FORMATTED OUTPUT (SYSTSPRT DD)
//*   - TSO/E MESSAGES (SYSTSPRT DD)
//* -----
//IPCS      EXEC PGM=IKJEFT01,DYNAMNBR=20,REGION=1500K
//IPCSDDIR DD DSN=SYS1.DDIR,DISP=(SHR)
//SYSTSPRT DD SYSOUT=*
//IPCSPRNT DD SYSOUT=*
//SYSTSIN  DD *
IPCS
LISTDUMP SYMPTOMS
END
```

Figure 62. Checking the sysplex dump directory—sample job for creating an IPCS report

Unable to open the sysplex dump directory

Possible Causes include the following:

- Data set not found. The volume is offline or otherwise unavailable.
- Abend occurred during processing. The data set has I/O errors.

Corrective Action: Check the sysplex dump directory setup:

1. Verify that the data set is available. It might be allocated by DUMPSRV.
2. An IPCS user has allocated the sysplex dump directory.
3. The z/OSMF user was not authorized to access the sysplex dump directory.
4. If you renamed the sysplex dump directory to be a name other than SYS1.DDIR, update BLSCUSER with the new name, as described in “Establishing a larger sysplex dump directory” on page 106.
5. Check SYSLOG and OPERLOG for messages about the sysplex dump directory data set or volume.

For more information, see “Creating the sysplex dump directory” on page 105.

Another resource is using the sysplex dump directory

Possible Cause: Another program is accessing the sysplex dump directory (by default SYS1.DDIR) exclusively and must free it. Programs that obtain exclusive (ENQ) access to the data set include DUMPSRV post-dump processing and common event adapter (CEA) when using IPCS service routines.

Corrective Actions: Check the sysplex dump directory usage:

1. Enter the **D GRS** command and check for contention on the sysplex dump directory data set.
2. If an IPCS user is holding the ENQ exclusively, consider cancelling that user's TSO session.
3. If CEA is holding the ENQ exclusively, enter the following command to end the CEA usage of the directory data set: **MODIFY CEA,DROIPCS**
4. Try the request again later.

For more information, see “Creating the sysplex dump directory” on page 105.

Unable to generate prepared data set

Possible Cause: There was a SYSREXX processing failure when preparing diagnostic data to send through FTP. Or, the prepare request failed because the logrec data set is empty (CEA reason code 378).

Corrective Action: Verify that the System REXX exec library is accessible and the SYSREXX address space is active. Verify that the compiled REXX exec CEACDMPP exists and is accessible to System REXX. See “Ensuring that System REXX is set up and active” on page 109.

User is not SAF authorized

Possible Cause: The user is not authorized to view information about the OPERLOG snapshot. The name of the data set (snapshot) appears in the buffer returned with the message.

Corrective Action: The security administrator must authorize the user of the service to the high level qualifier of this data set, which is specified in the CEAPRMxx parmlib member.

System logger not available

Possible Cause: The CEA component cannot access the OPERLOG or logrec snapshot log stream when preparing incident data to be sent.

Corrective Action: Enter the **D LOGGER** command and verify that system logger is active. For information about system logger and the log streams, see:

- “Defining a couple data set for system logger” on page 96
- “Enabling the operations log (OPERLOG)” on page 98
- “Defining and activating the LOGREC log stream” on page 100.

Unable to find the active DAE data set name

Possible Cause: Dump analysis and elimination (DAE) is not active.

Corrective Action: Check the DAE setup. For information, see “Configuring dump analysis and elimination” on page 104.

System REXX cannot process the request

Possible Cause: The System REXX environment cannot process an exec. This problem usually indicates that the runtime support for compiled REXX has not been set up.

Corrective Action: The REXX library or the REXX Alternate library data set must be added to the LINKLIST concatenation or LPA. For more information, see *IBM Compiler and Library for REXX on System z: User's Guide and Reference*, SH19-8160.

Unable to allocate the prepared data set to be tersed

Possible Cause: When preparing the dump or a log snapshot data set to be sent through FTP, the resulting data set is allocated and processed by the AMATERSE program. The dynamic allocation failed.

Corrective Action: Check message CEZ0500E for the dynamic allocation messages. For more information about these situations, see *z/OS MVS System Messages*.

Unable to find the OPERLOG snapshot

Possible Cause: The OPERLOG snapshot was not created. When accessing the OPERLOG snapshots, the system logger service IXGCONN received a bad return or reason code, indicating that the OPERLOG snapshot does not exist. It is possible that system logger is not active.

Corrective Action: Check the system logger setup:

1. Verify that the user has authorization to the OPERLOG DASD log stream.
2. Enter the **DISPLAY LOGGER, LOGSTREAM** command and verify the name of the OPERLOG snapshots (defined when configuring the DASD log streams).

For more information, see “Enabling the operations log (OPERLOG)” on page 98.

Sysplex dump directory has no space allocated

Possible Cause: The sysplex dump directory (SYS1.DDIR) has no space available to record new SVC dumps.

Corrective Action: Increase the size of the sysplex dump directory by doing one or both of the following:

1. Delete unneeded incidents from z/OSMF
2. Create a larger sysplex dump directory and copying the contents of the older data to the new directory data set. For more information, see “Establishing a larger sysplex dump directory” on page 106.

No diagnostic data available

Possible Cause: When preparing incident materials to be sent through FTP, z/OSMF could not allocate a new data set to contain the tersed diagnostic snapshot.

Corrective Action: Look for system messages indicating why the failure occurred in the CIM trace associated with the failed return code. For assistance, contact IBM Support.

Unable to allocate new data set

Possible Cause: The error log did not accumulate any data within the time interval specified in the CEAPRMxx member.

Corrective Action: To specify a larger time interval for error log snapshots, modify the CEAPRMxx member statements as shown in Figure 63 on page 204.

Notes:

1. The maximum time interval for a logrec summary is four hours.
2. During processing, the IVP creates a test SVC dump on the system. The test dump is not an ABEND type of incident, and therefore might not post any data in the error log. If this is the only problem reported by the IVP, you can ignore this problem.

```
DUMPCAPTURETIME
(
SLIP(OPERLOG(01:00:00) LOGREC(01:00:00)
LOGRECSUMMARY(04:00:00))
DUMP(OPERLOG(01:00:00) LOGREC(01:00:00)
LOGRECSUMMARY(04:00:00))
ABEND(OPERLOG(01:00:00) LOGREC(01:00:00)
LOGRECSUMMARY(04:00:00))
)
```

Figure 63. Specifying a larger time interval for error log snapshots

Internal error encountered. CEA return code: CEA reason code:

Possible Cause: An internal error occurred.

Corrective Action: Look for system messages indicating why the failure occurred in the CIM trace associated with the failed return code. See “CEA reason codes for the Incident Log task” on page 297. For assistance, contact IBM Support.

Problems when accessing the user interface

This topic provides troubleshooting tips for resolving problems related to the user interface of z/OSMF.

Troubleshooting topics are included for the following problems and scenarios:

- “Browser cannot connect to z/OSMF”
- “Missing initialization message or JSP processing error when attempting to use z/OSMF” on page 205
- “Certificate error in the Mozilla Firefox browser” on page 205
- “Cannot log into z/OSMF” on page 207
- “Re-authenticating in z/OSMF” on page 208
- “Message or help information is not available” on page 209
- “Action or link that was previously provided is not available” on page 209
- “A script takes too long to run or is not responding” on page 210.

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 144.

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/V2R1/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/V2R1/lib  
ls: FSUM6785 File or directory "/usr/lpp/zosmf/V2R1/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” on page 206
- “Importing the CA certificate into the browser” on page 206.

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 207. 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 64 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 64. 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.

5. Ensure that the appropriate script has been run for the user ID; see Chapter 8, “Authorizing users to z/OSMF,” on page 131.

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 490 minutes from the time you log into z/OSMF. Your installation can choose to modify this setting (the `ltpatimeout` setting) during the configuration of z/OSMF. For more details, see Appendix D, “Modifying the advanced settings for the z/OSMF configuration,” on page 293.

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. The z/OSMF help files must reside at the location:

`<IZU_CONFIG_DIR>/helps/eclipse/plugins`

where `<IZU_CONFIG_DIR>` is the z/OSMF configuration directory (by default, `/etc/zosmf`).

System programmer response

Use the following procedure to resolve this error:

1. Verify that symlinks exist in the `/etc/zosmf/helps/eclipse/plugins` subdirectory. The symlinks should refer to the z/OSMF product file system (configuration variable `IZU_CODE_ROOT`).
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” on page 211

- “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.”

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 213
- “CEA cannot allocate a data set for dump prepare or snapshot” on page 213
- “Diagnostic log streams and other incident data for deleted incidents are not being deleted over time” on page 213
- “Problems when attempting to send data” on page 213.

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 z/OS system console command `F CEA,DROIPCS` to disconnect CEA from the IPCS sysplex dump directory data set.

CEA cannot allocate a data set for dump prepare or snapshot

Possible Cause: CEA alias is not cataloged properly.

Corrective Action: If your installation has a user catalog setup instead of using the MASTER catalog, you might need to define the CEA alias to the user catalog. For example:

```
DEFINE ALIAS(NAME(CEA) RELATE(YOUR_CATALOG_NAME))
```

Diagnostic log streams and other incident data for deleted incidents are not being deleted over time

Possible Cause: If you modified the HLQ parameter value in the CEAPRMxx parmlib member, CEA no longer detects the previously-stored diagnostic data files stored under the old high level qualifier.

Corrective Action: Carefully remove the data manually. The data exists in both log stream and data set format. Use caution as to not remove any needed data. Remove data sets and log streams manually. To list the available log streams, enter the following z/OS system console command: `D LOGGER,L`.

Most log streams with the status of AVAILABLE are the result of diagnostic snapshots taken at the time of the dump. The old high level qualifier appears in the log streams that were created earlier by CEA. To delete log streams, enter the following command: `SETLOGR FORCE,DELETE,LSN=logstreamname`.

To remove data sets, do the following:

- List the data sets having the same HLQ as the available log streams.
- Delete the data sets.

Problems when attempting to send data

When you invoke the Send Diagnostic Data wizard from the Incident Log task, the information supplied in the page is used to produce one FTP job for each diagnostic data file being sent. Thus, if an incident has a dump data set and three log snapshot files, four FTP jobs are created (and the FTP Job Status table will have four entries). To debug the FTP jobs, you need access to the job output. 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 18. 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 186.

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:

<i>action</i>	The action being performed on the procedure. This can be the start or completion of the procedure.
---------------	--

<i>procedure-name</i>	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 <i>branch-country-name</i> code must be <i>branch-country-range</i> 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.

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 occurred.

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 specified 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:** *rexex-exec-name1*, *rexex-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:

rexex-exec-name1
Name of the first generated RACF exec.

rex-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 evaluated.

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 Incident 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 Incident 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 occurred. 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:

- 04.01.00 indicates V2R1 for the product (z/OS or z/OSMF)
- 03.23.00 indicates V1R13 for the product (z/OS or z/OSMF)
- 03.22.00 indicates V1R12 for the product (z/OS or z/OSMF).

Thus, for example, the value 04.01.00 indicates V2R1 of the product (z/OS or z/OSMF).

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:

- 04.01.00 indicates V2R1 for the product (z/OS or z/OSMF)
- 03.23.00 indicates V1R13 for the product (z/OS or z/OSMF)
- 03.22.00 indicates V1R12 for the product (z/OS or z/OSMF).

Thus, for example, the value 04.01.00 indicates V2R1 of the product (z/OS or z/OSMF).

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-UUID*, or enter the keyword AUTOUID:

Explanation: The message prompts you to input unauthenticated guest user UID in z/OSMF.

In the message text:

unauthenticated-UUID
unauthenticated user UID.

System programmer response: Enter a valid value.

User response: No action is required.

IZUG334I Enter the z/OSMF Unauthenticated *unauthenticated-UUID*, or enter the keyword AUTOUID, or press Enter to accept the default *default-unauthenticated-UUID*:

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-UUID
unauthenticated guest user UID.

default-unauthenticated-UUID
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 *plugin-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 to 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 IZUGn.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

Appendix A. Security configuration requirements for z/OSMF

You can use the generated REXX exec, **izuconfig1.cfg.rexx**, to create a base set of 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 **izuconfig1.cfg.rexx** program. 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 268
- “User IDs that z/OSMF creates during configuration” on page 269
- “Security groups that z/OSMF creates during configuration” on page 269
- “Resource authorizations for the z/OSMF core functions” on page 270
- “Resource authorizations for hardware cryptography” on page 274
- “Resource authorizations for Common Information Model” on page 275
- “Resource authorizations for Provisioning Manager” on page 275
- “Resource authorizations for common event adapter (CEA)” on page 276
- “Resource authorizations for the z/OS jobs REST interface” on page 277
- “Resource authorizations for Workload Management” on page 278
- “Resource authorizations for the z/OSMF optional plug-ins” on page 278
- “Default profiles, resource names, and group assignments” on page 282.

Class activations that z/OSMF requires

For a RACF installation, the security classes shown in Table 33 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 generated REXX exec, **izuconfig1.cfg.rexx**. To have the commands issued when the exec runs, uncomment the sections. Or, ask your security administrator to enter the commands directly, as shown in Table 33.

Table 33. 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 26.	SETOPTS 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).	SETOPTS CLASSACT(APPL) SETOPTS RACLIST(APPL) GENERIC(APPL)
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.	SETOPTS CLASSACT(EJBROLE) SETOPTS RACLIST(EJBROLE) GENERIC(EJBROLE)

Table 33. Class activations that z/OSMF requires (continued)

Class	Purpose	RACF commands for activating
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: <ul style="list-style-type: none"> • 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 26.	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 installation specifies a system authorization facility (SAF) profile prefix to be used for naming z/OSMF resources. z/OSMF stores this value as configuration variable IZU_SAF_PROFILE_PREFIX.

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 generated REXX exec programs. In the examples in this document, the SAF prefix is shown as *<SAF-prefix>*. By default, the SAF prefix is IZUFLT. If your installation selects to use a different value, substitute the value in the examples.

User IDs that z/OSMF creates during configuration

The generated REXX exec, **izuconfig1.cfg.rexx**, creates a set of product user IDs; see Table 34.

Table 34. 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	izuconfig1.cfg.rexx
IZUSVR	User ID for the z/OSMF started tasks, which are named IZUANG1 and IZUSVR1, by default.	9010	izuconfig1.cfg.rexx

Table 34 shows the IBM default values. If you specify different user IDs during the configuration process, the generated exec uses your specified values in place of the IBM default values.

Security groups that z/OSMF creates during configuration

The generated REXX exec, **izuconfig1.cfg.rexx**, 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 35 lists the groups that **izuconfig1.cfg.rexx** creates. Note that the group names can change, based on the values you provide during the configuration process. Table 35 shows the IBM default values.

Table 35. 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	izuconfig1.cfg.rexx
IZUUSER	Security group for the z/OSMF user role.	9004	izuconfig1.cfg.rexx
IZUSECAD	Security group for the z/OS security administrator role in z/OSMF.	9006	izuconfig1.cfg.rexx
IZUUNGRP	Security group for the z/OSMF unauthenticated user ID.	9012	izuconfig1.cfg.rexx

Resource authorizations for the z/OSMF core functions

Table 36 describes the access requirements for the z/OSMF core functions. The generated REXX exec program, **izuconfig1.cfg.rexx**, 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 36 shows the IBM default values.

Table 36. 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 26.
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 274.
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.

Table 36. Security setup requirements for z/OSMF core functions (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
EJBROLE	<SAF-prefix>.IzuManagementFacilityImportUtility.izuUsers	IZUADMIN IZUSER	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.
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 IZUSER	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.

Table 36. Security setup requirements for z/OSMF core functions (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
SERVER	BBG.SECFPFX.<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.
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 26.
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.

Table 36. 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.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.
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.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 <i>View</i> function.
ZMFAPLA	<SAF-prefix>.ZOSMF.SETTINGS.FTP_SERVERS.MODIFY	IZUADMIN	READ	Allow a user to access the z/OSMF Task Settings task <i>Modify</i> 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 <i>View</i> function.
ZMFAPLA	<SAF-prefix>.ZOSMF.SETTINGS.SYSTEMS.MODIFY	IZUADMIN	READ	Allow a user to access the z/OSMF Task Settings task <i>Modify</i> function.
ZMFAPLA	<SAF-prefix>.ZOSMF.WORKFLOW.WORKFLOWS	IZUADMIN IZUSECAD IZUUSER	READ	Allow a user to access the z/OSMF Workflows task. See Table Note 5.

Table Notes:

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 14, “Adding links to z/OSMF through the `izusetup.sh` script,” on page 167.
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 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. Table 37 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 generated REXX exec, `izuconfig1.cfg.rexx`. To have the commands issued when the exec runs, uncomment the sections.

Table 37. 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.
CSFSERV	CSFKTB	IZUSVR	READ	Key token build 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 13, “Configuring your system for asynchronous job notifications,” on page 157.

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 “Ensure that the administrator role is authorized to the CIM server” on page 89.

During the configuration process, you must supply the names of the security groups that your installation has created for authorizing users to the CIM resources on your system. The RACF commands contained in the generated z/OSMF REXX programs contain commands for connecting users to the groups and thus, depend on the groups to exist.

Table 38 lists the CIM security groups that are required for the optional plug-ins.

Table 38. 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.

During the configuration process, your installation might need to 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 RACF commands contained in the generated z/OSMF REXX programs contain commands for connecting users to these groups and thus depend on the CIM groups to exist.

Resource authorizations for 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 39 lists the default values for the Provisioning Manager. Note that your installation might have selected to use different values for these settings.

Table 39. 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

During the configuration process, you must supply the names of the security groups that your installation has created for authorizing users to the Provisioning Manager on your system. The RACF commands contained in the generated z/OSMF REXX programs contain commands for connecting users to the groups and thus, depend on the groups to exist.

Table 40 lists the security groups that are required for the Capacity Provisioning plug-in.

Table 40. 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 <i>Edit</i> function.	None; your installation must specify a GID for this group.	Member CPOSEC1 in SYS1.SAMPLIB.
CPOQUERY	Security group for users of the Capacity Provisioning task <i>View</i> 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 generated REXX exec, izuconfig1.cfg.rexx, 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 41 on page 277 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 41. 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 26.
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 26.

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 42 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 42. 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 43.

Table 43. 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

Table 43. JESJOBS class authorizations needed for performing job modify operations (continued)

Operation	JESJOBS resource	Access required
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.

During the configuration process, you must 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 RACF commands contained in the generated z/OSMF REXX programs contain commands for connecting users to the group and thus, depend on the group to exist.

Table 44 describes the security group that is required for the Workload Management plug-in.

Table 44. 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 45 describes the security requirements that are required for the z/OSMF optional plug-ins. The generated REXX exec program, **izuconfig1.cfg.rexx**, includes sample RACF commands for creating these authorizations.

Note that these values can change, based on the values you provide. The values in Table 45 are based on the defaults. If your installation uses a different value, such as a different group name, the generated values can change.

Table 45. Security setup requirements for the z/OSMF optional plug-ins

Resource class	Resource name	Who needs access?	Type of access required	Why

Table 45. Security setup requirements for the z/OSMF optional plug-ins (continued)

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.VIEW	IZUADMIN IZUUSER	READ	Allow a user to access the Capacity Provisioning <i>View</i> function.
ZMFAPLA	<SAF-prefix>.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT.DOMAIN	IZUADMIN	READ	Allow a user to use the Capacity Provisioning task <i>Edit</i> 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 <i>Edit</i> function to edit a Capacity Provisioning policy.
Configuration Assistant. The following access controls must be set for the Configuration Assistant plug-in.				
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	<i>your_master_catalog</i>	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.

Table 45. Security setup requirements for the z/OSMF optional plug-ins (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
JESSPOOL	<i>your_system_name</i> .+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 IVP program to issue operator commands to accomplish its function.
SERVAUTH	CEA.CEADOCMD	IZUADMIN IZUUSER	READ	Allow a user to cancel the FTP job.
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.CEDELETEINCIDENT	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.

Table 45. 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.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.				
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 <i>objectType</i> and <i>objectSuffix</i> , see “Creating access controls for the Software Management task” on page 115.	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 <i>Product Information File Retrieve</i> function.
Workload Management. The following access controls must be set for the Workload Management plug-in. For additional authorizations, see Table Note 1.				

Table 45. 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>.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 <i>View</i> function.
ZMFAPLA	<SAF-prefix>.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.MODIFY	IZUADMIN	READ	Allow a user to access the Workload Management <i>Modify</i> function.
ZMFAPLA	<SAF-prefix>.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.INSTALL	IZUADMIN	READ	Allow a user to access the Workload Management <i>Install</i> 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 275.
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 276.

Default profiles, resource names, and group assignments

For your reference, Table 46 on page 283 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 46 on page 283. By default, the prefix is IZUFLT.

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 46. 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 IZUSER
<SAF-prefix> ZOSMF:CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT	ZOSMF:CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT	Capacity Provisioning Edit function	IZUADMIN
<SAF-prefix> ZOSMF:CONFIGURATION_ASSISTANT.ASSISTANT	ZOSMF:CONFIGURATION_ASSISTANT.CONFIGURATION_ASSISTANT	Configuration Assistant task	IZUADMIN IZUSER
<SAF-prefix> ZOSMF:SOFTWARE_DEPLOYMENT	ZOSMF:SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT	Software Management task	IZUADMIN IZUSER
<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 115.	Software Management task objects	IZUADMIN IZUSER
<SAF-prefix> ZOSMF:SOFTWARE_DEPLOYMENT.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 IZUSER
<SAF-prefix> ZOSMF:ISPF	ZOSMF:ISPF.ISPF	ISPF task	IZUADMIN IZUSER
<SAF-prefix> ZOSMF:RESOURCE_MONITORING	ZOSMF:RESOURCE_MONITORING.PERFDESKS	Resource Monitoring task	IZUADMIN IZUSER
<SAF-prefix> ZOSMF:RESOURCE_MONITORING	ZOSMF:RESOURCE_MONITORING.OVERVIEW	System Status task	IZUADMIN IZUSER
<SAF-prefix> ZOSMF:WORKLOAD_MANAGEMENT.VIEW	ZOSMF:WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.VIEW	Workload Management View function	IZUADMIN IZUSER
<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 <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 14, "Adding links to z/OSMF through the izusetup.sh script," on page 167.	Links task	IZUADMIN IZUSER
<SAF-prefix> ZOSMF:ADMINTASKS	ZOSMF:ADMINTASKS.APPLINKING ZOSMF:ADMINTASKS.LINKTASK ZOSMF:ADMINTASKS.LOGGER ZOSMF:ADMINTASKS.UI_LOG_MANAGEMENT	Links task	IZUADMIN IZUSER
<SAF-prefix> ZOSMF:ADMINTASKS	ZOSMF:ADMINTASKS.APPLINKING ZOSMF:ADMINTASKS.LINKTASK ZOSMF:ADMINTASKS.LOGGER ZOSMF:ADMINTASKS.UI_LOG_MANAGEMENT	z/OSMF Administration tasks	IZUADMIN

Table 46. 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 IZUSER
	ZOSMF.SETTINGS.FTP_SERVERS.VIEW	z/OSMF Settings FTP Servers <i>View</i> function	IZUADMIN IZUSER
	ZOSMF.SETTINGS.FTP_SERVERS.MODIFY	z/OSMF Settings FTP Servers <i>Modify</i> function	IZUADMIN
<SAF-prefix> ZOSMF.SETTINGS.SYSTEMS*	ZOSMF.SETTINGS.SYSTEMS	z/OSMF Settings Systems task	IZUADMIN IZUSER
	ZOSMF.SETTINGS.SYSTEMS.VIEW	z/OSMF Settings Systems <i>View</i> function	IZUADMIN IZUSER
	ZOSMF.SETTINGS.SYSTEMS.MODIFY	z/OSMF Settings Systems <i>Modify</i> function	IZUADMIN
<SAF-prefix> ZOSMF.WORKFLOW.*	ZOSMF.WORKFLOW.WORKFLOWS	Workflows task.	IZUADMIN IZUSECAD IZUSER

Appendix B. izusetup.sh script

z/OSMF provides a front end interactive script, called **izusetup.sh**, that you can use to create a z/OSMF configuration on your z/OS system. After the configuration is created, you can use this script to modify the configuration, for example, by adding optional plug-ins and links.

Function

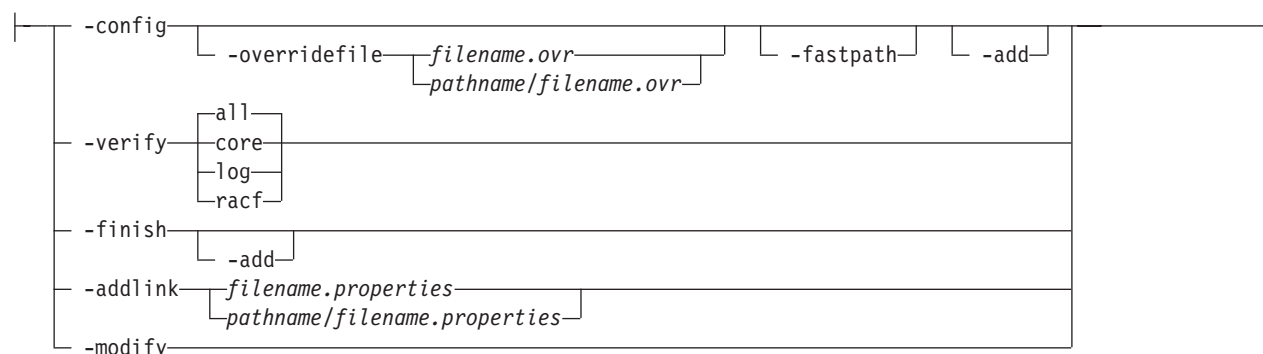
The **izusetup.sh** script provides a number of options for creating and modifying a z/OSMF configuration.

You can run this script from an OMVS or telnet/rlogin session. You cannot run this script from ISHELL.

Syntax

►► izusetup.sh — -file filename.cfg | pathname/filename.cfg | Options | ►►

Options:



Required parameters

Always include the -file parameter, which specifies the name of the configuration file that the **izusetup.sh** script is to use as input.

You must also specify one of the following parameters, which identify the particular operation that the **izusetup.sh** script is to perform. You cannot specify more than one of these operations on the same invocation.

-config

This parameter begins the z/OSMF configuration process. The script performs a number of actions to create a new z/OSMF configuration, such as creating a REXX exec with sample RACF commands for setting up security. Also, the script also creates and mounts the z/OSMF data file system if it does not already exist.

-verify

This parameter verifies the configuration of z/OSMF. To indicate the scope of this verification, specify -verify with one of the following options:

- racf** Verify the RACF security setup for all configured tasks and functions. This option should be used by your security administrator.
- core** Verify the system setup for the core functions only.
- log** Verify the system setup for the Incident Log task only, as listed in Table 17 on page 95.
- all** Verify the system setup for all configured tasks and functions. **all** is the default.

-finish

This parameter completes the configuration of z/OSMF.

-addlink

This parameter adds a link to the z/OSMF navigation area through the specified link properties file. Use this option only at the direction of IBM Support or your vendor. For information, see Chapter 14, “Adding links to z/OSMF through the `izusetup.sh` script,” on page 167.

-modify

This parameter allows you to modify the z/OSMF server configuration settings. The script takes as input values that you specify in a separate file and applies the values to your z/OSMF configuration. Use this option only at the direction of IBM Support. For information, see Appendix D, “Modifying the advanced settings for the z/OSMF configuration,” on page 293.

Optional parameters

You can specify one of the following optional parameters with a required parameter.

-add

This parameter indicates that you want to add plug-ins to an already configured instance of z/OSMF. Specify the `-add` option with the existing options `-config` or `-finish`.

You can specify which plug-ins are to be added in your override file, which you specify on the optional `-overridefile` option. In the override file, mark the plug-ins to be added with the character **A**. If you omit the override file, the script prompts you to specify which plug-ins are to be added.

When specified with the optional `-fastpath` parameter, the script runs without any interactive prompting. Instead, the script uses the values from the configuration file and the override file, if specified. Omitted values will cause the script to end with errors.

For more information, see Chapter 7, “Adding plug-ins to a z/OSMF configuration,” on page 127.

-fastpath

This optional parameter indicates that you want to use the variable values that are specified in the configuration file, the override file, or a combination of both files. When you specify this parameter, during the configuration process, you are not prompted for new values for the variables.

You must ensure that any variables specified in the override file are set to valid values for your installation. Some variables are initially set to the following value, which is not a valid setting: `NO.DEFAULT.VALUE`.

For more information, see “Choosing a script mode: Interactive or fastpath” on page 21.

-overridefile *filename.ovr*

This optional parameter indicates that you want to use the variable values that are specified in the override file. For *filename.ovr*, specify the name of the override file that the **izusetup.sh** script is to use as input.

The override file takes precedence over the same values specified in the configuration file. For any configuration values not found in either of these files, the script prompts you for valid values.

For more information, see “Using an override file” on page 21.

Examples

In the following example, the **izusetup.sh** script begins the configuration process for z/OSMF. Your input values will be saved in the configuration file `izuconfig1.cfg`.

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

The script locates the configuration file (`izuconfig1.cfg`) in the directory specified on the `IZU_CONFIG_DIR` configuration variable. By default, this is `/etc/zosmf`.

In the following example, the **izusetup.sh** script runs the configuration process for any new plug-ins to be added. Because the optional parameter `-fastpath` is omitted, the script will run in interactive mode, prompting you for which plug-ins are to be configured and for related setup information.

```
izusetup.sh -file izuconfig1.cfg -config -add
```

In the following example, the **izusetup.sh** script refreshes the z/OSMF server configuration settings to use one or more replacement values that you specified.

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

Appendix C. Default configuration file and default override file

A default configuration file, called `izudflt.cfg`, and a default override file, called `izudflt.ovr`, are provided with z/OSMF. You can use these files to provide your input to the **izusetup.sh** script.

The contents of these files are shown in the following sections:

- “Default configuration file”
- “Default override file” on page 291.

Default configuration file

The default configuration file, `izudflt.cfg`, contains the variables and associated default values that the **izusetup.sh** script uses to configure your z/OSMF instance. This file is located in the `<IZU_CODE_ROOT>/defaults` directory.

Table 47. Default configuration file

Variable name	Default value	Description
IZU_CONFIG_FILE_VERSION	2.1.0	Version number, which identifies the format of this configuration file.
IZU_DATA_DIR	/var/zosmf/data	Mount point (the fully-qualified path name) for the z/OSMF data file system.
IZU_DATA_FS_NAME	IZU.SIZUDATA	z/OSMF data file system.
IZU_DATA_FS_TYPE	ZFS	Type of file system (zFS or HFS) to be used for creating the z/OSMF data file system.
IZU_DATA_FS_VOLUME	1*	Volume serial number (VOLSER) of the DASD to be used for creating the z/OSMF data file system, or * to let SMS select a volume.
IZU_DATA_FS_SIZE	200	Initial space allocation, in cylinders, for the z/OSMF data file system data set. The script uses 90% of this value for the primary allocation and 10% for the secondary allocation.
IZU_AUTOUID_OVERRIDE	NO.DEFAULT.VALUE	If you have AUTOUID enabled, this variable indicates whether (Y or N) RACF is to assign unused UIDs for your security group IDs.
IZU_AUTOGID_OVERRIDE	NO.DEFAULT.VALUE	If you have AUTOGID enabled, this variable indicates whether (Y or N) RACF is to assign unused GIDs for your security group IDs.
IZU_ADMIN_GROUP_NAME	IZUADMIN	Security group for the z/OSMF administrator role. Any user IDs connected to this group are considered to be z/OSMF administrators.
IZU_ADMIN_GROUP_GID	9003	Group ID (GID) for the z/OSMF administrator role.
IZU_USERS_GROUP_NAME	IZUUSER	Security group for the z/OSMF user role.
IZU_USERS_GROUP_GID	9004	Group ID (GID) for the z/OSMF user role.
IZU_HTTP_SSL_PORT	443	Port number for SSL encrypted traffic from the active instance of z/OSMF on your system.
IZU_HTTP_PORT	80	Port number for non-encrypted traffic from the active instance of z/OSMF on your system.
IZU_APPSERVER_HOSTNAME	@HOSTNAME	z/OSMF server host name.
IZU_CIM_ADMIN_GROUP_NAME	CFZADMGP	Security group for the CIM Administrator role.
IZU_CIM_USER_GROUP_NAME	CFZUSRGP	Group ID (GID) for the CIM Administrator role.
IZU_ZOS_SECURITY_ADMIN_GROUP_NAME	IZUSECAD	Security group for the z/OS Security Administrator role.

Table 47. Default configuration file (continued)

Variable name	Default value	Description
IZU_ZOS_SECURITY_ADMIN_GROUP_GID	9006	Group ID (GID) for the z/OS Security Administrator role.
IZU_CA_CONFIGURE	NO	Indicates whether (Y or N) the Configuration Assistant plug-in is to be included in z/OSMF.
IZU_CP_CONFIGURE	NO	Indicates whether (Y or N) the Capacity Provisioning plug-in is to be included in z/OSMF.
IZU_CP_QUERY_GROUP_NAME	CPOQUERY	Security group for users of the Capacity Provisioning task view function.
IZU_CP_CONTROL_GROUP_NAME	CPOCTRL	Security group for users of the Capacity Provisioning task edit function.
IZU_DM_CONFIGURE	NO	Indicates whether (Y or N) the Software Deployment plug-in is to be included in z/OSMF.
IZU_IL_CONFIGURE	NO	Indicates whether (Y or N) the Incident Log plug-in is to be included in z/OSMF.
IZU_IL_CEA_CONFIGURE	Y	Indicates whether (Y or N) z/OSMF is to enable the common event adapter (CEA) component and related parmlib options for using the Incident Log task.
IZU_CEA_HLQ	CEA	The high level qualifier to be used for CEA data sets, as defined in the CEAPRMxx parmlib member (one to eight characters). This value is used in creating RACF commands for the Incident Log task.
IZU_COUNTRY_CODE	NO.DEFAULT.VALUE	IBM-defined country code for your site (3-character alphanumeric).
IZU_BRANCH_CODE	NO.DEFAULT.VALUE	IBM-defined branch code (or branch office) for your site (3-character alphanumeric).
IZU_STORAGE_VALUE	NO.DEFAULT.VALUE	Indicates where CEA is to store the snapshot information for Incident Log processing. Specify either an SMS storage class (in double quotes) or up to seven volumes (in double quotes), as follows: <ul style="list-style-type: none"> • "STORCLAS(STRCLS)" • "VOLSER(volume1, volume2, volume3,...volume7)" The double quotes are required.
IZU_CEAPRM_SOURCE_PARMLIB	SYS1.PARMLIB	Source data set that contains the IBM-supplied member, CEAPRM00. Usually, this is your SMPE-installed SYS1.PARMLIB data set. Ensure that the data set exists and is cataloged.
IZU_CEAPRM_TARGET_PARMLIB	SYS1.PARMLIB	Target data set to be used for the newly created CEAPRMnn member for Incident Log processing.
IZU_IEADMC_SOURCE_PARMLIB	SYS1.SAMPLIB	Source data set that contains the IBM-supplied member, IEADMCZM. Usually, this is your SMPE-installed SYS1.SAMPLIB data set. Ensure that the data set exists and is cataloged.
IZU_IEADMC_TARGET_PARMLIB	SYS1.PARMLIB	Target data set to be used for the newly created IEADMCnn member for Incident Log processing.
IZU_CEA_PARM_NAME	01	Two-character suffix of a new CEAPRMxx parmlib member to be used for enabling captures or "snapshots" of the system logs. Two characters are required.
IZU_IEA_PARM_NAME	ZM	Two-character suffix of a new IEADMCxx parmlib member to be used for setting dump options. Two characters are required.
IZU_WISPF_CONFIGURE	NO	Indicates whether (Y or N) the ISPF plug-in is to be included in z/OSMF.
IZU_RMF_CONFIGURE	NO	Indicates whether (Y or N) the Resource Monitoring plug-in is to be included in z/OSMF.

Table 47. Default configuration file (continued)

Variable name	Default value	Description
IZU_WLM_CONFIGURE	NO	Indicates whether (Y or N) the Workload Management plug-in is to be included in z/OSMF.
IZU_WLM_GROUP_NAME	WLMGRP	Security group for users of the Workload Management task.
IZU_STARTED_TASK_USERID_NAME	IZUSVR	z/OSMF started task user ID.
IZU_STARTED_TASK_USERID_UID	9010	UID for the z/OSMF started task user ID.
IZU_STARTED_TASK_USERID_HOME	/var/zosmf/data/home/izusvr	Home directory for the z/OSMF started task user ID.
IZU_STARTED_TASK_USERID_PROGRAM	/bin/sh	Program path for the z/OSMF started task identity for z/OS UNIX system services.
IZU_SAF_PROFILE_PREFIX	IZUDFLT	z/OSMF SAF profile prefix.
IZU_DEFAULT_CERTAUTH	Y	Indicates 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.
IZU_UNAUTHENTICATED_NAME	IZUGUEST	Security group for unknown users. Provides basic privileges to access the Welcome page, but nothing more.
IZU_UNAUTHENTICATED_UID	9011	Represents an unknown user for security purposes. This user ID is used by the z/OSMF server when no other user credentials are available for web container access. This is a restricted user ID; do not assign a password.
IZU_RESTAPI_FILE_PROC	IZUFPROC	TSO logon procedure to be used for operations with the z/OS data set and file REST interface services.
IZU_RESTAPI_FILE_ACCT	IZUACCT	TSO account number to be used for the procedure for the z/OS data set and file REST interface services.
IZU_RESTAPI_FILE_REGION	32768	TSO address space region size (in kilobytes) to be used for the procedure for the z/OS data set and file REST interface services.

Default override file

The override response file is the last configuration file to be processed. Therefore, you can use this file to:

- Override values in the configuration file without directly modifying the configuration file.
- Make variable substitutions.

A default override response file is located in the <IZU_CODE_ROOT>/defaults directory. Figure 65 on page 292 shows the content of the default override file.

```

# Licensed Materials - Property of IBM
# 5610-A01
# Copyright IBM Corp. 2012
#
# Status = HSMA210
#
# Information:
#
# SID=%I%
# Delta Date=%G%
# Delta Time=%U%
#
# The izudflt.ovr file does not contain every variable=value pair that is in the izudflt.cfg file.
# Those variables that are least likely to be modified do not appear in this file.
# If your installation requires a change to a variable that isn't in this file, and you would prefer
# to configure it in your override file, simply add it with the modified value.
#
# Do not update or remove variable IZU_OVERRIDE_FILE_VERSION. The information
# is required for the configuration processing.
IZU_OVERRIDE_FILE_VERSION=2.1.0
IZU_DATA_DIR=/var/zosmf/data
IZU_DATA_FS_NAME=IZU.SIZUDATA
IZU_DATA_FS_TYPE=ZFS
IZU_DATA_FS_VOLUME='*'
IZU_DATA_FS_SIZE=200
IZU_AUTOUID_OVERRIDE=NO.DEFAULT.VALUE
IZU_AUTOGID_OVERRIDE=NO.DEFAULT.VALUE
IZU_ADMIN_GROUP_NAME=IZUADMIN
IZU_ADMIN_GROUP_GID=9003
IZU_USERS_GROUP_NAME=IZUUSER
IZU_USERS_GROUP_GID=9004
IZU_HTTP_SSL_PORT=443
IZU_APPSERVER_HOSTNAME=@HOSTNAME
IZU_CIM_ADMIN_GROUP_NAME=CFZADMGP
IZU_CIM_USER_GROUP_NAME=CFZUSRGP
IZU_ZOS_SECURITY_ADMIN_GROUP_NAME=IZUSECAD
IZU_ZOS_SECURITY_ADMIN_GROUP_GID=9006
IZU_CA_CONFIGURE=NO
IZU_CP_CONFIGURE=NO
IZU_CP_QUERY_GROUP_NAME=CPOQUERY
IZU_CP_CONTROL_GROUP_NAME=CPOCTRL
IZU_DM_CONFIGURE=NO
IZU_IL_CONFIGURE=NO
IZU_IL_CEA_CONFIGURE=Y
IZU_CEA_HLQ='CEA'
IZU_COUNTRY_CODE=NO.DEFAULT.VALUE
IZU_BRANCH_CODE=NO.DEFAULT.VALUE
IZU_STORAGE_VALUE=NO.DEFAULT.VALUE
IZU_CEAPRM_SOURCE_PARMLIB=SYS1.PARMLIB
IZU_CEAPRM_TARGET_PARMLIB=SYS1.PARMLIB
IZU_IADMC_SOURCE_PARMLIB=SYS1.SAMPLIB
IZU_IADMC_TARGET_PARMLIB=SYS1.PARMLIB
IZU_CEA_PARM_NAME=01
IZU_IEA_PARM_NAME=ZM
IZU_WISPF_CONFIGURE=NO
IZU_RMF_CONFIGURE=NO
IZU_WLM_CONFIGURE=NO
IZU_WLM_GROUP_NAME=WLMGRP
IZU_STARTED_TASK_USERID_NAME=IZUSVR
IZU_STARTED_TASK_USERID_UID=9010
IZU_STARTED_TASK_HOME=/var/zosmf/data/home/izusvr
IZU_STARTED_TASK_PROGRAM=/bin/sh
IZU_SAF_PROFILE_PREFIX=IZUDFLT
IZU_DEFAULT_CERTAUTH=Y
IZU_UNAUTHENTICATED_NAME=IZUGUEST
IZU_UNAUTHENTICATED_UID=9011
IZU_RESTAPI_FILE_PROC=IZUFPROC
IZU_RESTAPI_FILE_ACCT=IZUACCT
IZU_RESTAPI_FILE_REGION=32768

```

Figure 65. Default override file

Appendix D. Modifying the advanced settings for the z/OSMF configuration

z/OSMF includes a number of advanced settings that affect the behavior of the product. In most cases, you should not need to change these values. In some situations, however, you might be asked by IBM Support to modify the z/OSMF advanced settings. To do so, you will use the **izusetup.sh** script with option **-modify**.

About this script

The **izusetup.sh** script with option **-modify** allows you to modify the z/OSMF advanced settings. The script takes as input values that you specify in a text file and applies the values to your z/OSMF configuration.

Table 48 describes the z/OSMF advanced settings. You can change one or more of the settings in each invocation of the **izusetup.sh** script.

Table 48. z/OSMF advanced settings

izuadmin.env variable	Description	Allowable range of values	Default value
ltpatimeout	Amount of time (in minutes) for LTPA credentials to be forwarded between servers. z/OSMF user sessions expire when this period of time has elapsed. For information, see "Re-authenticating in z/OSMF" on page 208.	25 – 35971	490
ltpacachetimeout	Amount of time (in seconds) for authentication settings to be held in cache.	1500 – 2158260 This value must be less than or equal to the ltpatimeout value multiplied by 60.	29400
sessiontimeout	Amount of time (in minutes) for the session management session timeout.	This value must be at least 5 greater than the ltpatimeout value.	495
izuilunitvalue	Device to be used for storing data sets and z/OS UNIX files for the FTP jobs. This setting is applicable if your z/OSMF configuration includes the Incident Log plug-in.	N/A	SYSDA
izuiltempdirvalue	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.	N/A	/tmp
izugwrkmanwlmclass	WLM transaction class to be used for managing the execution of long-running work. This setting is applicable if your z/OSMF configuration includes the Software Deployment plug-in.	One to eight alphanumeric characters (A-Z, a-z, 0-9) or special characters (#, \$, or @).	IZUGWORK

Table 48. z/OSMF advanced settings (continued)

izuadmin.env variable	Description	Allowable range of values	Default value
cimjnitimeout	Amount of time (in seconds) that z/OSMF is to wait for a response from the CIM server. If timeouts from CIM providers occur frequently, increasing this value can help to reduce the number of timeouts.	1 – 3600	300
izutracespec	Initial trace state for the z/OSMF server. These settings are read when the server is started. If there is a problem with starting the server, this value is used to enable tracing for server startup.	This value is provided by IBM Support.	Reserved by IBM.
izunotificationsmax	Maximum number of z/OSMF user notifications that can be created for your installation.	1 – 1000	500
izunotificationexpiration	Expiration (in days) for z/OSMF user notifications at your installation.	0 – 1825	30
izuworkflowsmax	Maximum number of z/OSMF workflows that can be created for your installation.	1 – 500	200

Before running the script

Check for a modified version of the **izuadmin.env** file in the z/OSMF configuration directory. If your installation currently uses a modified version of the **izuadmin.env** file, perhaps from a previous z/OSMF configuration, it is recommended that you make a backup copy of the file and make note of any customized settings that should be preserved in the new copy. By default, the z/OSMF configuration directory is `/etc/zosmf` and is specified through the environment variable, `IZU_CONFIG_DIR`, as described in “Setting the z/OSMF environment variables for your shell session” on page 30.

Ensure that the z/OSMF environment variables are set properly for your z/OS UNIX shell session. See “Setting the z/OSMF environment variables for your shell session” on page 30.

You can run this script regardless of whether the z/OSMF server is running. Your changes, however, do not take effect until after the server is started or recycled. For information about starting and stopping the server, see “Step 6: Start the z/OSMF server” on page 41.

Modifying your current settings

A sample **izuadmin.env** file is supplied with z/OSMF in the following directory:

`<IZU_CODE_ROOT>/defaults/`

where `<IZU_CODE_ROOT>` is the z/OSMF product file system. By default, this is `/usr/lpp/zosmf/V2R1`.

To override any of the current settings, use this procedure:

1. Copy the file **izuadmin.env** from the directory `<IZU_CODE_ROOT>/defaults` to the directory `<IZU_CONFIG_DIR>`.
2. Edit the `<IZU_CONFIG_DIR>/izuadmin.env` file using an editor of your choice, updating the settings as needed. Figure 66 on page 295 shows which settings are processed by the **izusetup.sh** script.

```

ltpatimeout=490
ltpacachetimeout=29400
sessiontimeout=495
izugwrkmanwlmclass=IZUGWORK
#cimjnitimeout=300
#izutracespec="com.ibm.zosmf.*=INFO:com.ibm.zosmf.environment.ui=finer"
#izunotificationsmax=750
#izunotificationexpiration=100
#izuworkflowsmax=200

```

Figure 66. Settings that are processed through the `izusetup.sh -modify` script

Observe the following considerations for the **izuadmin.env** file:

- Do not modify the file version identifier: `izufileversion=n.nn.n`
- Do not modify or delete settings other than those shown in Figure 66
- If you omit a setting, comment it out, or set it to null, the IBM default value is used
- Some input fields are commented. To modify these settings, you must remove the comment character '#'.

3. Run the **izusetup.sh** script, as described in “Running the script.”

Tip: Suppose that you only want to display the current settings for your configuration without making any changes. You can do so through the **izusetup.sh** script. Run the **izusetup.sh** script with option `-modify` as described previously, but without making any changes to the **izuadmin.env** file. The **izusetup.sh** script displays the current settings for your configuration.

Running the script

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 following directory:

<IZU_CODE_ROOT>/bin

where <IZU_CODE_ROOT> is the z/OSMF product file system. By default, this is /usr/lpp/zosmf/V2R1.

Syntax

Use the following syntax:

```

▶▶ izusetup.sh -file [izuconfig1.cfg | pathname/izuconfig1.cfg] -modify ▶▶

```

where:

- `-file` is a required parameter; use it to specify the configuration file (*izuconfig1.cfg*) for your installation. On the `-file` parameter, *pathname* is optional. If you omit a path name, the script attempts to obtain the configuration file from the z/OSMF configuration directory: <IZU_CONFIG_DIR>.
- `-modify` is a required parameter; use it to indicate that the z/OSMF server configuration settings are to be modified.

Example

The following example shows a typical invocation of the **izusetup.sh** script:

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

Observe that:

- -file is required; it specifies the configuration file, which is named `izuconfig1.cfg` in this example.
- -modify is required.

Results

The **izusetup.sh** script writes the new settings for your configuration to standard output and to the script log file:

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

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

The script also write progress messages to this location. Check the messages to determine whether a problem occurred during script processing. If so, you must resolve the problem before the request can be completed.

During processing, the **izusetup.sh** script runs another script called **izuadmin.sh** to handle your request. As a result, some of the messages issued during processing refer to the **izuadmin.sh** script.

Appendix E. 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 300 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 49 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 49. 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 107.	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. See “Creating the commands to authorize a user ID” on page 131.	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	CEAIPROSERVER 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

Table 49. 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: <ul style="list-style-type: none"> • 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 104.		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: <ul style="list-style-type: none"> • DIAG=8 • DIAG2=851. Also, check message CEZ05000E in SYSLOG. CEASERRO_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: <ul style="list-style-type: none"> • 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 109.	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 109.	CEZ05006E	IZUP643E	CEASYSREXXBAD ENVIRONMENT
871	367	System REXX cannot process the exec at this time.	Try the request again later.	CEZ05007W	IZUP644E	CEAEXEETIMEOUT
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.	Perform the corrective action described in “User is not SAF authorized” on page 202.	CEZ05010E		CEANOSAF OPERLOGSNAP

Table 49. 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 96. 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 <i>nnnnn.ccc.bbb</i> where <i>nnnnn</i> is the PMR number, <i>bbb</i> is the branch code, and <i>ccc</i> 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.	<ul style="list-style-type: none"> Ensure that only one user is attempting to access the dump information at one time. To check for enqueue contention, enter the following command at the operator console: D GRS Wait for the enqueue to be released and try again. 	CEZ05017E	IZUP641E	CEAIPCSNQ 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 105.	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 49. 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 106.			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 16, "Deleting incidents and diagnostic data," on page 173. 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 50 describes the CEA reason codes that an HTTP client application might encounter when using the z/OS jobs REST interface services.

Table 50. 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 277.	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.	CEASSJOBNOTFOUND

Appendix F. Contents of the RACF commands execs

During the configuration process, z/OSMF creates REXX execs with sample RACF commands for your installation. Your security administrator can use these programs to create authorizations for the z/OSMF core functions and optional plug-ins.

Generally, the REXX execs contain commands for:

- Creating profiles in ZMFAPLA for each of the z/OSMF tasks to be enabled on your system
- Creating groups and permitting those groups to z/OSMF resources. By default, z/OSMF creates the groups IZUADMIN and IZUUSER, which correspond to the administrator and user roles, respectively. z/OSMF also creates the group IZUSECAD, to allow your z/OS security administrator to perform the security-related steps in the Workflows task.

When you create a base configuration, z/OSMF creates the REXX exec **izuconfig1.cfg.rexx**, which contains sample RACF commands for securing the z/OSMF core functions and tasks. These commands are shown in “Commands for securing the core functions”

When you add optional plug-ins to a z/OSMF configuration, z/OSMF creates the REXX exec **izuconfig1.cfg.add.rexx** for securing the plug-ins. These commands are shown in the following sections:

- “Commands for permitting z/OSMF tasks to the CIM server” on page 307
- “Commands for configuring the Capacity Provisioning plug-in” on page 308
- “Commands for configuring the Configuration Assistant plug-in” on page 310
- “Commands for configuring the Incident Log plug-in” on page 312
- “Commands for configuring the ISPF plug-in” on page 315
- “Commands for configuring the Resource Monitoring plug-in” on page 317
- “Commands for configuring the Software Deployment plug-in” on page 319
- “Commands for configuring the Workload Management plug-in” on page 321

Commands for securing the core functions

When you create a base z/OSMF configuration, the REXX exec **izuconfig1.cfg.rexx** contains RACF commands for securing the z/OSMF core functions. The contents of the exec are shown in the following figures:

- Figure 67 on page 302
- Figure 68 on page 303
- Figure 69 on page 304
- Figure 70 on page 305
- Figure 71 on page 306.

```

/* ----- */
/* Licensed Material - Property of IBM */
/* 5610-A01 */
/* Copyright IBM Corp. 2010, 2013 */
/* */
/* Status = HSMA210 */
/* ----- */
/* */
/* Description : This REXX exec contains RACF commands to assist */
/* your security administrator with z/OSMF security setup. */
/* */
/* This exec was generated as a result of running the z/OSMF */
/* izusetup.sh script in configuration mode, */
/* or the izuauthuser.sh script. */
/* */
/* Review this exec before running it and modify it as needed to */
/* ensure that the options it sets, or the profiles it defines, */
/* or the connections it makes */
/* are workable in your environment and consistent with your */
/* installation's security practices and site policies. */
/* */
/* If your installation uses a security product other than RACF, */
/* you must create equivalent authorizations in your security product. */
/* ----- */

address TS0

/* Keep track of maximum return code from RACF commands. */
MaxRC = 0

/*-----*/
/* */
/* z/OSMF configured for SAF authorization mode. */
/* */
/*-----*/

/*-----*/
/* */
/* Begin "Core" Setup */
/* */
/*-----*/

/* This commented section contains the CLASS activation commands */
/* Insure the following classes are active before executing this script */
/* Or creating profiles in these classes. */
/* */
/* Activate the APPL class */
/*Call RacfCmd "SETROPTS CLASSACT(APPL)" */
/*Call RacfCmd "SETROPTS RACLIST(APPL) GENERIC(APPL)" */
/* */
/* Activate the EJBROLE class */
/*Call RacfCmd "SETROPTS CLASSACT(EJBROLE)" */
/*Call RacfCmd "SETROPTS RACLIST(EJBROLE) GENERIC(EJBROLE)" */
/* */
/* Activate the FACILITY class */
/*Call RacfCmd "SETROPTS CLASSACT(FACILITY)" */
/*Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)" */
/* */
/* Activate the SERVER class */
/*Call RacfCmd "SETROPTS CLASSACT(SERVER)" */
/*Call RacfCmd "SETROPTS RACLIST(SERVER)" */
/* */
/* Activate the SERVAUTH class */
/*Call RacfCmd "SETROPTS CLASSACT(SERVAUTH)" */
/*Call RacfCmd "SETROPTS RACLIST(SERVAUTH) GENERIC(SERVAUTH)" */
/* */
/* Activate the STARTED class */
/*Call RacfCmd "SETROPTS CLASSACT(STARTED)" */
/*Call RacfCmd "SETROPTS RACLIST(STARTED) GENERIC(STARTED)" */
/* */
/* Activate the ZMFAPLA class */
/*Call RacfCmd "SETROPTS CLASSACT(ZMFAPLA)" */
/*Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) GENERIC(ZMFAPLA)" */
/* */
/* Activate the ACCTNUM class */
/*Call RacfCmd "SETROPTS CLASSACT(ACCTNUM)" */

```

Figure 67. Sample RACF commands for configuring the core functions of z/OSMF (Part 1 of 5)

```

/* Activate the TSOPROC class */
/*Call RacfCmd "SETROPTS CLASSACT(TSOPROC)" */
/* */
/* Create the z/OSMF Administrators group */
Call RacfCmd "ADDGROUP IZUADMIN OMVS(GID(9123))"

/* Create the z/OSMF Users group */
Call RacfCmd "ADDGROUP IZUUSER OMVS(GID(9004))"

/* Create the z/OSMF Unauthenticated group */
Call RacfCmd "ADDGROUP IZUUNGRP OMVS(GID(234))"

/* Create the started task USERID for the z/OSMF Server */
/* Please note, the HOME directory is created in the -finish step. */
/* If this directory is AUTOMOUNT managed, pre-create it before the -finish step */
Call RacfCmd "ADDUSER IZUSVR DFLTGRP(IZUADMIN) OMVS(UID(1234) HOME(/u/izusvr/jgc) PROGRAM(/bin/sh))
NAME('zOSMF Started Task USERID') NOPASSWORD NOOIDCARD"

/* Change concurrent open file number for started task USERID */
Call RacfCmd "ALTUSER IZUSVR OMVS(FILEPROC(10000))"

/* Create the z/OSMF unauthenticated USERID */
Call RacfCmd "ADDUSER IZUGUEST RESTRICTED DFLTGRP(IZUUNGRP) OMVS(UID(12332111))
NAME('zOSMF Unauthenticated USERID') NOPASSWORD NOOIDCARD"

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

/* Define the APPL profile for the z/OSMF server */
CALL RacfCmd "RDEFINE APPL IZUDFLT UACC(NONE)"

/* Define the SERVER profiles for the z/OSMF server */
CALL RacfCmd "RDEFINE SERVER BBG.SECPF.XIZUDFLT UACC(NONE)"
CALL RacfCmd "RDEFINE SERVER BBG.ANGEL UACC(NONE)"
CALL RacfCmd "RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM UACC(NONE)"
CALL RacfCmd "RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM.SAFCRED UACC(NONE)"
CALL RacfCmd "RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM.ZOSWLM UACC(NONE)"
CALL RacfCmd "RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM.TXRRS UACC(NONE)"
CALL RacfCmd "RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM.ZOSDUMP UACC(NONE)"

/* Permit the z/OSMF unauthenticated USERID access*/
Call RacfCmd "PERMIT IZUDFLT CLASS(APPL) ID(IZUGUEST) ACCESS(READ)"

/* Permit the started task USERID access*/
CALL RacfCmd "PERMIT BBG.SECPF.XIZUDFLT CLASS(SERVER) ACCESS(READ) ID(IZUSVR)"
CALL RacfCmd "PERMIT BBG.ANGEL CLASS(SERVER) ACCESS(READ) ID(IZUSVR)"
CALL RacfCmd "PERMIT BBG.AUTHMOD.BBGZSAFM CLASS(SERVER) ACCESS(READ) ID(IZUSVR)"
CALL RacfCmd "PERMIT BBG.AUTHMOD.BBGZSAFM.SAFCRED CLASS(SERVER) ACCESS(READ) ID(IZUSVR)"
CALL RacfCmd "PERMIT BBG.AUTHMOD.BBGZSAFM.ZOSWLM CLASS(SERVER) ACCESS(READ) ID(IZUSVR)"
CALL RacfCmd "PERMIT BBG.AUTHMOD.BBGZSAFM.TXRRS CLASS(SERVER) ACCESS(READ) ID(IZUSVR)"
CALL RacfCmd "PERMIT BBG.AUTHMOD.BBGZSAFM.ZOSDUMP CLASS(SERVER) ACCESS(READ) ID(IZUSVR)"

/* Define the BPX.CONSOLE profile to suppress the BPXM023I message prefix for console messages */
CALL RacfCmd "RDEFINE FACILITY BPX.CONSOLE UACC(NONE)"

/* Permit the started task USERID access*/
CALL RacfCmd "PERMIT BPX.CONSOLE CLASS(FACILITY) ID(IZUSVR) ACCESS(READ)"

/* Define the Sync-to-OS-thread FACILITY profile */
CALL RacfCmd "RDEFINE FACILITY BBG.SYNC.IZUDFLT UACC(NONE)"

/* Permit the started task USERID access*/
CALL RacfCmd "PERMIT BBG.SYNC.IZUDFLT CLASS(FACILITY) ID(IZUSVR) ACCESS(CONTROL)"

/* Define the FACILITY profile for working with digital certificates */
CALL RacfCmd "RDEFINE FACILITY IRR.DIGTCERT.LIST UACC(NONE)"
CALL RacfCmd "RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE)"

/* Permit the started task USERID access*/
CALL RacfCmd "PERMIT IRR.DIGTCERT.LIST CLASS(FACILITY) ID(IZUSVR) ACCESS(READ)"
CALL RacfCmd "PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(IZUSVR) ACCESS(READ)"

```

Figure 68. Sample RACF commands for configuring the core functions of z/OSMF (Part 2 of 5)

```

/* Create the CA certificate for the z/OSMF server */
CALL RacfCmd "RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('z/OSMF CertAuth for Security Domain') OU('IZUDFLT'))
              WITHLABEL('zOSMFCA') TRUST NOTAFTER(DATE(2022/06/27))"
CALL RacfCmd "RACDCERT ADDRING(IZUKeyring.IZUDFLT) ID(IZUSVR)"

/* Create the server certificate for the z/OSMF server */
CALL RacfCmd "RACDCERT ID( IZUSVR ) GENCERT SUBJECTSDN(CN('PEV051.POK.IBM.COM') O('IBM') OU('IZUDFLT'))
              WITHLABEL('DefaultzOSMFCert.IZUDFLT')" ,
              "SIGNWITH(CERTAUTH LABEL('zOSMFCA')) NOTAFTER(DATE(2022/06/27))"
CALL RacfCmd "RACDCERT ALTER(LABEL('DefaultzOSMFCert.IZUDFLT')) ID('IZUSVR') TRUST"
CALL RacfCmd "RACDCERT ID( IZUSVR ) CONNECT (LABEL('DefaultzOSMFCert.IZUDFLT') RING(IZUKeyring.IZUDFLT) DEFAULT)"
CALL RacfCmd "RACDCERT ID( IZUSVR ) CONNECT (LABEL('zOSMFCA') RING(IZUKeyring.IZUDFLT) CERTAUTH)"

/* Assumption: SERVAUTH class is active */
/* Call RacfCmd "SETROPTS GENERIC(SERVAUTH)" */

/* Define the CEA resource profile required for z/OSMF server */
CALL RacfCmd "RDEFINE SERVAUTH CEA.CEATSO.* UACC(NONE)"

/* Define the Account Number resource profile for REST File API */
CALL RacfCmd "RDEFINE ACCTNUM #124JGDIRUTNCHD UACC(NONE)"

/* Define the TSO Procedure resource profile for REST File API */
CALL RacfCmd "RDEFINE TSOPROC IZUFPROC UACC(NONE)"

/* List-of-groups authority checking supplements the normal RACF access authority checking */
/* by allowing all groups of which a user ID is a member to enter into the access list checking process. */
/* Un-comment the following line to activate this. */
/* Call RacfCmd "SETROPTS GRPLIST" */

/* Create the z/OS Security Administrators group */
CALL RacfCmd "ADDGROUP IZUSECAD OMVS(GID(0))"

/* Define the ZMFAPLA profile for the z/OSMF server */
CALL RacfCmd "RDEFINE ZMFAPLA IZUDFLT.ZOSMF UACC(NONE)"

/* The EJBROLE definitions are case-sensitive in RACF. Insure you preserve case for these commands */
/* Assumption: EJBROLE is defined, activated, and raclisted. */
CALL RacfCmd "RDEFINE EJBROLE IZUDFLT.*.izuUsers UACC(NONE)"

/* Define the z/OSMF Server profile */
CALL RacfCmd "RDEFINE SERVER BBG.SECCLASS.ZMFAPLA UACC(NONE)"

/* Permit the started task USERID access */
CALL RacfCmd "PERMIT BBG.SECCLASS.ZMFAPLA CLASS(SERVER) ID(IZUSVR) ACCESS(READ)"

/* Roles processing will permit the z/OSMF Server groups to the Application Server resources */
/* Assumption: APPL class has been defined, activated, and raclisted. */

/* Permit the Administrators group to this profile */
CALL RacfCmd "PERMIT CEA.CEATSO.* CLASS(SERVAUTH) ID(IZUADMIN) ACCESS(READ)"

/* Permit the Users group to this profile */
CALL RacfCmd "PERMIT CEA.CEATSO.* CLASS(SERVAUTH) ID(IZUUSER) ACCESS(READ)"

/* Permit the started task USERID to this profile */
CALL RacfCmd "PERMIT CEA.CEATSO.* CLASS(SERVAUTH) ID(IZUSVR) ACCESS(READ)"

/* Make changes effective */
CALL RacfCmd "SETROPTS RACLIST(SERVAUTH) REFRESH"

/* Permit the Administrators group to these profiles */
CALL RacfCmd "PERMIT #124JGDIRUTNCHD CLASS(ACCTNUM) ID(IZUADMIN) ACCESS(READ)"
CALL RacfCmd "PERMIT IZUFPROC CLASS(TSOPROC) ID(IZUADMIN) ACCESS(READ)"

/* Permit the Users group to these profiles */
CALL RacfCmd "PERMIT #124JGDIRUTNCHD CLASS(ACCTNUM) ID(IZUUSER) ACCESS(READ)"
CALL RacfCmd "PERMIT IZUFPROC CLASS(TSOPROC) ID(IZUUSER) ACCESS(READ)"

```

Figure 69. Sample RACF commands for configuring the core functions of z/OSMF (Part 3 of 5)


```

/*****
/* If your installation utilizes hardware crypto in combination with */
/* ICSF, various services like CSFRNGL, CSFDSV, CSFOWH, CSFIQF , etc. */
/* may be protected by profiles established in your security product. */
/* In certain cases, z/OSMF will utilize these services, and the z/OSMF */
/* started task USERID will need to be permitted to these profiles. */
/* If concrete profiles in the CSFSERV class has been defined */
/* to protect these resources, then, the following commented commands */
/* would permit the started task userid to that profile which is used by */
/* associated ICSF service. */
/*
/*Call RacfCmd "PERMIT CSFIQF CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* encipher callable service */
/*Call RacfCmd "PERMIT CSFENC CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* cryptographic variable encipher callable */
/*Call RacfCmd "PERMIT CSFCVE CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* decipher callable service */
/*Call RacfCmd "PERMIT CSFDEC CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* symmetric algorithm encipher callable service */
/*Call RacfCmd "PERMIT CSFAE CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* symmetric algorithm decipher callable service */
/*Call RacfCmd "PERMIT CSFSAD CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* one-way hash generate callable service */
/*Call RacfCmd "PERMIT CSFOWH CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* random number generate callable service */
/*Call RacfCmd "PERMIT CSFRNG CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* random number generate long callable service */
/*Call RacfCmd "PERMIT CSFRNGL CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* PKA key generate callable service */
/*Call RacfCmd "PERMIT CSFPKG CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* digital signature generate service */
/*Call RacfCmd "PERMIT CSFDSG CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* digital signature verify callable service */
/*Call RacfCmd "PERMIT CSFDSV CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* PKA key token change callable service */
/*Call RacfCmd "PERMIT CSFPKT CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* retained key list callable service */
/*Call RacfCmd "PERMIT CSFRKL CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* PKA Public Key Extract callable service */
/*Call RacfCmd "PERMIT CSFPKX CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* PKA encrypt callable service */
/*Call RacfCmd "PERMIT CSFPKE CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* PKA decrypt callable service */
/*Call RacfCmd "PERMIT CSFPKD CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* PKA key import callable service */
/*Call RacfCmd "PERMIT CSFPKI CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* multiple clear key import callable service */
/*Call RacfCmd "PERMIT CSFCKM CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* key generate callable service */
/*Call RacfCmd "PERMIT CSFKGN CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* ECC Diffie-Hellman callable service */
/*Call RacfCmd "PERMIT CSFEDH CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/* key token build callable service */
/*Call RacfCmd "PERMIT CSFKTB CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)" */
/*
/*Call RacfCmd "SETOPTS RACLIST(CSFSERV) REFRESH"
*****/

/* Profile Definitions for "Core" */
Call RacfCmd "RDEFINE ZMFAPLA IZUDFLT.ZOSMF.ADMINTASKS.** UACC(NONE)"
Call RacfCmd "RDEFINE ZMFAPLA IZUDFLT.ZOSMF.LINK.** UACC(NONE)"
Call RacfCmd "RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SETTINGS.*.VIEW UACC(NONE)"
Call RacfCmd "RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SETTINGS.*.MODIFY UACC(NONE)"
Call RacfCmd "RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SETTINGS.SYSTEMS UACC(NONE)"
Call RacfCmd "RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS UACC(NONE)"

/*-----*/
/* End "Core" Setup */
/*-----*/

/*-----*/
/* Begin "Workflow" Setup */
/*-----*/

/* Profile Definitions for "Workflow" */
Call RacfCmd "RDEFINE ZMFAPLA IZUDFLT.ZOSMF.WORKFLOW.** UACC(NONE)"

/*-----*/
/* End "Workflow" Setup */
/*-----*/

```

Figure 70. Sample RACF commands for configuring the core functions of z/OSMF (Part 4 of 5)

```

/*-----*/
/* Begin "zOSMF User Role" Setup */
/*-----*/

Call RacfCmd "PERMIT IZUDFLT CLASS(APPL) ID(IZUUSER) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ID(IZUUSER) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/* Permit definitions for "Core" */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.LINK.** CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.SETTINGS.*.VIEW CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.SETTINGS.SYSTEMS CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/* Permit definitions for "Workflow" */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.WORKFLOW.** CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/*-----*/
/* End "zOSMF User Role" Setup */
/*-----*/

/*-----*/
/* Begin "zOSMF Administrator Role" Setup */
/*-----*/

Call RacfCmd "PERMIT IZUDFLT CLASS(APPL) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Permit definitions for "Core" */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.ADMINTASKS.** CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.LINK.** CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.SETTINGS.*.VIEW CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.SETTINGS.*.MODIFY CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.SETTINGS.SYSTEMS CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Permit definitions for "Workflow" */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.WORKFLOW.** CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/*-----*/
/* End "zOSMF Administrator Role" Setup */
/*-----*/

/*-----*/
/* Begin "zOS Security Administrator Role" Setup */
/*-----*/

Call RacfCmd "PERMIT IZUDFLT CLASS(APPL) ID(IZUSECAD) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ID(IZUSECAD) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IZUSECAD) ACCESS(READ)"

/* Permit definitions for "Workflow" */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.WORKFLOW.** CLASS(ZMFAPLA) ID(IZUSECAD) ACCESS(READ)"

/*-----*/
/* End "zOS Security Administrator Role" Setup */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ACCTNUM) REFRESH"
Call RacfCmd "SETROPTS RACLIST(TSOPROC) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"
/* Exit with maximum return code from RACF commands. */
Exit MaxRC;

```

Figure 71. Sample RACF commands for configuring the core functions of z/OSMF (Part 5 of 5)

Commands for permitting z/OSMF tasks to the CIM server

If your installation configures one or more optional plug-ins that require the use of the CIM server on your z/OS system, the REXX exec **izuconfig1.cfg.add.rexx** includes instructions for authorizing users to the CIM server resources, as shown in Figure 72. These instructions, and the sample command, are commented out in the generated exec.

```
/* During the z/OSMF configuration process, your installation selected */
/* one or more CIM dependent plug-in(s). As a result, your security */
/* administrator must ensure that the z/OSMF Administrator has the proper */
/* access to CIM resources. It is assumed that the CIM security */
/* job (CFZSEC), or equivalent, was run as part of the initial */
/* configuration for CIM. */

/* Connect the started task USERID to the CIM USER group */
Call RacfCmd "CONNECT (IZU_STARTED_TASK_USERID_NAME) GROUP(IZU_CIM_USER_GROUP_NAME)"

/* Exit with maximum return code from RACF commands. */
```

Figure 72. Sample RACF command for authorizing users to the CIM server resources

Commands for configuring the Capacity Provisioning plug-in

If your installation configures the Capacity Provisioning plug-in, the REXX exec `izuconfig1.cfg.add.rexx` includes authorizations for the Capacity Provisioning task, as shown in the following figures:

- Figure 73
- Figure 74 on page 309.

The exec includes RACF commands for creating specific profiles for the Capacity Provisioning task and granting access to the specific profiles to the z/OSMF administrators group, and z/OSMF users group.

```
/*-----*/
/*  Begin "Capacity Provisioning" Setup                                */
/*-----*/

/*  Profile Definitions for "Capacity Provisioning"  */
Call RacfCmd "RDEFINE ZMFAPLA
IZUDFLT.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.VIEW UACC(NONE)"

Call RacfCmd "RDEFINE ZMFAPLA
IZUDFLT.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT.** UACC(NONE)"

/*-----*/
/*  End "Capacity Provisioning" Setup                                */
/*-----*/

/*-----*/
/*  Begin "zOSMF User Role" Setup                                    */
/*-----*/

Call RacfCmd "PERMIT IZUDFLT CLASS(APPL) ID(IZUUSER) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ID(IZUUSER) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/*  Permit the Users role to the CEA address space services profile */
Call RacfCmd "PERMIT CEA.CEATSO.* CLASS(SERVAUTH) ID(IZUUSER) ACCESS(READ)"

/*  Permit definitions for "Capacity Provisioning"  */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.VIEW
CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/*-----*/
/*  End "zOSMF User Role" Setup                                    */
/*-----*/

/*  Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVAUTH) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"
```

Figure 73. Sample RACF commands for configuring the Capacity Provisioning plug-in (Part 1 of 2)

```

/*-----*/
/* Begin "zOSMF Administrator Role" Setup */
/*-----*/

Call RacfCmd "PERMIT IZUDFLT CLASS(APPL) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Permit the Administrators group to the CEA address space services profile */
Call RacfCmd "PERMIT CEA.CEATSO.* CLASS(SERVAUTH) ID(IZUADMIN) ACCESS(READ)"

/* Permit definitions for "Capacity Provisioning" */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.VIEW
CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT.**
CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/*-----*/
/* End "zOSMF Administrator Role" Setup */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVAUTH) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"

/*-----*/
/* Begin "zOS Security Administrator Role" Setup */
/*-----*/

/* No security setup procedure is required. */

/*-----*/
/* End "zOS Security Administrator Role" Setup */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVAUTH) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"

/* During the z/OSMF configuration process, your installation selected */
/* one or more CIM dependent plug-in(s). As a result, your security */
/* administrator must ensure that the z/OSMF Administrator has the proper */
/* access to CIM resources. It is assumed that the CIM security */
/* job (CFZSEC), or equivalent, was run as part of the initial */
/* configuration for CIM. */

/* Connect the started task USERID to the CIM USER group */
Call RacfCmd "CONNECT (IZUSVR) GROUP(CFZUSRGP)"

/* Exit with maximum return code from RACF commands. */

```

Figure 74. Sample RACF commands for configuring the Capacity Provisioning plug-in (Part 2 of 2)

Commands for configuring the Configuration Assistant plug-in

If your installation configures the Configuration Assistant plug-in, the REXX exec `izuconfig1.cfg.add.rexx` includes authorizations for the Configuration Assistant task, as shown in the following figures:

- Figure 75
- Figure 76 on page 311.

```
/*-----*/
/*                                          */
/*  Begin "Configuration Assistant" Setup  */
/*                                          */
/*-----*/

/* Profile Definitions for "Configuration Assistant" */
Call RacfCmd "RDEFINE ZMFAPLA IZUDFLT.ZOSMF.CONFIGURATION_ASSISTANT.** UACC(NONE)"

/*-----*/
/*                                          */
/*  End "Configuration Assistant" Setup      */
/*                                          */
/*-----*/

/*-----*/
/*                                          */
/*  Begin "zOSMF User Role" Setup          */
/*                                          */
/*-----*/

Call RacfCmd "PERMIT IZUDFLT CLASS(APPL) ID(IZUUSER) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ID(IZUUSER) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/* Permit definitions for "Configuration Assistant" */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.CONFIGURATION_ASSISTANT.** CLASS(ZMFAPLA)
ID(IZUUSER) ACCESS(READ)"

/*-----*/
/*                                          */
/*  End "zOSMF User Role" Setup            */
/*                                          */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"
```

Figure 75. Sample RACF commands for configuring the Configuration Assistant plug-in (Part 1 of 2)

```

/*-----*/
/*                                          */
/*  Begin "zOSMF Administrator Role" Setup  */
/*                                          */
/*-----*/

Call RacfCmd "PERMIT IZUDFLT CLASS(APPL) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.izuUsers CLASS(EJBROLE) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Permit definitions for "Configuration Assistant" */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.CONFIGURATION_ASSISTANT.** CLASS(ZMFAPLA)
ID(IZUADMIN) ACCESS(READ)"

/*-----*/
/*                                          */
/*  End "zOSMF Administrator Role" Setup    */
/*                                          */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"

/*-----*/
/*                                          */
/*  Begin "zOS Security Administrator Role" Setup  */
/*                                          */
/*-----*/

/* No security setup procedure is required. */

/*-----*/
/*                                          */
/*  End "zOS Security Administrator Role" Setup    */
/*                                          */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"
/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"

/* Exit with maximum return code from RACF commands. */

```

Figure 76. Sample RACF commands for configuring the Configuration Assistant plug-in (Part 2 of 2)

Commands for configuring the Incident Log plug-in

If your installation configures the Incident Log plug-in, the REXX exec `izuconfig1.cfg.add.rexx` includes authorizations for the Incident Log task, as shown in the following figures:

- Figure 77
- Figure 78 on page 313
- Figure 79 on page 314.

```
/*-----*/
/*  Begin "Incident Log" Setup                               */
/*-----*/

/*----- */
/* Setup for CIM Providers to use CEA for Incident Log        */
/*-----*/

/* Assumption SERVAUTH class is active */
Call RacfCmd "SETROPTS GENERIC(SERVAUTH)"

/* Define the CEA resource profiles required to perform/retrieve */
/* properties for JES.                                         */
Call RacfCmd "RDEFINE SERVAUTH CEA.CEAGETPS UACC(NONE)"
Call RacfCmd "RDEFINE SERVAUTH CEA.CEADOCMD UACC(NONE)"

/* Grant the z/OSMF groups, authority to the following and to grant access */
/* to perform JES operations and obtain job properties.          */
Call RacfCmd "PERMIT CEA.CEAGETPS CLASS(SERVAUTH) ID(IZUADMIN) ACCESS(UPDATE)"
Call RacfCmd "PERMIT CEA.CEAGETPS CLASS(SERVAUTH) ID(IZUUSER) ACCESS(UPDATE)"
Call RacfCmd "PERMIT CEA.CEADOCMD CLASS(SERVAUTH) ID(IZUADMIN) ACCESS(UPDATE)"
Call RacfCmd "PERMIT CEA.CEADOCMD CLASS(SERVAUTH) ID(IZUUSER) ACCESS(UPDATE)"

/* Permit z/OSMF groups to Incident Log */
Call RacfCmd "RDEFINE SERVAUTH CEA.CEAPDWB* UACC(NONE)"
Call RacfCmd "PERMIT CEA.CEAPDWB* CLASS(SERVAUTH) ID(IZUADMIN) ACCESS(UPDATE)"
Call RacfCmd "PERMIT CEA.CEAPDWB* CLASS(SERVAUTH) ID(IZUUSER) ACCESS(UPDATE)"
Call RacfCmd "RDEFINE SERVAUTH CEA.CEADOCONSOLECMD UACC(NONE)"
Call RacfCmd "PERMIT CEA.CEADOCONSOLECMD CLASS(SERVAUTH) ID(IZUADMIN) ACCESS(UPDATE)"
Call RacfCmd "PERMIT CEA.CEADOCONSOLECMD CLASS(SERVAUTH) ID(IZUUSER) ACCESS(UPDATE)"

/* Activate authority checking for the SERVAUTH class: */
Call RacfCmd "SETROPTS RACLIST(SERVAUTH) CLASSACT(SERVAUTH)"

/* If the SERVAUTH class already active, issue: */
Call RacfCmd "SETROPTS RACLIST(SERVAUTH) REFRESH"
```

Figure 77. Sample RACF commands for configuring the Incident Log plug-in (Part 1 of 3)

```

/* If your installation sets up PROTECT-ALL (RACF exit to protect all datasets) */
/* you will need to setup a CEA.* RACF profile and permit user identity. */
/* The HLQ CEA is the CEA HLQ provided during the configuration prompts. */
/* */
/* Please ensure the commands are appropriate for your environment. */

/* You may want to consider assigning an owner or group to the data set profile. */
/* The commands is: */
/* Call RacfCmd "ADDSD 'CEA.*' OWNER(userid or group-name) UACC(NONE)" */
Call RacfCmd "ADDSD 'CEA.*' UACC(NONE)"
Call RacfCmd "PERMIT 'CEA.*' ID(IZUADMIN) ACCESS(ALTER)"
Call RacfCmd "PERMIT 'CEA.*' ID(IZUUSER) ACCESS(ALTER)"
Call RacfCmd "SETROPTS GENERIC(DATASET) REFRESH"

/* ----- */
/* Additional considerations */
/* ----- */
/* If your installation has user catalog setup instead of using the */
/* master catalog, you may need to define CEA alias to the user */
/* catalog. */
/* Call RacfCmd "DEFINE ALIAS(NAME(CEA) RELATE('your_catalog_name'))"

/* If your installation has master catalog setup you may need to permit the */
/* user to the master catalog dataset class. */
/* Call RacfCmd "PERMIT 'your_master_catalog' CLASS(DATASET) */
/* ID('your_cim_admin_name') ACCESS(UPDATE)" */
/* Call RacfCmd "SETROPTS GENERIC(DATASET) REFRESH"

/* If your installation is using SYSLOG for the Operations Log, you may need to */
/* define and permit the CEA user id to JESSPOOL class below. */
/* REDEFINE JESSPOOL 'your_system_name'.+MASTER+.SYSLOG.*.* UACC(NONE) */
/* PERMIT 'your_system_name'.+MASTER+.SYSLOG.*.* CLASS(JESSPOOL) */
/* ID('your_cea_user_id') ACC(READ) */
/* SETR RACLIST(JESSPOOL) REFRESH

/* If your installation protects MVS commands with RACF class OPERCMDS */
/* you need to give the CIM Admin identity permission. This is required */
/* for the incident log verify step. */
/* This template does not have RDEFINES for these resources. */
/* If your installation doesn't define these, you will need to either */
/* define them first or change the PERMIT to a higher level qualifier. */
/* Call RacfCmd "PERMIT MVS.DISPLAY.*.* CLASS(OPERCMDS) */
/* ID('your_cim_admin_name') ACCESS(READ)" */
/* Call RacfCmd "PERMIT MVS.DUMP CLASS(OPERCMDS) */
/* ID('your_cim_admin_name') ACCESS(CONTROL)" */
/* Call RacfCmd "PERMIT MVS.MODIFY.JOB.CEA CLASS(OPERCMDS) */
/* ID('your_cim_admin_name') ACCESS(UPDATE)" */
/* Call RacfCmd "SETROPTS RACLIST(OPERCMDS) REFRESH"

/* Profile Definitions for "Incident Log" */
Call RacfCmd "RDEFINE ZMFAPLA IZUDFLT.ZOSMF.INCIDENT_LOG.*.* UACC(NONE)"

/*-----*/
/* End "Incident Log" Setup */
/*-----*/

/*-----*/
/* Begin "zOSMF User Role" Setup */
/*-----*/

Call RacfCmd "PERMIT IZUDFLT CLASS(APPL) ID(IZUUSER) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ID(IZUUSER) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/* Permit definitions for "Incident Log" */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.INCIDENT_LOG.*.* CLASS(ZMFAPLA) */
ID(IZUUSER) ACCESS(READ)"

/*-----*/
/* End "zOSMF User Role" Setup */
/*-----*/

```

Figure 78. Sample RACF commands for configuring the Incident Log plug-in (Part 2 of 3)

```

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"

/*-----*/
/* Begin "zOSMF Administrator Role" Setup */
/*-----*/

Call RacfCmd "PERMIT IZUDFLT CLASS(APPL) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.*izuUsers CLASS(EJBROLE) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Permit definitions for "Incident Log" */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.INCIDENT_LOG.** CLASS(ZMFAPLA)
ID(IZUADMIN) ACCESS(READ)"

/*-----*/
/* End "zOSMF Administrator Role" Setup */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"

/*-----*/
/* Begin "zOS Security Administrator Role" Setup */
/*-----*/

/* No security setup procedure is required. */

/*-----*/
/* End "zOS Security Administrator Role" Setup */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"
/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"

/* During the z/OSMF configuration process, your installation selected */
/* one or more CIM dependent plug-in(s). As a result, your security */
/* administrator must ensure that the z/OSMF Administrator has the proper */
/* access to CIM resources. It is assumed that the CIM security */
/* job (CFZSEC), or equivalent, was run as part of the initial */
/* configuration for CIM. */

/* Connect the started task USERID to the CIM USER group */
Call RacfCmd "CONNECT (IZUSVR) GROUP(CFZUSRGP)"

/* Exit with maximum return code from RACF commands. */

```

Figure 79. Sample RACF commands for configuring the Incident Log plug-in (Part 3 of 3)

Commands for configuring the ISPF plug-in

If your installation configures the ISPF plug-in, the REXX exec **izuconfig1.cfg.add.rexx** includes authorizations for the ISPF task, as shown in the following figures:

- Figure 80
- Figure 81 on page 316.

```
/*-----*/
/*  Begin "ISPF" Setup                                */
/*-----*/

/* Assumption: SERVAUTH class is active */
/* Call RacfCmd "SETROPTS GENERIC(SERVAUTH)" */

/* Profile Definitions for "ISPF" */
Call RacfCmd "RDEFINE ZMFAPLA IZUDFLT.ZOSMF.ISPF.** UACC(NONE)"

/*-----*/
/*  End "ISPF" Setup                                */
/*-----*/

/*-----*/
/*  Begin "zOSMF User Role" Setup                    */
/*-----*/

Call RacfCmd "PERMIT IZUDFLT CLASS(APPL) ID(IZUUSER) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ID(IZUUSER) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/* Permit definitions for "ISPF" */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.ISPF.** CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/*-----*/
/*  End "zOSMF User Role" Setup                    */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"
```

Figure 80. Sample RACF commands for configuring the ISPF plug-in (Part 1 of 2)

```

/*-----*/
/* Begin "zOSMF Administrator Role" Setup */
/*-----*/

Call RacfCmd "PERMIT IZUDFLT CLASS(APPL) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Permit definitions for "ISPF" */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.ISPF.** CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/*-----*/
/* End "zOSMF Administrator Role" Setup */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"

/*-----*/
/* Begin "zOS Security Administrator Role" Setup */
/*-----*/

/* No security setup procedure is required. */

/*-----*/
/* End "zOS Security Administrator Role" Setup */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"
/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"

/* Exit with maximum return code from RACF commands. */

```

Figure 81. Sample RACF commands for configuring the ISPF plug-in (Part 2 of 2)

Commands for configuring the Resource Monitoring plug-in

If your installation configures the Resource Monitoring plug-in, the REXX exec **izuconfig1.cfg.add.rexx** includes authorizations for the Resource Monitoring task and the System Status task, as shown in the following figures:

- Figure 82
- Figure 83 on page 318

```
/*-----*/
/*                                          */
/*   Begin "Resource Monitoring" Setup    */
/*                                          */
/*-----*/

/* Profile Definitions for "Resource Monitoring" */
Call RacfCmd "RDEFINE ZMFAPLA IZUDFLT.ZOSMF.RESOURCE_MONITORING.** UACC(NONE)"

/*-----*/
/*                                          */
/*   End "Resource Monitoring" Setup      */
/*                                          */
/*-----*/

/*-----*/
/*                                          */
/*   Begin "zOSMF User Role" Setup       */
/*                                          */
/*-----*/

Call RacfCmd "PERMIT IZUDFLT CLASS(APPL) ID(IZUUSER) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ID(IZUUSER) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/* Permit definitions for "Resource Monitoring" */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.RESOURCE_MONITORING.** CLASS(ZMFAPLA)
ID(IZUUSER) ACCESS(READ)"

/*-----*/
/*                                          */
/*   End "zOSMF User Role" Setup         */
/*                                          */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"
```

Figure 82. Sample RACF commands for configuring the Resource Monitoring plug-in (Part 1 of 2)

```

/*-----*/
/*                                          */
/*  Begin "zOSMF Administrator Role" Setup  */
/*                                          */
/*-----*/

Call RacfCmd "PERMIT IZUDFLT CLASS(APPL) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Permit definitions for "Resource Monitoring" */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.RESOURCE_MONITORING.** CLASS(ZMFAPLA)
ID(IZUADMIN) ACCESS(READ)"

/*-----*/
/*                                          */
/*  End "zOSMF Administrator Role" Setup    */
/*                                          */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"

/*-----*/
/*                                          */
/*  Begin "zOS Security Administrator Role" Setup  */
/*                                          */
/*-----*/

/* No security setup procedure is required. */

/*-----*/
/*                                          */
/*  End "zOS Security Administrator Role" Setup    */
/*                                          */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"
/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"

/* Exit with maximum return code from RACF commands. */

```

Figure 83. Sample RACF commands for configuring the Resource Monitoring plug-in (Part 2 of 2)

Commands for configuring the Software Deployment plug-in

If your installation configures the Software Deployment plug-in, the REXX exec `izuconfig1.cfg.add.rexx` includes authorizations for the Software Management task, as shown in the following figures:

- Figure 84
- Figure 85 on page 320.

The exec includes RACF commands for controlling user access to the Software Management task and its objects, as described in “Creating access controls for the Software Management task” on page 115.

```
/*-----*/
/*  Begin "Software Deployment" Setup                                */
/*-----*/

/*  Profile Definitions for "Software Deployment" */
Call RacfCmd "RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SOFTWARE_DEPLOYMENT.** UACC(NONE) "

Call RacfCmd "RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.** UACC(NONE) "

Call RacfCmd "RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.PRODUCT_INFO_FILE.* UACC(NONE) "

/*-----*/
/*  End "Software Deployment" Setup                                */
/*-----*/

/*-----*/
/*  Begin "zOSMF User Role" Setup                                  */
/*-----*/

Call RacfCmd "PERMIT IZUDFLT CLASS(APPL) ID(IZUUSER) ACCESS(READ) "
Call RacfCmd "PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ID(IZUUSER) ACCESS(READ) "
Call RacfCmd "PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ) "

/*  Permit definitions for "Software Deployment" */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.SOFTWARE_DEPLOYMENT.** CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ) "
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.** CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(CONTROL) "

/*-----*/
/*  End "zOSMF User Role" Setup                                  */
/*-----*/

/*  Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY) "
```

Figure 84. Sample RACF commands for configuring the Software Deployment plug-in (Part 1 of 2)

```

/*-----*/
/* Begin "zOSMF Administrator Role" Setup */
/*-----*/

Call RacfCmd "PERMIT IZUDFLT CLASS(APPL) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Permit definitions for "Software Deployment" */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.SOFTWARE_DEPLOYMENT.** CLASS(ZMFAPLA)
ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.** CLASS(ZMFAPLA)
ID(IZUADMIN) ACCESS(CONTROL)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.PRODUCT_INFO_FILE.*
CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/*-----*/
/* End "zOSMF Administrator Role" Setup */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"

/*-----*/
/* Begin "zOS Security Administrator Role" Setup */
/*-----*/

/* No security setup procedure is required. */

/*-----*/
/* End "zOS Security Administrator Role" Setup */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"
/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"

/* Exit with maximum return code from RACF commands. */

```

Figure 85. Sample RACF commands for configuring the Software Deployment plug-in (Part 2 of 2)

Commands for configuring the Workload Management plug-in

If your installation configures the Workload Management plug-in, the REXX exec **izuconfig1.cfg.add.rexx** includes authorizations for the Workload Management task, as shown in the following figures:

- Figure 86
- Figure 87 on page 322
- Figure 88 on page 323.

The exec includes RACF commands for granting the Workload Management task access to the WLM couple data set, and for connecting the z/OSMF started task user ID to the CIM user group, as described in “Updating z/OS for the Workload Management plug-in” on page 123.

```
/*-----*/
/*  Begin "Workload Management" Setup                               */
/*-----*/

/* Define Workload Management facility */

/* The following commented command is to be issued only if the profile does not exist */
/* It normally would have been created during z/OS setup                               */
/* Call RacfCmd "RDEFINE FACILITY MVSADMIN.WLM.POLICY UACC(NONE)"                      */

/* Permit the Workload Management group */
Call RacfCmd "PERMIT MVSADMIN.WLM.POLICY CLASS(FACILITY) ID(WLMGRP) ACCESS(UPDATE)"

/* Permit the started task userid USERID */
Call RacfCmd "PERMIT MVSADMIN.WLM.POLICY CLASS(FACILITY) ID(IZUSVR) ACCESS(READ)"

/* Make changes effective */
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"

/* Profile Definitions for "Workload Management" */
Call RacfCmd
"RDEFINE ZMFAPLA IZUDFLT.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.VIEW UACC(NONE)"

Call RacfCmd
"RDEFINE ZMFAPLA IZUDFLT.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.MODIFY UACC(NONE)"

Call RacfCmd
"RDEFINE ZMFAPLA IZUDFLT.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.INSTALL UACC(NONE)"

/*-----*/
/*  End "Workload Management" Setup                               */
/*-----*/
```

Figure 86. Sample RACF commands for configuring the Workload Management plug-in (Part 1 of 3)

```

/*-----*/
/*  Begin "zOSMF User Role" Setup                               */
/*-----*/

Call RacfCmd "PERMIT IZUDFLT CLASS(APPL) ID(IZUUSER) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ID(IZUUSER) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/* Permit definitions for "Workload Management" */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.VIEW
CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)"

/*-----*/
/*  End "zOSMF User Role" Setup                               */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"

/*-----*/
/*  Begin "zOSMF Administrator Role" Setup                     */
/*-----*/

Call RacfCmd "PERMIT IZUDFLT CLASS(APPL) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/* Permit definitions for "Workload Management" */
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.VIEW
CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.MODIFY
CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"
Call RacfCmd "PERMIT IZUDFLT.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.INSTALL
CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)"

/*-----*/
/*  End "zOSMF Administrator Role" Setup                     */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"

```

Figure 87. Sample RACF commands for configuring the Workload Management plug-in (Part 2 of 3)

```

/*-----*/
/*  Begin "zOS Security Administrator Role" Setup      */
/*-----*/

/* No security setup procedure is required. */

/*-----*/
/*  End "zOS Security Administrator Role" Setup      */
/*-----*/

/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"
/* Need to REFRESH these classes for Roles */
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"
Call RacfCmd "SETROPTS RACLIST(ZMFAPLA) REFRESH"
Call RacfCmd "SETROPTS RACLIST(SERVER) REFRESH"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
Call RacfCmd "SETROPTS RACLIST(FACILITY) GENERIC(FACILITY)"

/* During the z/OSMF configuration process, your installation selected */
/* one or more CIM dependent plug-in(s). As a result, your security */
/* administrator must ensure that the z/OSMF Administrator has the proper */
/* access to CIM resources. It is assumed that the CIM security */
/* job (CFZSEC), or equivalent, was run as part of the initial */
/* configuration for CIM. */

/* Connect the started task USERID to the CIM USER group */
Call RacfCmd "CONNECT (IZUSVR) GROUP(CFZUSRGP)"

/* Exit with maximum return code from RACF commands. */

```

Figure 88. Sample RACF commands for configuring the Workload Management plug-in (Part 3 of 3)

Appendix G. Format of the installation verification program report

When you use the **izusetup.sh** script to verify the system setup for the Incident Log task, the installation verification program (IVP) report is created. For your reference, this section shows the format of the IVP report.

For a description of the IVP report, see “Reviewing the results of the `izuincidentlogverify.report` file” on page 198.

The format of the IVP report is shown in Figure 89, Figure 90 on page 326, and Figure 91 on page 327.

```
/* ----- */
/* Licensed Materials - Property of IBM          */
/* 5610-A01                                       */
/* Copyright IBM Corp. 2009, 2013                */
/*                                               */
/* Status = HSMA210                             */
/*                                               */
/* Information:                                  */
/*                                               */
/* SID=%I%                                       */
/* Delta Date=%G%                               */
/* Delta Time=%U%                               */
/*                                               */
/* ----- */

User ID: IBMUSER
Date: 03.02.13
Time: 23.01.31

-----
Incident Log Verification Report
-----

To verify that your system is set-up correctly for the Incident Log task,
z/OSMF creates an SVC dump on the system and performs a series
of tests on the dump. For each test that is performed, this report shows
either "SUCCESS" or an error message that indicates a potential problem
in your set-up. For the possible corrective actions, see the troubleshooting
section of z/OSMF Configuration Guide.

The following section describes key dependencies for the Incident Log
task. A value of "SUCCESS" indicates that the dependency is configured
and active on the system.

Sysplex Dump Directory : SUCCESS
CEA                     : SUCCESS
System REXX             : SUCCESS
System Logger Active    : SUCCESS
```

Figure 89. Format of the installation verification program report (Part 1 of 3)

Diagnostic Data Results

Four diagnostic data objects are associated with an incident:
The SVC dump and three "log snapshots". A value of "SUCCESS" indicates that the diagnostic objects were found for the incident. Identified errors are described in the Troubleshooting chapter of z/OSMF Configuration Guide.

SVCDump : SUCCESS
Operations Log : SUCCESS
Error Log : SUCCESS
Error Log Summary : SUCCESS

Incident Log Operations Results

Each diagnostic object is "prepared", that is, formatted and tersed. Usually, each diagnostic object is prepared before the incident is sent to IBM through FTP. A value of "SUCCESS" indicates that the diagnostic information was prepared successfully. Identified errors are described in the Troubleshooting chapter of z/OSMF Configuration Guide.

Prepare Dump Request : SUCCESS
Prepare Operations Log Request : SUCCESS
Prepare Error Log Request : No diagnostic data available.
Prepare Error Log Summary Request : SUCCESS
Prepare View Operations Log Request : SUCCESS
Prepare View Error Log Request : SUCCESS
Prepare View Error Log Summary Request : SUCCESS
Set PMR Request : SUCCESS
Set Tracking Request : SUCCESS
Set User Comment Field Request : SUCCESS

CEA Parmlib Member

The common event adapter (CEA) component of z/OS captures diagnostic data objects. The following section describes the relevant properties in the active CEAPRMxx parmliib member. Identified errors are described in the Troubleshooting chapter of z/OSMF Configuration Guide.

SnapShot : Y
Branch : 000
Country : 000
Storage Value : AUXPK1
HLQ : CEA

SLIP OperLog time : 1800
SLIP LOGREC time : 3600
SLIP LOGRECSUMMARY time : 14400
DUMP OperLog time : 1800
DUMP LOGREC time : 3600
DUMP LOGRECSUMMARY time : 14400
ABEND OperLog time : 1800
ABEND LOGREC time : 3600
ABEND LOGRECSUMMARY time : 14400

Figure 90. Format of the installation verification program report (Part 2 of 3)

Incident Log Logstreams Properties

OPERLOG and sysplex logrec diagnostic snapshots are written to system logger log streams. The following section describes the log stream properties expected to be active on the system. Identified errors are described in the Troubleshooting chapter of z/OSMF Configuration Guide.

Operations Log : OPERLOG
Logrec : LOGSTREAM
LOGR Subsystem Active : TRUE
Primary Logger CDS : "CIMPROV.LOGR001"
Alternate Logger CDS : "CIMPROV.LOGR002"
Number of LSR for Primary CDS : 60
CEA OperLog Logstream Model : "CEA.MODEL.OPERLOG"
CEA Logrec Logstream Model : "CEA.MODEL.LOGREC"

Sysplex Dump Directory Properties

The sysplex dump directory contains the inventory of SVC dumps that are described by z/OSMF incidents. The following section describes the sysplex dump directory that is active on the z/OS system. Identified errors are described in the Troubleshooting chapter of z/OSMF Configuration Guide.

Name :
Size : cylinders
On Shared Volume : TRUE
Free Space Available : TRUE
IPCS Initialized : TRUE

Figure 91. Format of the installation verification program report (Part 3 of 3)

Appendix H. Example of the migration report

When you use the **izumigration.sh** script to migrate your configuration file to the latest format, the script creates a report file named **izumigration.report**. The report file records the actions that were taken to migrate your configuration and override files—the settings that have been modified, removed, or added between releases. For your reference, this section shows a sample of the migration report file.

The following example shows the major sections of the migration report file. In this example, the report file records the results of updating the configuration file and the override file from the z/OSMF V1R13 format to the z/OSMF V2R1 format.

The sample migration report is presented in a multi-part figure, as follows:

- Figure 92 on page 330
- Figure 93 on page 331
- Figure 94 on page 332
- Figure 95 on page 333.

```

/*-----*/
Invocation command: ./izumigrate.sh -file /u/in2/izudflt.R13.cfg

User ID: IBMUSER
Date: 07.30.13
Time: 01.37.30

The following environment variables were in effect during the creation
of this report file:

IZU_CODE_ROOT=/usr/lpp/zosmf/V2R1
IZU_CONFIG_DIR=/u/current_config
IZU_LOGFILE_DIR=/var/zosmf/configuration/logs

/*-----*/
/*-----*/

Configuration File Processing
-----
Previous configuration file was saved as: "/u/in2/izudflt.R13.cfg.V1R13"

Updated configuration file was created as: "/u/in2/izudflt.R13.cfg"

The complete list of properties contained in the default configuration file for the current release of z/OSMF are:

IZU_CONFIG_FILE_VERSION=2.1.0
IZU_DATA_DIR=/var/zosmf/data
IZU_DATA_FS_NAME=IZU.SIZUDATA
IZU_DATA_FS_TYPE=ZFS
IZU_DATA_FS_VOLUME='*'
IZU_DATA_FS_SIZE=200
IZU_AUTOUID_OVERRIDE=NO.DEFAULT.VALUE
IZU_AUTOGID_OVERRIDE=NO.DEFAULT.VALUE
IZU_ADMIN_GROUP_NAME=IZUADMIN
IZU_ADMIN_GROUP_GID=9003
IZU_USERS_GROUP_NAME=IZUUSER
IZU_USERS_GROUP_GID=9004
IZU_HTTP_SSL_PORT=32208
IZU_APPSERVER_HOSTNAME=NO.DEFAULT.VALUE
IZU_CIM_ADMIN_GROUP_NAME=CFZADMGP
IZU_CIM_USER_GROUP_NAME=CFZUSRGP
IZU_ZOS_SECURITY_ADMIN_GROUP_NAME=IZUSECAD
IZU_ZOS_SECURITY_ADMIN_GROUP_GID=9006
IZU_UNAUTHENTICATED_GROUP_NAME=IZUUNGRP
IZU_UNAUTHENTICATED_GROUP_GID=9012
IZU_CA_CONFIGURE=NO.DEFAULT.VALUE
IZU_CP_CONFIGURE=NO.DEFAULT.VALUE
IZU_CP_QUERY_GROUP_NAME=CPOQUERY
IZU_CP_CONTROL_GROUP_NAME=CPOCTRL
IZU_DM_CONFIGURE=NO.DEFAULT.VALUE
IZU_IL_CONFIGURE=NO.DEFAULT.VALUE
IZU_IL_CEA_CONFIGURE=Y
IZU_CEA_HLQ='CEA'
IZU_COUNTRY_CODE=NO.DEFAULT.VALUE
IZU_BRANCH_CODE=NO.DEFAULT.VALUE
IZU_STORAGE_VALUE=NO.DEFAULT.VALUE
IZU_CEAPRM_SOURCE_PARMLIB=SYS1.PARMLIB
IZU_CEAPRM_TARGET_PARMLIB=SYS1.PARMLIB
IZU_IADMC_SOURCE_PARMLIB=SYS1.SAMPLIB
IZU_IADMC_TARGET_PARMLIB=SYS1.PARMLIB
IZU_CEA_PARM_NAME=01
IZU_IEA_PARM_NAME=ZM
IZU_WISPF_CONFIGURE=NO.DEFAULT.VALUE
IZU_RMF_CONFIGURE=NO.DEFAULT.VALUE
IZU_WLM_CONFIGURE=NO.DEFAULT.VALUE
IZU_WLM_GROUP_NAME=WLMGRP

```

Figure 92. Sample migration report file (Part 1 of 4)

```

Plug-in Configuration Property
-----
Configuration Assistant = IZU_CA_CONFIGURE
Incident Log            = IZU_IL_CONFIGURE
Workload Management     = IZU_WLM_CONFIGURE
Resource Monitoring     = IZU_RMF_CONFIGURE
Capacity Provisioning   = IZU_CP_CONFIGURE
ISPF                   = IZU_WISPF_CONFIGURE
Software Deployment     = IZU_DM_CONFIGURE
/*-----*/

Removed Properties
-----
The following properties are removed from the updated configuration file.
These properties are no longer supported in the current release of z/OSMF.
In the list below, each property is shown with its value as specified in
the previous configuration file. This value is either an installation
supplied value, if one was specified, or the IBM default value.

IZU_SMS_CONFIGURE=
IZU_STORAGE_GROUP_NAME=
IZU_STORAGE_GROUP_GID=
IZU_AUTHORIZATION_MODE=SAF
IZU_WAS_CONFIG_FILE_KNOWN=Y
IZU_WAS_CONFIG_FILE_LOCATION=/etc/zWebSphereOEM/V7R0/conf/CONFIG1/CONFIG1.responseFile
IZU_APPSERVER_GROUP=WSCFG1
IZU_APPSERVER_ROOT=/zWebSphereOEM/V7R0/config1
IZU_WAS_PROFILE_PREFIX=BBNBASE
IZU_CLUSTER_TRANSITION_NAME=BBNC001
IZU_CELL_SHORT_NAME=BBNBASE
IZU_CONTROL_USERID=WSCRUI
IZU_SERVANT_USERID=WSSRUI
IZU_ORB_PORT=32203
IZU_WBEM_ROOT=/usr/lpp/wbem
IZU_ADMIN_NAME=ZOSMFAD
IZU_ADMIN_UID=9001
IZU_ADMIN_HOME=/u/zosmfad
IZU_ADMIN_PROGRAM=/bin/sh
IZU_ADMIN_PROC=NO.DEFAULT.VALUE
IZU_ADMIN_ACCOUNT=NO.DEFAULT.VALUE

Added Properties
-----
The following properties are added to the updated configuration file.
These properties are new for z/OSMF since the time of your last
configuration. In the list below, each property is shown with its
IBM default value, unless a value from your previous configuration applies
to an added property. In this case, your value is used in its place.

IZU_ZOS_SECURITY_ADMIN_GROUP_NAME=IZUSECAD
IZU_ZOS_SECURITY_ADMIN_GROUP_GID=9006
IZU_UNAUTHENTICATED_GROUP_NAME=IZUUNGRP
IZU_UNAUTHENTICATED_GROUP_GID=9012
IZU_STARTED_TASK_USERID_NAME=IZUSVR
IZU_STARTED_TASK_USERID_UID=9010
IZU_STARTED_TASK_HOME=/var/zosmf/data/home/izusvr
IZU_STARTED_TASK_PROGRAM=/bin/sh
IZU_SAF_PROFILE_PREFIX=IZUDFLT
IZU_DEFAULT_CERTAUTH=Y
IZU_UNAUTHENTICATED_NAME=IZUGUEST
IZU_UNAUTHENTICATED_UID=9011
IZU_HTTP_PORT=80

Updated Properties
-----
The following properties have been updated in the configuration file for the
current release.

IZU_CONFIG_FILE_VERSION=2.1.0

/*-----*/

The migration of the configuration file has completed.

/*-----*/

```

Figure 93. Sample migration report file (Part 2 of 4)

```

/*-----*/
Invocation command: ./izumigrate.sh -overridefile /u/in/R13.izudflt.ovr

User ID: IBMUSER
Date: 08.08.13
Time: 07.37.43

The following environment variables were in effect during the creation
of this report file:

IZU_CODE_ROOT=/usr/lpp/zosmf/V2R1

IZU_CONFIG_DIR=/u/current_config

IZU_LOGFILE_DIR=/var/zosmf/configuration/logs

/*-----*/
/*-----*/

Override File Processing
-----
Previous override file was saved as: "/u/in/R13.izudflt.ovr.V1R13"

Updated override file was created as: "/u/in/R13.izudflt.ovr"

The complete list of properties contained in the default override file for the current release of z/OSMF are:

IZU_OVERRIDE_FILE_VERSION=2.1.0
IZU_DATA_DIR=/var/zosmf/data
IZU_DATA_FS_NAME=IZU.SIZUDATA
IZU_DATA_FS_TYPE=ZFS
IZU_DATA_FS_VOLUME='*'
IZU_DATA_FS_SIZE=200
IZU_AUTOUID_OVERRIDE=NO.DEFAULT.VALUE
IZU_AUTOGID_OVERRIDE=NO.DEFAULT.VALUE
IZU_ADMIN_GROUP_NAME=IZUADMIN
IZU_ADMIN_GROUP_GID=9003
IZU_USERS_GROUP_NAME=IZUUSER
IZU_USERS_GROUP_GID=9004
IZU_HTTP_SSL_PORT=32208
IZU_APPSERVER_HOSTNAME=NO.DEFAULT.VALUE
IZU_CIM_ADMIN_GROUP_NAME=CFZADMGP
IZU_CIM_USER_GROUP_NAME=CFZUSRGP
IZU_ZOS_SECURITY_ADMIN_GROUP_NAME=IZUSECAD
IZU_ZOS_SECURITY_ADMIN_GROUP_GID=9006
IZU_UNAUTHENTICATED_GROUP_NAME=IZUUNGRP
IZU_UNAUTHENTICATED_GROUP_GID=9012
IZU_CA_CONFIGURE=NO.DEFAULT.VALUE
IZU_CP_CONFIGURE=NO.DEFAULT.VALUE
IZU_CP_QUERY_GROUP_NAME=CPOQUERY
IZU_CP_CONTROL_GROUP_NAME=CPOCTRL
IZU_DM_CONFIGURE=NO.DEFAULT.VALUE
IZU_IL_CONFIGURE=NO.DEFAULT.VALUE
IZU_IL_CEA_CONFIGURE=Y
IZU_CEA_HLQ='CEA'
IZU_COUNTRY_CODE=NO.DEFAULT.VALUE
IZU_BRANCH_CODE=NO.DEFAULT.VALUE
IZU_STORAGE_VALUE=NO.DEFAULT.VALUE
IZU_CEAPRM_SOURCE_PARMLIB=SYS1.PARMLIB
IZU_CEAPRM_TARGET_PARMLIB=SYS1.PARMLIB
IZU_IADMC_SOURCE_PARMLIB=SYS1.SAMPLIB
IZU_IADMC_TARGET_PARMLIB=SYS1.PARMLIB
IZU_CEA_PARM_NAME=01
IZU_IEA_PARM_NAME=ZM
IZU_WISPF_CONFIGURE=NO.DEFAULT.VALUE
IZU_RMF_CONFIGURE=NO.DEFAULT.VALUE
IZU_WLM_CONFIGURE=NO.DEFAULT.VALUE
IZU_WLM_GROUP_NAME=WLMGRP
IZU_STARTED_TASK_USERID_NAME=IZUSVR
IZU_STARTED_TASK_USERID_UID=9010
IZU_STARTED_TASK_HOME=/var/zosmf/data/home/izusvr
IZU_STARTED_TASK_PROGRAM=/bin/sh

```

Figure 94. Sample migration report file (Part 3 of 4)


```

IZU_SAF_PROFILE_PREFIX=IZUDFLT
IZU_DEFAULT_CERTAUTH=Y
IZU_UNAUTHENTICATED_NAME=IZUGUEST
IZU_UNAUTHENTICATED_UID=9011
IZU_HTTP_PORT=80

```

If a property was removed from the current release of z/OSMF and it was found in your override file, the migration process will remove that property from your override file.

If a property has been added to the current release of z/OSMF and it corresponds to a property in your override file, that property will be added to your override file with your existing value.

Plug-in Configuration Property

```

-----
Configuration Assistant = IZU_CA_CONFIGURE
Incident Log           = IZU_IL_CONFIGURE
Workload Management    = IZU_WLM_CONFIGURE
Resource Monitoring    = IZU_RMF_CONFIGURE
Capacity Provisioning  = IZU_CP_CONFIGURE
ISPF                   = IZU_WISPF_CONFIGURE
Software Deployment    = IZU_DM_CONFIGURE

```

```
/*-----*/
```

```
/*-----*/
```

Removed Properties

The following properties have been removed from the override file for the current release and are no longer supported. The properties are displayed with their default values unless a corresponding value was found in your override file. In this case, your value is used in its place.

```

IZU_SMS_CONFIGURE=NO.DEFAULT.VALUE
IZU_STORAGE_GROUP_NAME=IZUSTGA
IZU_STORAGE_GROUP_GID=9005
IZU_ADMIN_NAME=ZOSMFAD
IZU_ADMIN_UID=9001
IZU_ADMIN_HOME=/u/zosmfad
IZU_ADMIN_PROGRAM=/bin/sh
IZU_ADMIN_PROC=NO.DEFAULT.VALUE
IZU_ADMIN_ACCOUNT=NO.DEFAULT.VALUE

```

Added Properties

The following properties have been added to the override file for the current release. The properties are displayed with their default values unless a corresponding value was found in your override file. In this case, your value is used in its place.

```

IZU_ZOS_SECURITY_ADMIN_GROUP_NAME=IZUSECAD
IZU_ZOS_SECURITY_ADMIN_GROUP_GID=9006
IZU_UNAUTHENTICATED_GROUP_NAME=IZUUNGRP
IZU_UNAUTHENTICATED_GROUP_GID=9012

```

Updated Properties

The following properties have been updated in the override file for the current release:

```
IZU_OVERRIDE_FILE_VERSION=2.1.0
```

```
/*-----*/
```

The migration of the override file has completed.

```
/*-----*/
```

You can migrate your system to the new release of z/OSMF. Follow the steps described in the z/OSMF Configuration Guide to configure the new release of z/OSMF.

```
/*-----*/
```

Figure 95. Sample migration report file (Part 4 of 4)

Appendix I. Summary of message changes for z/OSMF V2R1

The 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.

New messages

The messages listed in the following table are new in z/OSMF V2R1.

Component	Messages that are new
Configuration process	IZUG101W IZUG333I IZUG334I IZUG361I IZUG362I IZUG363E IZUG364E IZUG366E IZUG367W IZUG368I IZUG369I IZUG398I
Core functions	IZUG408I IZUG409I IZUG440W IZUG473E IZUG474E IZUG476E IZUG477E IZUG505E IZUG509I IZUG510I IZUG511I IZUG512E IZUG570E IZUG588E IZUG612E IZUG613E IZUG614E IZUG630E IZUG631E IZUG648E IZUG649E IZUG650E IZUG671E IZUG679E IZUG845I IZUG846W IZUG1053E IZUG1054E IZUG1055E IZUG1056E IZUG1057E IZUG1058I IZUG1059E IZUG1060E IZUG1061E IZUG1062E IZUG1063E IZUG1064E IZUG1065E IZUG1066W IZUG1067E IZUG1068I IZUG1069E IZUG1070I IZUG1071E IZUG1072I IZUG1073E IZUG1074E IZUG1075W IZUG1076E IZUG1077E IZUG1078I IZUG1079I IZUG1100E IZUG1101E IZUG1102E IZUG1103W IZUG1104E IZUG1105E IZUG1106E IZUG1107E IZUG1109E IZUG1110E IZUG1111E IZUG1112E IZUG1113E IZUG1114E IZUG1115E IZUG1116E IZUG1117E IZUG1118E IZUG1119I IZUG1120E IZUG1121E IZUG1122E IZUG1123E IZUG1125E IZUG1126E IZUG1127E IZUG1128I IZUG1129I IZUG1130W IZUG1131I
Configuration Workflow	IZUG2001I IZUG2002I IZUG2003I IZUG2004I IZUG2005I IZUG2006I IZUG2007I IZUG2008I IZUG2009I IZUG2010I IZUG2011I IZUG2012I IZUG2014I IZUG2015I IZUG2016I IZUG2017I IZUG2018I IZUG2019I IZUG2020I IZUG2021I IZUG2022I IZUG2023I IZUG2024I IZUG2025I IZUG2026I IZUG2027I IZUG2028W IZUG2029I IZUG2030I IZUG2031I IZUG2032I IZUG2033I IZUG2035I IZUG2036I IZUG2037I IZUG2039I IZUG2040I IZUG2041I IZUG2042I IZUG2043I IZUG2044I IZUG2045I IZUG2046I IZUG2047I IZUG2048I IZUG2049I IZUG2050I IZUG2061E IZUG2062E IZUG2063E IZUG2064E IZUG2065E IZUG2068E IZUG2069E IZUG2070E IZUG2071E IZUG2072E IZUG2073E IZUG2074E IZUG2075E IZUG2077E IZUG2078E IZUG2079E IZUG2080E IZUG2081E IZUG2082E IZUG2083E IZUG2084E IZUG2085E IZUG2086E IZUG2087E IZUG2088E IZUG2089E IZUG2091W IZUG2092W IZUG2094W IZUG2096W IZUG2097W IZUG2099W IZUG2100W IZUG2105W IZUG2108E IZUG2109E IZUG2110E IZUG2111I IZUG2112I IZUG2113W IZUG2114W IZUG2115E IZUG2116I IZUG2117W IZUG2118W IZUG2120E IZUG2121I IZUG2122E IZUG2123I IZUG2124W IZUG2125W IZUG2129W IZUG2130I IZUG2131I IZUG2132I IZUG2133W IZUG2134E IZUG2135E IZUG2136I IZUG2137I IZUG2138I IZUG2139I IZUG2140I IZUG2141I IZUG2142I IZUG2143E IZUG2144W IZUG2145I IZUG2147I IZUG2148I IZUG2149I IZUG2150I IZUG2151I IZUG2152I IZUG2153I IZUG2154E IZUG2155I IZUG2156I IZUG2157W
Deployment task	IZUD168E IZUD242W IZUD243I IZUD784E IZUD785W IZUD786I IZUD787I IZUD788I IZUD9734I IZUD995E
Workflows task	IZUWF0104E IZUWF0105E IZUWF0106E IZUWF0107E IZUWF0108E IZUWF0138I IZUWF0142E IZUWF0143E IZUWF0144E IZUWF0145E IZUWF0146E IZUWF0147E IZUWF0148E IZUWF0149E IZUWF0150E IZUWF0151E IZUWF0152W IZUWF0153I IZUWF0154E IZUWF0155E IZUWF0156E IZUWF0157E IZUWF0158E IZUWF0159I IZUWF0160I IZUWF0161I IZUWF0162I IZUWF0163I IZUWF0164I IZUWF0165E IZUWF0166I IZUWF0167E IZUWF0168E IZUWF0169E IZUWF0170E IZUWF0171E IZUWF0172E IZUWF0173W
Workload Management task	IZUW021E

Changed messages

The following messages were changed in z/OSMF V2R1:

Component	Messages that are changed
Configuration process	IZUG011I IZUG033I IZUG133I IZUG134I IZUG137E IZUG262I IZUG263I IZUG264I IZUG265I IZUG266I IZUG267I IZUG268I IZUG279E IZUG311E IZUG320E IZUG321W IZUG333I IZUG334I IZUG335E IZUG336I IZUG345I IZUG346I IZUG349I IZUG364E IZUG365I IZUG378I IZUG379I IZUG385I IZUG398I
Core functions	IZUG360I IZUG502E IZUG505E IZUG560W IZUG580E IZUG581E IZUG586E IZUG587E IZUG590E IZUG591E IZUG592E IZUG593E IZUG626E IZUG861W IZUG2008I IZUG2109E
Incident Log task	IZUP162E IZUP606E
Workflows task	IZUWF0005E IZUWF0012E IZUWF0015E IZUWF0020I IZUWF0021I IZUWF0022I IZUWF0023I IZUWF0024I IZUWF0025I IZUWF0026I IZUWF0028I IZUWF0031E IZUWF0045I IZUWF0046I IZUWF0047I IZUWF0049I IZUWF0051I IZUWF0053E IZUWF0057I IZUWF0058I IZUWF0059I IZUWF0086E IZUWF0089W IZUWF0139E IZUWF0140E IZUWF0141E

Deleted messages

The messages listed in the following table are no longer issued by their respective components in z/OSMF V2R1.

Component	Messages no longer issued
Configuration	IZUG152I IZUG153I IZUG154I IZUG155E IZUG156E IZUG269I IZUG270I IZUG307I IZUG308I IZUG309I IZUG322W IZUG323E IZUG324E IZUG325E IZUG326E IZUG327E IZUG328E IZUG329E IZUG330E IZUG331E IZUG332I IZUG334E IZUG363I IZUG366I
Core functions	IZUG421I IZUG422I IZUG427I IZUG433I IZUG435I IZUG570W IZUG573E IZUG575E IZUG576E IZUG577E IZUG579E IZUG670E IZUG671E IZUG672E IZUG673E IZUG674E IZUG675E IZUG2004I IZUG2023I IZUG2028I IZUG2035I IZUG2074E IZUG2075E IZUG2081E IZUG2089E
Deployment task	IZUD995E

Appendix J. 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 mhvrdfs@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.

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.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

Site Counsel
IBM Corporation
2455 South Road
Poughkeepsie, NY 12601-5400
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

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: <http://www.ibm.com/software/support/systemsz/lifecycle/>
- For information about currently-supported IBM hardware, contact your IBM representative.

Programming interface information

This information documents intended programming interfaces that allow the customer to write programs to obtain the services of z/OS or IBM z/OS Management Facility.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com)[®] are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at <http://www.ibm.com/legal/copytrade.shtml>.

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Intel is a trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names might be trademarks or service marks of others.

Glossary of terms and abbreviations

This glossary defines technical terms and abbreviations used in z/OSMF help information. If you do not find the term you are looking for, refer to the IBM Glossary of Computing Terms. The following cross-references are used in this glossary:

- **Contrast with:** This refers to a term that has an opposed or substantively different meaning.
- **See:** This refers the reader to (a) a related term, (b) a term that is the expanded form of an abbreviation or acronym, or (c) a synonym or more preferred term.
- **Synonym for:** This indicates that the term has the same meaning as a preferred term, which is defined in its proper place in the glossary.
- **Synonymous with:** This is a reference from a defined term to all other terms that have the same meaning.
- **Obsolete term for:** This indicates that the term should not be used and refers the reader to the preferred term.

This glossary includes terms and definitions from American National Standard Dictionary for Information Systems, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Definitions are identified by an asterisk (*) that appears between the term and the beginning of the definition; a single definition taken from ANSI is identified by an asterisk after the item number for that definition.

A

abend See *abnormal end*.

abnormal end

The termination of a task, job, or subsystem because of an error condition that recovery facilities cannot resolve during execution.

active service policy

In the Workload Management task, the service policy that WLM uses to manage the workload on the system.

AIX A UNIX operating system developed by IBM that is designed and optimized to run on POWER® microprocessor-based hardware such as servers, workstations, and blades.

allow next dump

In the Incident Log task, the option to have dump analysis and elimination (DAE) take and report the next dump that occurs for the same symptoms.

alphabetic character

A letter or other symbol, excluding digits, used in a language.

alphanumeric character

Character set composed of uppercase and lowercase letters and numbers, not symbols.

APF Authorized program facility.

APF-authorized

Pertaining to a program that is authorized by the authorized program facility (APF) to access restricted functions, such as supervisor calls (SVC) or SVC paths.

application environment

In the Workload Management task, a group of application functions requested by a client that execute in server address spaces.

authentication

Verification of the identity of a user or the user's eligibility to access an object.

automatic control

In the Workload Management task, a method of managing application environments. Under automatic control, the name of the startup JCL procedure has been defined for an application environment, giving WLM the ability to automatically start server address spaces. Contrast with *manual control*.

B**batch job**

A predefined group of processing actions submitted to the system to be performed with little or no interaction between the user and the system.

C**catalog**

A directory of files and libraries, with reference to their locations.

category

A group of related z/OSMF tasks. Each task in a category allows you to address some aspect of the category.

In the Software Management task, a grouping of deployments and software instances that are related in some way. For example, software instances used by a particular business unit might be included in a single category.

CDS See *couple data set*.

central processing unit (CPU)

Synonymous with *processor*.

CIM server

See *Common Information Model server*.

class An object that contains specifications, such as priority, maximum processing time, and maximum storage, to control the runtime environment of a job.

Parameter on the JCL JOB statement that specifies the class or group to which to assign a job. Assigning jobs to a class helps to:

- Achieve a balance between different types of jobs. A good balance of job class assignments helps to make the most efficient use possible of the system.
- Avoid contention between jobs that use the same resources.

class file

A compiled Java source file.

classification

In the Workload Management task, the first level qualifier in the classification rules. A classification specifies the subsystem type that receives the work request and contains all of the classification rules for that subsystem.

classification rules

In the Workload Management task, the rules WLM and subsystems use to assign a service class and, optionally, a report class to a work request.

client A system or process that is dependent on another system or process (usually called the server) to provide it with access to data, services, programs, or resources. Contrast with *server*.

clone To preserve the characteristics of the original but personalize instance-specific data. The result is a new instance of an entity (for example, of a virtual disk, a virtual computer system, or an operating system) rather than a backup of the original.

code page

A particular assignment of code points to graphic characters. Within a given code page, a code point can have only one specific meaning. A code page also identifies how undefined code points are handled.

A specification of code points from a defined encoding structure for each graphic character in a set or in a collection of graphic character sets. Within a code page, a code point can have only one specific meaning.

common event adapter (CEA)

A z/OS component that enables the delivery of z/OS management data to clients, such as the CIM server.

Common Information Model (CIM)

An implementation-neutral, object-oriented schema for describing network management information. The Distributed Management Task Force (DMTF) develops and maintains CIM specifications.

An open standard for systems management that defines the exchange of information between managed elements such as systems, networks, applications, and services.

Common Information Model Object Manager (CIMOM)

The common conceptual framework for data management that receives, validates, and authenticates the Common Information Model (CIM) requests from the client application. It then directs the requests to the appropriate component or service provider. Synonymous with *Common Information Model server*.

Common Information Model server (CIM server)

Software, such as OpenPegasus, that allows use of the CIM standard on a system.

An object management engine that exists between the managed system and the management product. z/OSMF interacts with the CIM server (or similar technology) through a layer that converts the data from the CIM model to a format that is usable by the z/OSMF tasks.

Synonymous with *Common Information Model Object Manager*.

component

A set of modules that performs a major function within a system.

component ID

Alphanumeric identifier that uniquely identifies the z/OS component.

content area

In a web page that is based on a page template, the editable region of the page.

Area of the z/OSMF browser interface (the central pane) in which data for the active task is displayed.

core functions

The base functions of z/OSMF. These functions are enabled when z/OSMF is installed and configured.

couple data set (CDS)

A data set that contains information related to a sysplex, its systems, cross-system coupling facility (XCF) groups, and their members. See also *sysplex couple data set* and *WLM couple data set*.

coupling facility

A special logical partition that provides high-speed caching, list processing, and locking functions in a sysplex.

CPU See *central processing unit*.

CPU service units

A measure of the task control block (TCB) execution time multiplied by an SRM constant which is CPU model dependent.

Custom-built Product Delivery Option (CBPDO)

A software delivery package consisting of uninstalled products and unintegrated service. Installation requires the use of SMP/E. CBPDO is one of the two entitled methods for installing z/OS; the other method is ServerPac.

D

data set

A named collection of related data records that is stored and retrieved by an assigned name. Equivalent to a file in other operating systems.

data type

The type of object associated with an incident, such as a dump or log.

DDS See *RMF Distributed Data Server*.

deploy

To install software into an operational environment.

deployment

In the Software Management task, a checklist that guides you through the software deployment process, and the object in which z/OSMF stores your input and any output generated for each step in the checklist.

description

See *incident description*.

destination

Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

diagnostic

Pertaining to the detection and isolation of an error.

diagnostic data

The collected information for an incident, such as dumps, OPERLOG, the logrec data set, and the logrec summary.

diagnostic details

Properties of an incident. The details include additional information about an incident and a list of the diagnostic data collected for the incident.

DNS See *Domain Name System*.

domain name server

In the Internet suite of protocols, a server program that supplies name-to-address translation by mapping domain names to IP addresses.

Domain Name System (DNS)

The distributed database system that maps domain names to IP addresses.

dump analysis and elimination (DAE)

A z/OS service that enables an installation to suppress SVC dumps and ABEND SYSUDUMP dumps that are not needed because they duplicate previously written dumps.

duration

In the Workload Management task, the amount of service (in service units) that the work can consume before it is switched to the goals of the next period.

E**Electronic Technical Response (ETR)**

See *problem management record*.

Environmental Record Editing and Printing (EREP)

The program that formats and prepares reports from the data contained in the error recording data set.

EREP See *Environmental Record Editing and Printing*.

error A discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition.

The smallest detectable anomaly or exception that can occur in an information system. Errors may be caused by hardware, software, internal code, media, or external causes, for example, people or environmental abnormalities.

error log

A data set or file that is used to record error information about a product or system. See *logrec*.

error message

An indication that an error has been detected.

error summary

A summary log of system errors. This log corresponds to a logrec summary report.

F**file permission bits**

In z/OS UNIX, information about a file that is used, along with other information, to determine if a process has read, write, or execute/search permission to a file or directory. The bits are divided into three parts, which are owner, group, and other.

File Transfer Protocol (FTP)

In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

firewall

A network configuration, usually both hardware and software, that prevents unauthorized traffic into and out of a secure network.

An intermediate server that functions to isolate a secure network from an insecure network.

fixed-length record

A record having the same length as all other records with which it is logically or physically associated. Contrast with *variable-length record*.

FMID See *Function Modification Identifier*.

FTP See *File Transfer Protocol*.

FTP data file
See *FTP.DATA file*.

FTP job
A job running on z/OS that sends incident-related information to an FTP server.

FTP job status
The state of the FTP job. For more details about the status of an FTP job, see the FTP job status details help topic.

FTP profile
Object that specifies the settings required for z/OSMF to gain access to an FTP server through an organization's FTP firewall or proxy.

FTP.DATA file
In z/OSMF, an installation-defined data set or UNIX file that is used to override the default system FTP configuration.

Function Modification Identifier (FMID)
A serviceable function of a z/OS software product, packaged in SMP/E installable format.

G

GDG See *generation data group*.

GDS See *generation data set*.

generation data group (GDG)
A chronological collection of historically related data sets that do not use the virtual storage access method (VSAM); each data set is called a generation data set.

generation data set (GDS)
One of the data sets in a generation data group (GDG); a GDS is historically related to the other data sets in the group.

graphical user interface (GUI)
A type of computer interface that presents a visual metaphor of a real-world scene, often of a desktop, by combining high-resolution graphics, pointing devices, menu bars and other menus, overlapping windows, icons and the object-action relationship.

group A collection of RACF-defined users who can share access authorities for protected resources.

guest In z/OSMF, a user who enters the system without an assigned role. Depending on how a guest user enters z/OSMF, a guest user is considered either authenticated or non-authenticated, as follows:

- **z/OSMF Authenticated Guest.** The user enters z/OSMF with a valid user ID and password, but is not defined to the z/OSMF user group.
- **z/OSMF Guest.** The user is neither logged into z/OSMF, nor assigned to the z/OSMF user group.

GUI See *graphical user interface*.

H

hardcopy log
In systems with multiple console support or a graphic console, a permanent record of system activity.

HFS See *hierarchical file system*.

hierarchical file system (HFS)

A system for organizing files in a hierarchy, as in a UNIX system.

HTTP proxy

Object that specifies the settings required for the primary system to gain access to a secondary system through an organization's HTTP proxy server.

I

I/O See *input and output*.

I/O service units

A measure of individual data set I/O activity and JES spool reads and writes for all data sets associated with an address space.

IBM Support Center

The IBM organization responsible for software service.

IBM WebSphere Application Server OEM Edition for z/OS

A native Web services runtime environment for select system-level applications that run on z/OS.

IBM z/OS Management Facility (z/OSMF)

A framework for managing various aspects of z/OS systems. z/OSMF includes an intuitive graphical user interface (GUI) for performing various management tasks. Structurally, z/OSMF is comprised of a web browser user interface and functions provided by z/OS components and the CIM server running in an address space on the host z/OS system.

IBMLink/ServiceLink

The IBM support site for opening, browsing, or updating customer problem management reports (PMRs). The site includes an interactive online database of PMRs. The contents include open and resolved authorized program analysis reports (APARs) and program temporary fix (PTF) information. The IBMLink/ServiceLink Web site is <http://www.ibm.com/ibmlink/servicelink>.

importance

In the Workload Management task, the degree of importance of a service class goal relative to other service class goals. There are five levels: lowest (5), low (4), medium (3), high (2), and highest (1).

incident

An event that is not part of the standard operation of a service and causes or may cause a disruption to or a reduction in the quality of services and customer productivity.

incident description

In the Incident Log task, the dump title for an incident, as it was specified by the operator or the abending system function.

Incident Log task

In z/OSMF, the management task that allows you to display a log of system records with details about each potential system problem. The Incident Log task provides a list of incidents through a summary view (*Incident Log* page) and a selectable detail view (*Diagnostic Details* page). The Incident Log task can help you obtain, aggregate, and send data to IBM Support or an independent software vendor (ISV) and manage the data associated with a particular problem.

initial program load (IPL)

The process of loading the operating system and other basic software into main storage.

The process by which an operating system is initialized at the beginning of the day or session. At IPL, the system operator enters the installation-specific information the operating system must

have in order to manage the installation's workloads. This information includes system parameters, system data set definitions, and other information needed for the operating system to begin operating.

input and output (I/O)

Pertaining to a device, process, channel, or communication path involved in data input, data output, or both.

installation

A particular computing system, including the work it does and the people who manage it, operate it, apply it to problems, service it, and use the results it produces.

installed service definition

In the Workload Management task, the service definition that resides in the WLM couple data set for the sysplex.

Internet Protocol (IP)

A protocol that routes data through a network or interconnected networks. Internet Protocol (IP) acts as an intermediary between the higher protocol layers and the physical network.

IP See *Internet Protocol*.

IP address

The unique 32-bit address (or, for IP version 6, the 128-bit address) that specifies the location of each device or workstation in the Internet. For example, 9.67.97.103 is an IP address. The address field contains two parts: the first part is the network address; the second part is the host number.

IPL See *initial program load*.

IPv4 Internet Protocol version 4.

IPv6 Internet Protocol version 6.

J

JCL See *job control language*.

job A separately executable unit of work.

job card

See *record*.

job control language (JCL)

A command language that identifies a job to an operating system and describes the job's requirements.

JOB statement

The JOB statement is the first control statement in a JCL job. It marks the beginning of a job and also specifies the name of the job. The JOB statement also might provide details and parameters that apply to all job steps within the job, such as accounting information and conditions for job termination. It also may contain any comments that help describe the statement.

L

link In the z/OSMF navigation area, a reference to an external Web resource that can be used when performing system management tasks. Your installation can customize z/OSMF with links to external sites for system management tools and information. z/OSMF comes supplied with several useful links by default.

Linux An open source operating system that runs on a wide range of hardware platforms and has many features that are similar to the UNIX system.

Linux data gatherer

See *RMF Linux data gatherer*.

local deployment

In the Software Management task, deployment of software to DASD volumes shared within the same sysplex where the primary system resides. Contrast with *remote deployment*.

lock The process by which integrity of data is ensured by preventing more than one user from accessing or changing the same data or object at the same time.

log in To connect to a computer system or network by entering identification and authentication information at the workstation.

log out

To discard authentication credentials and corresponding permissions. Once logged out, z/OSMF no longer recognizes the user and reverts to the authority of the z/OSMF Guest role.

log snapshot

A subset of log data preserved and associated with an incident.

logrec The z/OS error log, which contains error information in binary, written to a system-scope data set or a sysplex-wide log stream. See *error log*.

M**managed system**

A system that is being controlled by a given system management application.

manual control

In the Workload Management task, a method of managing application environments. Under manual control, the name of the startup JCL procedure has not been defined for an application environment. The installation, therefore, must manually start server address spaces, as needed. Contrast with *automatic control*.

member

A partition of a partitioned data set (PDS) or partitioned data set extended (PDSE).

metric A measurement type. Each resource that can be monitored for performance, availability, reliability, and other attributes has one or more metrics about which data can be collected.

metric group

In the Resource Monitoring task, a container that displays the samples that have been collected for the metrics included in the container and provides controls that you can use to browse through the collected samples.

Monitor III

See *RMF Monitor III*.

monitoring dashboard

In the Resource Monitoring task, a set of metric groups or custom views that you can use to monitor the performance of systems in your enterprise. Through the System Status task, you can control the scope of monitoring to include z/OS systems and sysplexes, AIX system complexes (System p®), Linux system complexes (System x® and System z), Linux images (System x and System z), and Windows system complexes.

MSGCLASS

Parameter on the JCL JOB statement that specifies the output class for output listings (SYSOUT). Output classes are defined by the installation to designate unit record devices, such as printers.

N

navigation area

Area of the z/OSMF browser interface from which the user can select among various systems management tasks. For example, to view potential problems, select the Incident Log task from the z/OSMF navigation area.

O

operations log (OPERLOG)

In a sysplex, the log of operational messages (WTOs and WTORs), which is stored in a z/OS system logger log stream.

OPERLOG

See *operations log*.

P

partitioned data set (PDS)

A data set in direct access storage that is divided into partitions, called members, each of which can contain a program, part of a program, or data. Synonymous with program library. Contrast with *sequential data set*.

partitioned data set extended (PDSE)

A system-managed data set that contains an indexed directory and members that are similar to the directory and members of partitioned data sets. A PDSE can be used instead of a partitioned data set.

pass phrase

A string consisting of mixed-case letters, numbers, and special characters, including blanks, that is used to control access to data and systems.

password

A string of characters known to a user who must specify it to gain full or limited access to a system and to the data stored within it. RACF uses a password to verify the identity of the user.

PDS See *partitioned data set*.

PDSE See *partitioned data set extended*.

PDUU See *z/OS Problem Documentation Upload Utility*.

performance period

In the Workload Management task, a service goal and importance level that is assigned to a service class for a specific duration.

plug-in

In z/OSMF, a collection of one or more system management tasks. A plug-in can be added to z/OSMF after the base configuration is created.

PMR See *problem management record*.

policy See *service policy*.

port An access point for data entry or exit.

port number

The part of a socket address that identifies a port within a host.

primary system

z/OS image that hosts the z/OSMF instance an enterprise uses to perform all of its z/OS management tasks.

primary z/OSMF instance

z/OSMF instance to which you will connect your browser to perform all z/OS management tasks.

problem determination

The process of determining the source of a problem.

The process of isolating the source of a suspected problem to a hardware or software component or product.

problem management record (PMR)

The number in the IBM support mechanism that represents a service incident with a customer.

A record of the activities performed during the course of resolving a customer reported problem. Customers with access to IBMLink can view their PMRs.

problem number

A tracking number used to refer to a problem reported to a service provider.

processor

In a computer, the part that interprets and executes instructions. Two typical components of a processor are a control unit and an arithmetic logic unit.

product information file

In the Software Management task, the file that contains product information, such as the product announce date, general availability date, and end of service date.

product set

The operating systems, subsystems, or products that should be installed, maintained, migrated, and deployed as a group.

profile

A file containing customized settings for a system or user.

proxy An application gateway from one network to another for a specific network application such as FTP.

R

RACF See *Resource Access Control Facility*.

reason code

A return code that describes the reason for the failure or partial success of an attempted operation.

record A group of related data, words, or fields treated as a unit, such as one name, address, and telephone number.

A self-contained collection of information about a single object. A record is made up of a number of distinct items, called fields. See *fixed-length record*, *variable-length record*.

remote deployment

In the Software Management task, deployment of software to DASD volumes accessible to a sysplex where the primary system does not reside. Contrast with *local deployment*.

Remote Technical Assistance and Information Network (RETAIN®)

Database used by IBM Support Centers to record all known problems with IBM licensed programs.

report class

In the Workload Management task, a group of work for which reporting information is collected separately. For example, you can have a report class for information combining two different service classes, or a report class for information on a single transaction.

Repository Authorization Mode

In previous releases of z/OSMF, the security authorization mode wherein user access to tasks is managed through user and role definitions in the z/OSMF data repository. Authorization to tasks is administered by the z/OSMF Administrator, through the Roles, Users, and Links tasks. As of z/OSMF V2R1, Repository Authorization Mode is no longer a supported option for z/OSMF. Instead, authorizations are managed through your security product, such as RACF. This mode of authorization was formerly known as *SAF Authorization Mode*.

resource

A facility of a computing system or operating system required by a job, task, or running program. Resources include main storage, input/output devices, the processing unit, data sets, files, libraries, folders, application servers, and control or processing programs.

In the Workload Management task, an actual physical entity such as a data base or a peripheral device, or an intangible quality such as a certain time of day or a certain day of the week.

Resource Access Control Facility (RACF)

A component of z/OS Security Server that provides access control by identifying and verifying the users to the system, authorizing access to protected resources, logging detected unauthorized attempts to enter the system, logging unauthorized attempts to enter the system, and logging detected accesses to protected resources.

resource group

In the Workload Management task, an amount of processing capacity across one or more z/OS images that is assigned to one or more service classes.

Resource Measurement Facility (RMF)

A feature of z/OS that measures selected areas of system activity and presents the data collected in the format of printed reports, System Management Facility (SMF) records, or display reports.

RETAIN

See *Remote Technical Assistance and Information Network*.

RMF See *Resource Measurement Facility*.

RMF Cross Platform Resource Monitoring (RMF XP)

Integrated solution of RMF to monitor the performance of heterogeneous environments, such as AIX running on System p, Linux running on System x or System z, or Windows running on System x.

RMF DDS

See *RMF Distributed Data Server*.

RMF Distributed Data Server (DDS)

The data server in a sysplex that gathers data from the RMF Monitor III distributed on each system in the sysplex.

RMF Linux data gatherer

An optional tool that gathers performance data for Linux images (System z and Intel). The tool is not supported by IBM, and it is not shipped with z/OSMF.

RMF Monitor III

A short-term data collector for z/OS images. It provides short-term data collection and online reports for continuous monitoring of system status and for solving performance problems, workflow delay monitoring, and goal attainment supervision.

RMF XP

See *RMF Cross Platform Resource Monitoring*.

role In z/OSMF, a functional grouping of task authorizations. A role represents the authorizations associated with that role.

S

SAF Authorization Mode

In previous releases of z/OSMF, the security authorization mode wherein user access to tasks is controlled through the z/OS system authorization facility (SAF). The authorization definitions used by SAF are managed by the installation's security management product. Authorization to tasks is granted based on user ID or the user's inclusion in a user group. In a system with RACF, for example, user authorization is based on RACF profiles and groups, and is maintained by the security administrator in the RACF database. As of z/OSMF V2R1, SAF Authorization Mode is the only supported option for z/OSMF. With this change, the need to distinguish between authorization *modes* is eliminated.

scheduling environment

In the Workload Management task, a list of resource names along with their required states. If a z/OS image satisfies all of the requirements in the scheduling environment associated with a given unit of work, that unit of work can be assigned to that z/OS image. If any of the requirements are not satisfied, then that unit of work cannot be assigned to that z/OS image.

secondary system

Any system that is not the primary system.

send diagnostic data

In the Incident Log task, the option to collect the information necessary for sending diagnostic data to IBM or another vendor and initiate the FTP action.

sequential data set

A data set whose records are organized on the basis of their successive physical positions, such as on magnetic tape.

A data set in which the contents are arranged in successive physical order and are stored as an entity. The data set can contain data, text, a program, or part of a program. Contrast with *partitioned data set (PDS)*.

server In a network, hardware or software that provides facilities to clients. Examples of a server are a file server, a printer server, or a mail server.

A computer that contains programs, data, or provides the facilities that other computers on the network can access.

The party that receives remote procedure calls. Contrast with *client*.

ServerPac

A software-delivery package consisting of products and service for which IBM has performed the System Modification Program/Extended (SMP/E) installation steps and some of the post-SMP/E installation steps.

service

In the Workload Management task, the amount of resources consumed by a work request. The service definition coefficients specified in the service definition and the CPU, SRB, I/O and storage service units are used to calculate service.

service class

In the Workload Management task, a group of work that has the same service goals or performance objectives, resource requirements, or availability requirements.

service coefficient

In the Workload Management task, a value that specifies which type of resource consumption

should be emphasized in the calculation of service rate. The types of resource consumption are central processing unit (CPU), input and output channel (IOC), main storage occupancy (MSO), and service request block (SRB).

service definition

In the Workload Management task, an explicit definition of all the workloads and processing capacity in a sysplex. A service definition consists of the following items: service definition details, service policies, workloads, service classes, resource groups, report classes, classification groups, classifications, application environments, resources, and scheduling environments.

service definition details

In the Workload Management task, section of the WLM service definition that contains the name, description, and functionality level of the service definition. It also contains the service definition coefficients and the service options.

service policy

In the Workload Management task, a named set of performance goals that WLM uses as a guideline when matching resources to work.

service request block (SRB)

A control block that represents a routine that performs a particular function or service in a specified address space.

session

The period of time during which a user of a terminal can communicate with an interactive system; usually, the elapsed time from when a terminal is logged into the system until it is logged out of the system.

A logical or virtual connection between two stations, software programs, or devices on a network that allows the two elements to communicate and exchange data.

The time during which an authenticated user is logged in.

software deployment

Process of making software available to be used on a system by users and other programs.

software instance

For z/OS platform software, the SMP/E target and distribution zones associated with a product set and the target and distribution libraries described by those zones.

Collection of one or more SMP/E target and distribution zone pairs defined under a single global zone, the related libraries, and any additional data sets associated with a product set.

Deployable unit of SMP/E installed software.

solution

A combination of products that addresses a particular customer problem or project.

source The initiator of an action or operation.

The input for an action or operation.

In the Incident Log task, it is the name of the data set or log stream in which the dump or log is stored.

source software instance

In the Software Management task, the input to the software deployment process. It is the software instance to be deployed.

source system

In the Software Management task, the z/OSMF host system that has access to the volumes and data sets where the source software instance resides.

SPECIAL attribute

A user attribute that gives the user full control over all of the RACF profiles in the RACF database and allows the user to issue all RACF commands, except for commands and operands related to auditing.

status The current condition or state of a program, object, or device, for example, the status of a printer.
The state of a job or job stream instance.

storage service units

A measure of the central storage page frames multiplied by 1/50 of the CPU service units. The 1/50 is a scaling factor designed to bring the storage service component in line with the CPU component.

superuser

In z/OS UNIX, a system user who operates with the special privileges needed to perform a specified administrative task.

superuser authority

In z/OS UNIX, the unrestricted authority to access and modify any part of the operating system, usually associated with the user who manages the system.

SVC dump

A dump that is issued when a z/OS or a DB2® functional recovery routine detects an error.

A representation of the virtual storage for the system when an error occurs. Typically, a system component requests an SVC dump from a recovery routine when an unexpected error occurs. However, an authorized program or the operator can also request an SVC dump when diagnostic dump data is needed to solve a problem.

SYSLOG

A Berkeley Software Distribution (BSD) logging system used to collect and manage other subsystem's logging data.

A single-system log of operational messages, stored in JES spool files.

sysplex (system complex)

Multiple systems communicating and cooperating with each other through multisystem hardware elements and software services to process the installation's workloads.

sysplex couple data set

A couple data set (CDS) that contains sysplex-wide data about systems, groups, and members that use cross-system coupling facility (XCF) services. All systems in a sysplex must be connected to the sysplex CDS. See also *couple data set* and *WLM couple data set*.

sysplex dump directory

A shared VSAM data set used to store properties (data values) associated with the SVC dumps created on a z/OS system or sysplex. By default, this data set is named SYS1.DDIR.

system

The combination of a configuration (hardware) and the operating system (software). Often referred to simply as the z/OS system.

In z/OSMF, a z/OS image that hosts a z/OSMF instance.

In the Software Management task, the z/OSMF host system that has access to the volumes and data sets where a software instance resides.

system-initiated abend

An abend caused by the operating system's inability to process a routine; may be caused by errors in the logic of the source routine. Contrast with *user-initiated abend*.

system log (SYSLOG)

In z/OS, the system log data set that includes all entries made by the WTL (write-to-log) macro as well as the hardcopy log. SYSLOG is maintained by JES in JES SPOOL space.

system logger

A central logging facility provided by MVS. The system logger provides an integrated MVS logging facility that can be used by system and subsystem components.

The z/OS component that creates sysplex-wide log streams, such as OPERLOG and the sysplex-wide logrec data set.

system REXX

The z/OS component that provides a programming interface for running REXX execs outside of TSO/E or the batch environment.

SYSREXX

A system function used to invoke REXX execs from a programmable interface imbedded in authorized system code.

T

target The destination for an action or operation.

The output of an action or operation.

target software instance

In the Software Management task, the software instance that will be created as a result of a deployment. It is the output of the software deployment process.

target system

In the Software Management task, the z/OSMF host system that has access to the volumes and data sets where the target software instance will reside.

task In z/OSMF, a systems management function that is selectable from the product's navigation area.

TCP/IP data file

See *TCPIP.DATA* file.

TCPIP.DATA file

In z/OSMF, an installation-defined data set or UNIX file that is used to override the default system TCP/IP configuration.

terse The process of compacting (packing) data before transmitting a copy to another site, typically employing FTP as the transmission mechanism. A complementary unpack service is provided to create a similar data set at the receiving site. On z/OS, the AMATERSE service aid program is used to compact data.

tracking ID

In the Incident Log task, a local problem tracking number, available to correlate an incident with a problem management system.

U

user-initiated abend

A request made by user code to the operating system to abnormally terminate a routine. Contrast with *system-initiated abend*.

V

variable-length record

A record having a length independent of the length of other records with which it is logically or physically associated. Contrast with *fixed-length record*.

velocity

In the Workload Management task, a type of service class goal that you can use to specify the rate at which you expect work to be processed for a given service class when that work is ready to run. It is a measure of the acceptable processor and storage delays while work is running.

virtual storage access method (VSAM)

An access method for direct or sequential processing of fixed-length and variable-length records on disk devices. The records in a VSAM data set or file can be organized in logical sequence by a key field (key sequence), in the physical sequence in which they are written on the data set or file (entry sequence), or by relative-record number.

VSAM

See *virtual storage access method*.

W

WLM See *Workload Manager*.

WLM Administrative Application

The Interactive System Productivity Facility (ISPF) application used to specify WLM service definitions.

WLM couple data set

A type of data set that is created through the XCF couple data set format utility for the WLM function. The data set contains the service definition information.

work qualifier

In the Workload Management task, an attribute of incoming work. Work qualifiers include: subsystem type, subsystem instance, userid, accounting information, transaction name, transaction class, source LU, netid, and LU name.

work request

A piece of work, such as a request for service, a batch job, a transaction, or a command.

workload

In the Workload Management task, a group of service classes to be tracked, managed, and reported as a unit.

Workload Management task

In z/OSMF, the management task that allows you to manage WLM service definitions and to operate WLM. You can use this task to define, modify, view, import, export, print, or install a service definition or activate a service policy.

Workload Manager (WLM)

A z/OS component that prioritizes workloads and matches them with available resources.

write to operator (WTO)

A system service used to send messages to an operator console informing the operator of errors or system conditions that might need correcting. A response is not required.

write to operator with reply (WTOR)

A system service used to send messages to an operator console informing the operator of errors and system conditions that might need correcting. A response is required.

WTO See *write-to-operator*.

WTOR

See *write-to-operator-with-reply*.

Z

z/OS An IBM mainframe operating system that uses 64-bit real storage.

z/OS file system (zFS)

A type of file system that resides in a VSAM linear data set (LDS).

z/OS host system

The system on which z/OSMF is running.

z/OS Problem Documentation Upload Utility (PDUU)

A parallel File Transfer Protocol (FTP) utility that is designed to send documentation in a more efficient manner to IBM FTP sites. For more information about the utility, see *z/OS MVS Diagnosis: Tools and Service Aids*.

z/OSMF

See *IBM z/OS Management Facility*.

zFS See *z/OS file system*.

Index

Special characters

_BPXX_AUTOCVT environment variable 187
-add option 127, 285
-addlink option 167, 285
-config option 33, 55, 285
-fastpath option 22, 33, 34, 35, 286
-finish option 39, 285
-list roles option 131
-modify option 285, 293
-overridefile option 22, 33, 286
-role option 131
-verify option 38, 171, 285
/tmp directory 188
 modifying the default 22
.profile file
 defining for the administrator 90
\$TMPDIR environment variable 188

A

About page
 description 186
About this document xi, xv
accessibility 337
 features of the GUI 337
administration task
 links 170
advanced settings
 modifying 293
 reviewing 22, 39
AGGRGROW setting
 used for z/OSMF 27, 39
alias
 removing for UNIX commands 32
Application Linking Manager task
 overview 155
ASSIZE recommendation 30
authenticated guest
 description 82
authorizing users to z/OSMF 131, 133, 200
automatic dump data set allocation
 (auto-dump)
 using 103
automount facility
 consideration for using 28, 40
automount process
 consideration for using 27
AUTOMOVE setting
 consideration for using 27
AXR address space
 verifying active state 109, 200

B

backing store file
 transferring into z/OSMF 92
base configuration
 creating 29

base configuration (*continued*)
 description 13
BBO.SYNC.userid
 migration action 60
BLSCDDIR CLIST
 example 106
 using 105
BLSJPRMI program
 using 106
BPX.SRV.userid
 migration action 60
BPX.SRV.ZOSMFAD SURROGAT rule
 migration action 60
BPXPRMxx parmlib member
 settings for 27, 30
browser
 See web browser

C

CA
 See certificate authority
Capacity Provisioning task
 input for configuration 83
 overview 65
 RACF commands 308
 z/OS customization 90
CBPDO tape
 configuration steps to use 29
CEA
 See common event adapter (CEA)
CEA high-level qualifier 173
CEACDMPP exec 199, 202
CEAPRMxx parmlib member
 specifying an eighth volume 108
 specifying in IEASYSxx member 107, 108
 specifying the HLQ for snapshot data sets 173
CEASEC job
 using 107
CEASNPLG member of
 SYS1.SAMPLIB 96, 102, 173
ceatool program
 description 173
 examples 175
 invoking 174
certificate authority (CA)
 using 144, 157, 163
certificate error
 troubleshooting 204, 206, 207
CFZSEC job
 using 89, 275
CIM
 See Common Information Model
CIM class 158
CIM indication 157, 158
CIM indication provider
 subscription 158
CIM server
 commands 159

CIM server (*continued*)
 customizing the administrator profile 159
 RACF commands 307
CIM_IVP_TIMEOUT variable 195
cimivp program
 time out condition 195
cimjnitimeout setting 22, 293
CIMSERV profile in the WBEM class 89, 275
class activation 36, 267
clean-up actions after migration 58, 59, 60
client side log data 188, 191
cloning an instance 140
command aliasing
 removing for UNIX commands 32
common event adapter (CEA)
 address space
 assigning the TRUSTED attribute 108, 111
 disconnecting from the sysplex dump directory 213
 used during Incident Log task processing 93
 verifying active state 107, 200
 authorizing the z/OSMF administrator 107, 312
 CEAPRMxx parmlib member 96, 108
 deleting diagnostic data 173
 deleting incidents 173
 ensuring that CEA is active 107, 108
 full function mode 107
 high-level qualifier 173
 log stream recommendation 102
 modifying settings 108
 overview 4
 RACF security profiles 276, 278
 reason codes 297
 starting at IPL 96
 troubleshooting 200
Common Information Model (CIM)
 .profile file
 defining for the administrator 90
 provider
 increasing the timeout interval 22, 88, 293
 server
 automatic startup 88
 increasing the timeout interval for CIM providers 88
 logging 177
 overview 4
 security authorizations 89, 275
 starting 88, 159
 timeout setting 88
 trace 177
 WBEM root directory 30
configuration
 for z/OSMF 13

- Configuration Assistant for z/OS
 - Communications Server
 - transferring backing store file 92
- Configuration Assistant task
 - collecting information for
 - troubleshooting 210
 - common problems 210
 - overview 66
 - RACF commands 310
 - troubleshooting 210
 - z/OS customization 92
- configuration file
 - creating 33
 - defaults 289
 - description 13
 - naming 33, 34
 - overriding values in 21
- configuration process
 - authorizations needed 14, 89
 - overview 13
 - performers 29
- configuration script
 - prerequisites 29
 - priming the data file system 39
 - running 33, 38, 39, 293
 - selecting a user ID 14
 - syntax 29, 285
 - where to find 29
- convertFromREPtoSAF.rexx 48
- core functions
 - in a base configuration 63
 - input for configuration script 16
 - RACF commands 301
- CSFSERV class profiles 274

D

- data file system
 - mounted at IPL 27
 - priming during configuration 39
- default configuration file 289
- default override file 291
- disability 337
- dump analysis and elimination (DAE)
 - configuring 104
- DUMPSRV address space
 - recycling 106
- dynamic VIPA
 - using 137

E

- environment checker tool
 - using 178
- environment variables 13, 30
- error logging
 - at server startup 188
 - on a running server 189
- exec
 - convertFromREPtoSAF.rexx 48
 - izuconfig1.cfg.USERID.rexx 37, 133
 - izuconfig1.cfg.add.rexx 301, 307, 308, 310, 312, 315, 317, 319, 321
 - izuconfig1.cfg.rexx 36, 301

F

- fallback considerations 57
- fastpath mode
 - description 34
 - parameter on izusetup.sh 286
 - using 22, 35
- file system 16, 135
- Firefox browser
 - certificate error 205
- firewall consideration 88
- FTP job
 - modifying the device default 22
 - status codes 213
- full function mode for CEA 107
- full system replacement installation
 - considerations 5, 29, 48

G

- generic profile checking
 - enabled for security classes 267
- guest user
 - access to resources 82
 - customized Welcome page 153

H

- high availability
 - planning for 135, 137
- high level qualifer (HLQ)
 - for CEA data sets 84, 173
- HLQLONG statement 173
- host name
 - default 16
 - modifying 141
- host system
 - required software 29

I

- IBM 64-bit SDK for z/OS, Java
 - Technology Edition 4
- IBM z/OS Management Facility
 - base configuration 13, 29
 - component overview 4
 - configuration process 13
 - Lightweight Third Party
 - Authentication (LTPA) 147
 - multiple instances 21, 135, 137, 140, 141, 143, 144, 147
 - overview xi, 3, 4, 5, 6
 - planning checklist 7
 - post-configuration 149
 - publications xi
 - single sign-on (SSO) 147
 - summary of IT roles and skills 7
 - tasks overview 64
 - troubleshooting 177
 - information for 177
 - web site xi
- IBMzOS_JobsIndicationProvider 158
- IEADMCZM member
 - in SYS1.SAMPLIB 84, 289
- IKJTSOxx member 197

Incident Log task

- CEA reason codes 297
- common problems 212
- configuration updates
 - reference information 93
- device for storing data 22
- input for configuration 84
- IVP for checking the setup 39, 171, 197, 199
- modifying the device default 22
- overview 67
- RACF commands 312
- temporary directory 22
- troubleshooting 212
- verifying setup 39, 171
- z/OS customization 95

incidents

- deleting 173, 175

INPUT indicator 33

installation verification program (IVP)

- checking the setup 39, 171, 199
- checking the z/OS setup 197
- report format 325
- System REXX check 109, 200
- using 197

installer user ID

- creating a base configuration 29
- logging in to z/OSMF 45
- requirements for 14

Integrated Cryptographic Service Facility (ICSF)

- security authorizations 274

interactive mode

- running the izusetup.sh script 22

IPCS job

- sample JCL 200

ISPF task

- common problems 210
- overview 69
- RACF commands 315
- troubleshooting 210
- z/OS customization 111

IXCMIAPU utility program 102

IZU_APPSERVER_HOSTNAME variable 16

IZU_AUTOGID_OVERRIDE variable 16

IZU_AUTOUID_OVERRIDE variable 16

IZU_CODE_ROOT setting 30

IZU_CONFIG_DIR setting 29

izu_env.sh script

- description 13, 30

IZU_LOGFILE_DIR setting 30

izuadmin.env file 22, 39, 293

izuadmin.sh script 296

IZUANG1 started task

- cataloged procedure 24, 25, 51

izuauthuser.sh script 131, 200

izuconfig1.cfg file

- creating 33

izuconfig1.cfg.USERID.rexx 37, 133

izuconfig1.cfg.add.rexx

- contents of 82, 301, 307, 308, 310, 312, 315, 317, 319, 321

izuconfig1.cfg.rexx

- contents of 301
- using 36

IZUDFLT profile prefix 80, 82

- izudflt.cfg file
 - defaults 289
 - description 13
- IZUDFLT.izuNOUsers resource 131
- izudflt.ovr file
 - defaults 289
 - description 13
 - using 21
- IZUFPROC logon procedure
 - cataloged procedure 24, 25, 26, 51
 - permissions 24, 25, 26, 51
- IZUG0.log.lck file 187
- IZUGn.log file 186, 187
- izugwrkmanwlmclass setting 22, 293
- izuiltempdirvalue setting 22
- izuilunitvalue setting 22
- izuincidentlogverify.report file
 - creating 197
 - reviewing 39, 171
- IZUKeyring.IZU_SAF_PROFILE_PREFIX
 - description 144, 151
- IZUKeyring.IZUDFLT name 151
- izumigrate.sh script 53
- izunotificationexpiration setting 22, 293
- izunotificationsmax setting 22, 293
- izuNOUsers resource 131
- izusetup.sh script
 - add option 127, 285
 - addlink option 167, 285
 - config option 22, 33, 55, 285
 - fastpath option 22, 34, 286
 - finish option 39, 285
 - modify option 293
 - overridefile option 22, 286
 - verify all option 171
 - verify core option 171
 - verify log option 171
 - verify option 38, 285
 - verify racf option 171
 - description 13
 - overridefile file 21
 - running 33, 38, 39
 - syntax 285
- IZUSVR user ID
 - permissions 24, 25, 51, 274
- IZUSVR1 started task
 - cataloged procedure 24, 25, 51
- izutracespec setting 22, 293

J

- Java home directory
 - modifying the default 30
- JAVA_HOME setting 30
- job control language (JCL)
 - sample for renaming dumps in the sysplex dump directory 110

K

- keyring name
 - changing 151

L

- link
 - managing security in z/OSMF 170
- log data 188
 - client side 191
 - server side 190
- log file
 - description 186
 - working with 187
- log file directory 135
 - modifying the default 30
- log format 190
- log lock file 187
- logging error data for z/OSMF 188
- logging in to z/OSMF 22, 45, 208, 293
- LOGREC log stream
 - setting up 100
- LTPA
 - See Lightweight Third Party Authentication (LTPA)
- ltpacachetimeout setting 22, 293
- ltpatimeout setting 22, 208, 293

M

- mainframe education xi
- managing log lock files 187
- MAXPROCUSER value
 - consideration 196
- MEMLIMIT recommendation 30
- message IZUG295E 195
- messages for z/OSMF 215
- messages.log file 186
- migration
 - actions 47, 48, 50, 58, 61
 - description 47
 - upgrading the configuration file 53
 - upgrading the override file 53
- migration report file
 - example 329
- mount point 16, 135

N

- network consideration 88
- notifications
 - expiration limit 22
 - maximum number allowed 22
 - setting a maximum number 293
 - setting an expiration limit 293
- Notifications task
 - overview 70

O

- OMVS session
 - INPUT status indicator 33
- operations log (OPERLOG)
 - setting up 98, 99
- operator console messages 186
- override file
 - defaults 289
 - description 13, 21
 - parameter on izusetup.sh 286

P

- parmlib data set
 - access required 40
- PassTicket creation 51, 90, 91, 112
- PEGASUS_HOME setting 30
- planning checklist 7
- planning worksheet 82
- plug-in
 - planning your selections 63, 83
- post-configuration
 - for z/OSMF 149
- pre-migration actions 47
- primary instance
 - configuring 144, 147
- PROCUSERMAX value
 - consideration 196
- product file system
 - mounted at IPL 27
- product file system mount point
 - modifying the default 30
- product information files 121
- profile.add file 90
- project plan 7
- PTKTDATA security class
 - activating 91, 113

R

- RACDCERT command
 - error message 197
 - using 165
- RACF commands
 - Capacity Provisioning task 308
 - CIM server 307
 - Configuration Assistant task 310
 - core functions 301
 - Incident Log task 312
 - ISPF task 315
 - Resource Monitoring task 317
 - Software Management task 319
 - System Status task 317
 - Workload Management task 321
- RACF SPECIAL attribute 29
- re-authenticating 22, 208, 293
- reason codes
 - for common event adapter 297
- REGION recommendation 30
- Resource Monitoring task
 - browser consideration 114
 - overview 71
 - RACF commands 317
 - z/OS customization 112
- root code directory mount point
 - modifying the default 30
- runtime log 186, 187, 190

S

- SAF
 - See system authorization facility
- SAF Authorization Mode
 - conversion to 48
- SAF profile prefix
 - defining 268
- screen resolution
 - minimum supported 24

- script
 - izuadmin.sh script 296
 - izuauthuser.sh script 131
 - izumigrate.sh script 53
 - izusetup.sh script 33, 38
 - add option 127
 - addlink option 167
 - config option 55
 - finish option 39
 - modify option 293
 - verify all option 171
 - verify core option 171
 - verify log option 171
 - verify option 38
 - verify racf option 171
 - startServer.sh script 44
 - where to find 29
 - script mode
 - choosing 22
 - secondary instance
 - configuring 144, 147
 - Secure Sockets Layer (SSL) connection
 - enabling between client programs and z/OSMF 157, 163
 - enabling between instances of z/OSMF 144
 - security administration
 - overview 80, 82
 - security administrator
 - actions performed by 80, 82
 - managing links 170
 - security class
 - activating 36, 267
 - security concepts 15
 - security setup
 - authorizing users to z/OSMF 131
 - default for z/OSMF 267
 - verifying the RACF actions 38
 - Send Diagnostic Data wizard
 - troubleshooting 213
 - server log files 187
 - server side log data
 - description 190
 - ServerPac order
 - considerations xi, 5, 29, 48
 - service
 - applying updates to z/OSMF 6
 - session status
 - refreshing 33
 - sessiontimeout setting 22, 293
 - shell command
 - removing aliases 32
 - single sign-on (SSO)
 - enabling between instances of z/OSMF 147
 - Software Management task
 - migration consideration 50
 - RACF commands 319
 - z/OS customization 115, 144
 - software upgrade installation
 - considerations 5, 29, 48
 - SSL
 - See* Secure Sockets Layer (SSL)
 - SSO
 - See* single sign-on (SSO)
 - startServer.sh script
 - using 44
 - subscription
 - choosing a user ID 158
 - creating 159
 - customizing the administrator profile 159
 - Summary of Changes xvii
 - superuser authority
 - required for user ID 14, 89
 - SURROGAT class profile
 - checking 60
 - syntax diagrams
 - how to read xi
 - SYS1.SAMPLIB data set
 - CEASNPLG member 96, 102
 - sysplex dump directory
 - creating 105
 - migrating to a larger directory 106
 - renaming dumps in the directory 110
 - space shortage 106
 - using the BLSCDDIR CLIST 105
 - verifying setup 39
 - SYSREXX
 - See* System REXX (SYSREXX)
 - component
 - system authorization facility
 - overview 4
 - system log (SYSLOG)
 - capturing data from 102
 - system logger couple data set
 - creating 96
 - system prerequisites for z/OSMF
 - overview 87
 - System REXX (SYSREXX) component
 - ensuring that it is active 109
 - troubleshooting 200
 - System Status task
 - overview 75
 - RACF commands 317
 - z/OS customization 112
- T**
- temporary directory
 - modifying the default 22
 - tools for troubleshooting 178
 - trace data
 - using 188, 195
 - troubleshooting
 - action or link not available 209
 - browser problems 178
 - certificate error 204, 205, 206, 207
 - checking the About page 186
 - common problems 192
 - Configuration Assistant task 210
 - configuration problems 192
 - EJBROLE class not defined 209
 - enabling tracing 188
 - Firefox 180
 - help not available 209
 - Incident Log task 212
 - Internet Explorer 183
 - ISPF task 210
 - link not available 209
 - logon errors 207
 - messages 215
 - overview 177
 - Send Diagnostic Data wizard 213
- troubleshooting (*continued*)
- tools for 177, 178
 - user interface problems 204
 - using the Incident Log IVP 197
 - using the runtime logs 186, 187
 - workstation problems 178
- TRUSTED attribute
- assigning to the CEA addresss space 108, 111
- U**
- user
 - authorizing to z/OSMF tasks 131
 - user ID
 - authorizing to z/OSMF 37, 133
 - selecting for configuration 14
 - user login error 207
- V**
- verification report 325
 - verification script 171
- W**
- WBEM root directory
 - modifying the default 30
 - web browser
 - common problems 180, 183, 204
 - enabling prompting for file downloads 114, 125, 185
 - Internet Explorer 114, 125
 - recommended settings 180, 183, 185
 - supported browsers 24
 - troubleshooting
 - Firefox 180
 - Internet Explorer 183, 185
 - WebSphere constructs
 - removing after migration 60
 - WebSphere Liberty profile 4
 - messages 215
 - troubleshooting 177
 - Welcome page
 - accessing 44
 - customizing for guests 153
 - workflows
 - maximum number allowed 22
 - setting a maximum number 293
 - Workflows task
 - overview 76
 - RACF commands 301
 - Workload Management task
 - browser consideration 125
 - input for configuration 86
 - overview 77
 - RACF commands 321
 - z/OS customization 123
 - worksheets
 - for z/OSMF 82
 - workstation
 - logon errors 207
 - required software 24

Z

- z/OS Basic Skills information center xi
- z/OS data set and file REST interface
 - cataloged procedure 24, 25, 26, 51
 - RACF security profiles 276
 - setting up 24, 25, 26, 51
- z/OS jobs REST interface
 - CEA reason codes 300
 - post-configuration tasks 157, 158, 163
 - RACF security profiles 277
- z/OSMF
 - See* IBM z/OS Management Facility
- z/OSMF administrator
 - defining 89
- z/OSMF installer user ID
 - authorizing 37
 - increasing the PROCUSERMAX value 196
- z/OSMF server
 - cataloged procedures 24, 25, 51
 - changing the logging level 188, 189
 - defining in COMMNDxx member 43
 - displaying status 42
 - setting up 24, 25, 51
 - started tasks 24, 25, 51
 - starting 41
 - stopping 43
 - verifying operation 41
- z/OSMF started task user ID
 - setting password for 40
- ZOSMF.** generic profile
 - removing 61
- ZOSMFAD user ID
 - removing after migration 59
 - retaining from previous releases 50



Product Number: 5610-A01

Printed in USA

SA38-0657-03

