z/OS

IBM z/OS Management Facility User's Guide

Version 1 Release 11

SA38-0652-02

z/OS

IBM z/OS Management Facility User's Guide

Version 1 Release 11

SA38-0652-02

Note
Before using this information and the product it supports, be sure to read the general information under "Notices" on page 205.

Third Edition, December 2009

This edition applies to Version 1 Release 11 of IBM z/OS Management Facility (5655-S28), and to subsequent releases and modifications until otherwise indicated in new editions.

IBM welcomes your comments. A form for readers' comments may be provided at the back of this document, or you may address your comments to the following address:

International Business Machines Corporation
MHVRCFS, Mail Station P181
2455 South Road
Poughkeepsie, NY 12601-5400
United States of America

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

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

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

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

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

Contents

Tables

Figures

About this information

This document provides information to help you set up, configure, and use IBM® z/OS® Management Facility (z/OSMF). This document also provides information for troubleshooting problems related to the use of z/OSMF.

A companion document, *IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide*, GA38-0631, describes the prerequisite steps for configuring the application server runtime environment for z/OSMF. This work must be completed before using the procedures described in this document.

Who should use this information

This document provides information for anyone who needs to set up and use z/OSMF or diagnose problems with this product. This document assumes that you are familiar with the z/OS operating system and its associated products.

The planning and configuration information in this document is intended for installations that install z/OSMF from a Custom-Built Product Delivery Option (CBPDO) software delivery package, or from a ServerPac order using the ServerPac software upgrade method of installation. If you install z/OSMF as part of a ServerPac full system replacement, the z/OSMF configuration work described in this book is performed for you in a ServerPac post-installation job. It is recommended that you review the setup actions described in this book to ensure the z/OSMF configuration is correct for your environment.

The information in this document is also required for anyone who needs to configure additional instances of z/OSMF for backup or testing purposes.

Where to find more information

This document is the last in a sequence of three documents that you use to set up z/OSMF. Prior to doing the work in this document, you must complete the installation and setup tasks described in the following documents:

- *Program Directory for IBM z/OS Management Facility*, GI11-2886. This document describes the material and procedures for installing z/OSMF and for applying the requisite service for this product.
- *IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide*, GA38-0631. This document provides configuration information for setting up IBM WebSphere Application Server OEM Edition for z/OS, which is part of the configuration process for z/OSMF.

Where necessary, this document references information in other documents, using shortened versions of the document title. For complete titles and order numbers of the documents for all products that are part of z/OS, see *z/OS Information Roadmap*.

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

You can also visit the z/OS Internet Library http://www.ibm.com/systems/z/os/zos/bkserv/.

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/zoslnctr/v1r7/index.jsp

Summary of Changes

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

Summary of Changes for SA38-0652-02 z/OS Version 1 Release 11

This document contains information previously presented in *IBM z/OS Management Facility Version 1 Release 11* (SA38-0652-01).

This document has been updated in support of PTF UK52956 (APAR PK97274), as follows.

New information

The following new options for the **izusetup.sh** script provide you with more flexibility in specifying the configuration data for your environment:

- The -overridefile option allows you to supply your configuration data in an editable file. You can use the override file to replace the values in the configuration file. When used with the **izusetup.sh -config** script in interactive mode, the override file saves you from having to enter your installation-specific values in response to the script prompts. Instead, you need only review each value displayed by the script and press Enter to accept it.
- The -fastpath option allows you to run the **izusetup.sh** script "quietly,"rather than interactively through a series of script prompts. In this mode, you supply your configuration data through one or two input files (the configuration file or the override file, or both). Previously, the script supported interactive input only.

For more information about the new options, see the topic "Choosing a script mode" in Chapter 2 "Planning."

Changed information

PTF UK52956 reduces the number of steps needed to configure an instance of z/OSMF on your system. These steps are described in Chapter 3 ″Configuring z/OSMF.″

This document also contains terminology, maintenance, and editorial changes, including changes to improve consistency and retrievability.

Summary of Changes for SA38-0652-01 z/OS Version 1 Release 11

This document contains information previously presented in *IBM z/OS Management Facility Version 1 Release 11* (SA38-0652-00).

This document contains terminology, maintenance, and editorial changes, including changes to improve consistency and retrievability.

Chapter 1. Overview of z/OSMF

IBM z/OS Management Facility V1R11 (z/OSMF V1R11) provides a framework for managing various aspects of a z/OS system through a Web browser interface. By streamlining some traditional tasks and automating others, z/OSMF can help to simplify some areas of system management and reduce the level of expertise needed for managing a system.

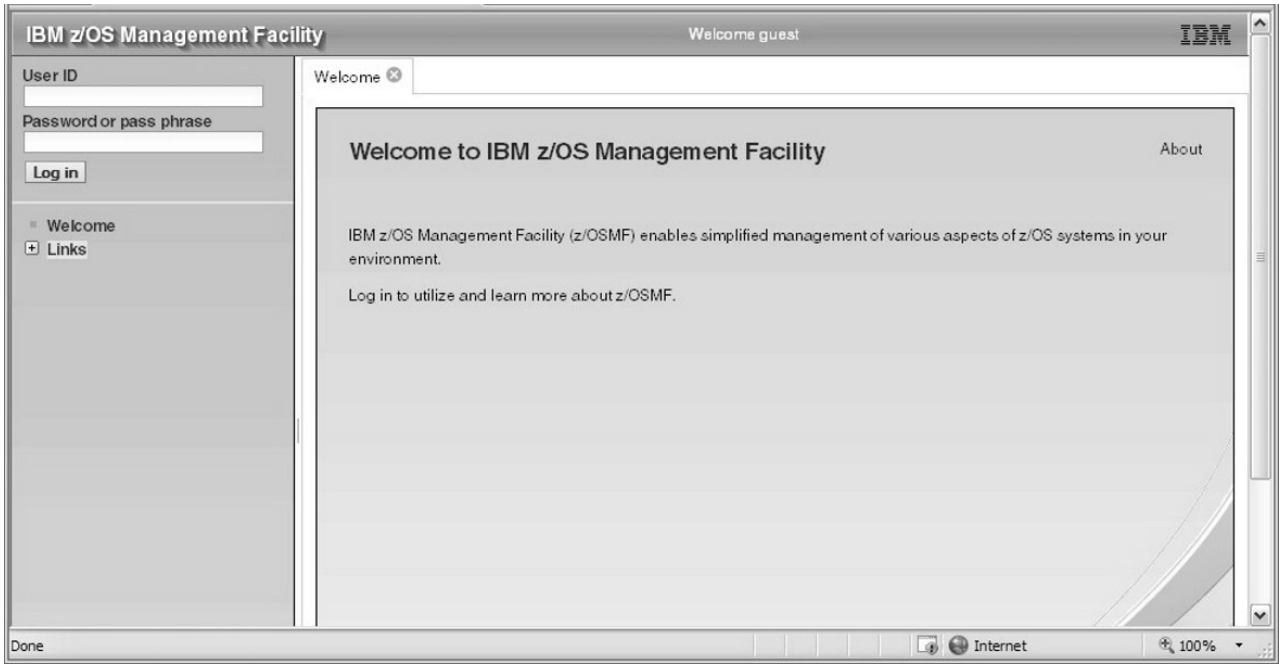


Figure 1. z/OSMF login page

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

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

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

In the first release of z/OSMF

z/OSMF V1R11, the initial release of the product, provides the infrastructure, services, and user interfaces that allow you to perform the following functions:

- Configure TCP/IP policy-based networking functions on z/OS V1R11 systems and later.
- Add links for external Web applications and Web sites to the z/OSMF navigation area.
- Perform problem data management tasks through the Incident Log, which centralizes problem data for your system and simplifies the process of sending diagnostic data to IBM.
- Manage user access to the z/OSMF product.

You can have only one instance of z/OSMF active in a system or sysplex at any given time. Multiple users can log into the same instance of z/OSMF using different computers, different browsers, or multiple instances of the same browser.

Though you can have only one instance of z/OSMF active in a sysplex, you can create additional instances of z/OSMF on other systems. You might do this, for example, for testing purposes, or for backup in case of system failure.

z/OSMF and related system components

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

Structurally, z/OSMF comprises a Web browser interface that communicates with the z/OSMF application running on the z/OS host system. Depending on the system management 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 functions available in z/OSMF. No separate client install is required.

z/OSMF includes the following software:

- IBM WebSphere® Application Server OEM Edition for z/OS Version 7.0, which provides a native application server runtime environment for z/OSMF. It is new for z/OS V1R10.
- A set of administration and system management tasks that run on IBM WebSphere Application Server OEM Edition for z/OS.
- Technologies for serving the Web browser interface, such as JavaScript™ and a Dojo framework.

Depending on the system management task being performed by the user, z/OSMF makes use of new enabling technologies on z/OS. For example, the Incident Log task of z/OSMF uses services provided by the following z/OS components:

- Common Information Model (CIM) server running on the host z/OS system. This component provides the z/OS data and administrative capability.
- Common event adapter (CEA). This component enables CIM providers to identify, receive and process selected z/OS events.
- System REXX (SYSREXX). This component provides an infrastructure through which REXX execs may be run outside the normal TSO/E or batch environments, using a programming interface.

The goal of this architecture is to provide simplified systems management function through a common, easy-to-use, graphical user interface. Figure 2 shows the architecture flow for the Incident Log task, starting with z/OSMF and continuing through IBM WebSphere Application Server OEM Edition for z/OS, with information passed to the CIM server, through CEA, and finally System REXX.

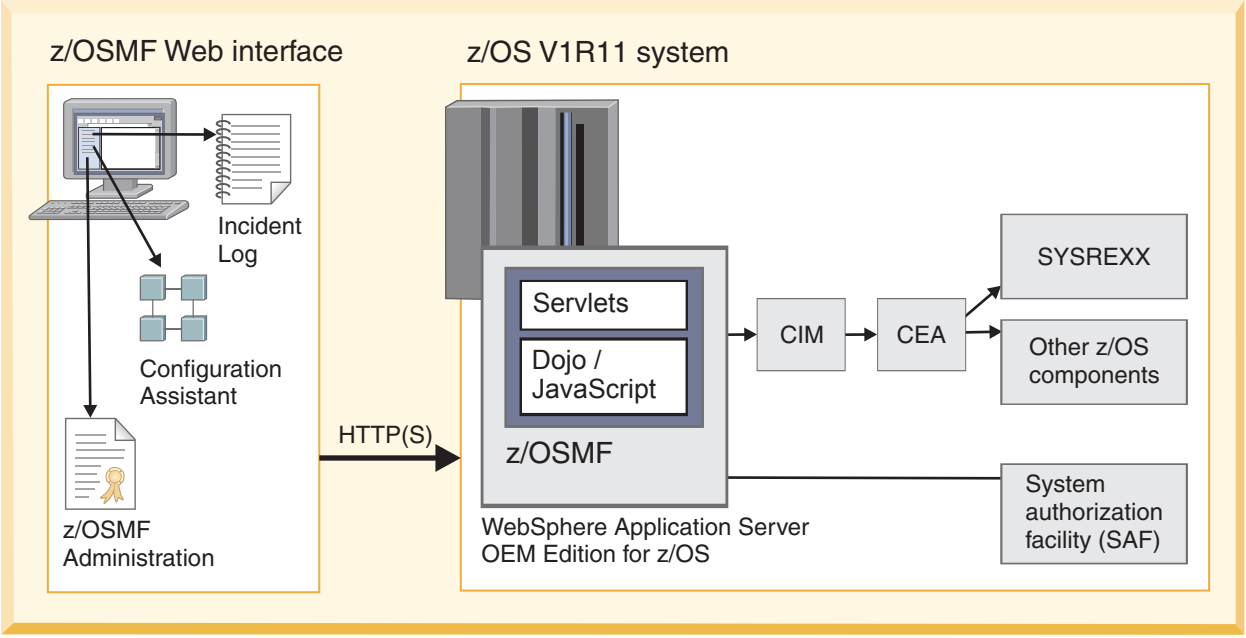


Figure 2. z/OSMF architecture and flow for the Incident Log task

What setup is needed for z/OSMF?

If you receive z/OSMF as part of a ServerPac order, and you select the full system replacement installation type, z/OSMF is set up for you. Here, z/OSMF is configured through a ServerPac post-installation job, using mostly IBM-supplied defaults. If you use full system replacement, it is recommended that you review the setup steps in this document to ensure that z/OSMF is configured correctly for your installation.

If you receive z/OSMF in a Custom-Built Product Delivery Option (CBPDO) software delivery package, or in a ServerPac order for which you have selected the software upgrade installation type, you require the planning and configuration information in this document. Your installation's system programmer must set up the product runtime, IBM WebSphere Application Server OEM Edition for z/OS, and z/OSMF through a configuration shell script that is provided with the product.

For a software upgrade installation, if you accept the system defaults, ServerPac provides customization guidance for configuring z/OSMF. See the copy of *ServerPac: Installing Your Order* that is supplied with your order.

Setting up z/OSMF involves the following work:

- To set up IBM WebSphere Application Server OEM Edition for z/OS, the system programmer runs a WebSphere configuration shell script, which prompts for and

saves configuration settings and creates the necessary jobs to run. Other WebSphere scripts run after the initial script to create the instance of IBM WebSphere Application Server OEM Edition for z/OS and complete the setup.

- To set up z/OSMF, the system programmer invokes a z/OSMF configuration shell script with a series of options. These script invocations perform a number of setup tasks, including setting up the z/OSMF data file system, deploying z/OSMF into IBM WebSphere Application Server OEM Edition for z/OS, and creating sample commands for authorizing users to system resources. During this processing, the script issues messages and creates log statements to indicate the actions performed and any setup errors that are encountered.

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

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

The z/OSMF configuration script creates RACF commands in a REXX exec, which your security administrator can verify and run. Though the script generates RACF commands by default, you can create a REXX exec with equivalent SAF commands if your installation uses another security management product.

The z/OSMF configuration process creates an initial user ID for the z/OSMF administrator. With this user ID, the administrator can log into z/OSMF and add more users and administrators as needed.

More information about security setup is provided in "Establishing security for z/OSMF" on page 55.

Getting started with z/OSMF

After z/OSMF is installed and configured, an authorized user can log into z/OSMF with a Web browser. Your installation's system programmer must provide users with the Web link (URL) to use.

Figure 1 on page 1 displays the login page for z/OSMF. The z/OSMF interface consists of a login area in the top left corner, a navigation area of task categories below the login area, and a work area on the right. More information about the layout of the z/OSMF interface is provided in "Working with the z/OSMF interface" on page 49.

The Welcome task is launched when you open your browser to z/OSMF. After you log into z/OSMF, the Welcome task provides information to help you get started with z/OSMF and learn more about the product, as shown in Figure 3 on page 5.

z/OSMF uses the concept of *Roles* to group similar users for managing user access to tasks. Role definitions can be modified at any time by the z/OSMF administrator through the z/OSMF interface. Though any z/OS user with sufficient RACF authorization can log into z/OSMF, a user must be assigned a role of Administrator or User to start working with z/OSMF tasks. For more information, see "Defining z/OSMF users and roles" on page 54.

Logging into z/OSMF requires a user ID and password (or pass phrase) to authenticate. All actions taken from that browser session after successful

authentication are performed under the identity that was used to log in. The z/OSMF interface customizes this view, based on the user's role definition. As a result, each user's navigation area displays only those tasks for which the user is authorized.

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

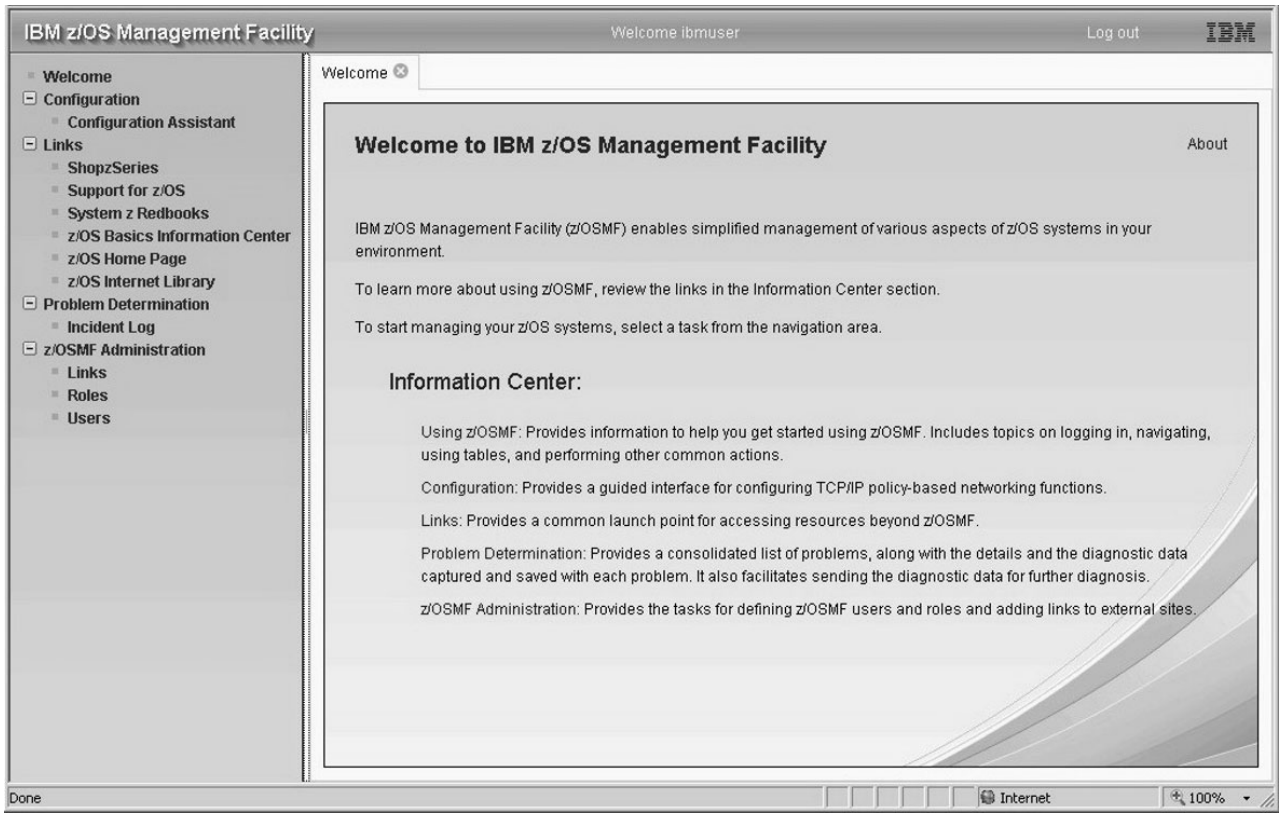


Figure 3. z/OSMF Welcome task (after administrator login)

As shown in Figure 3, z/OSMF V1R11 provides the following categories and related tasks:

Configuration
For z/OS V1R11 systems or later, select this category to view tasks for working with the system configuration. This category contains Configuration Assistant for z/OS Communications Server, which provides a guided interface for configuring TCP/IP policy-based networking functions. An overview of Configuration Assistant is provided in "Configuration Assistant task overview" on page 58.

Links
Select this category to view links to other Web sites for system management tools and information. Some useful links were provided with the installation of z/OSMF. Your installation can add its own links to this category.

Problem Determination
Select this category to view tasks that can help you manage problems on z/OS. This category contains the Incident Log task, which provides a consolidated list of system problems, along with the details and the diagnostic data captured

and saved with each problem. This task also helps you send the diagnostic data to IBM or a vendor for further diagnosis. An overview of the Incident Log task is provided in "Incident Log task overview" on page 60.

z/OSMF Administration
Contains the product administration tasks, such as defining z/OSMF roles and users. This category also allows your installation to define links for other external Web applications and Web sites that users can launch. This allows you to have a single launch point for all of your z/OS management Web applications and Web sites. An overview of the administration tasks is provided in "z/OSMF administration" on page 54.

Information about using z/OSMF is provided in Chapter 4, "Using z/OSMF," on page 49.

Getting help in z/OSMF

z/OSMF provides extensive online help information to assist you with understanding and performing a task, troubleshooting problems, entering information, and using all aspects of z/OSMF. Three types of help are available in z/OSMF: panel-level help, message help, and field-level help. You can access the help information after you have authenticated to z/OSMF.

Panel-level help

Panel-level help provides more details about a panel or dialog box. For example, panel-level help describes each field or column displayed on a panel and the actions you can initiate from a panel. To open panel-level help, click the **Help** link (located in the upper right-hand corner of each panel) or the **Help** button (located near the bottom of each dialog box, if help is available). Details about the panel or dialog box are displayed in a new browser window. The browser window is divided into two sections: the navigation area and the content area. The help information is displayed in the content area. A hierarchical list of z/OSMF-specific help topics is displayed in the navigation area. The active help topic is highlighted in the navigation area so that you can see where it is located within the hierarchy and easily navigate to related information.

Message help

Message help provides more details about a message. Message help includes a detailed explanation of the message, a description of any reason codes that are listed in the message, and suggestions for actions you can implement to resolve the issue. To open message help, click the **message ID** link that is displayed in the message.

Field-level help

Field-level help describes the type of data to enter into a field, the format of that data, and indicates when required information has been omitted. Field-level help is displayed to the right of the field when an error occurs. Also, a status icon is displayed within the field. After you correct the errors, the status icon and the message are removed.

Solving problems in z/OSMF

Information on troubleshooting problems in z/OSMF, including a summary of tools provided to assist with diagnosis, is provided in Chapter 6, "Troubleshooting," on page 71.

Descriptions of the messages you might encounter while using z/OSMF are provided in Chapter 7, "Messages for z/OSMF," on page 107.

Chapter 2. Planning for z/OSMF

Before you begin installing and configuring z/OSMF, determine on which z/OS operating system image you want to install this product. z/OSMF V1R11 can be installed on z/OS Version 1 Release 10 or later. To use the Configuration Assistant task in z/OSMF, your system must be running z/OS V1R11 or later.

Required system software

The following software must be installed on the z/OS host system:

- IBM WebSphere Application Server OEM Edition for z/OS is installed on the z/OS system and the appropriate program directory jobs have been run. You must install IBM WebSphere Application Server OEM Edition for z/OS, even if your system already includes a running instance of WebSphere Application Server for z/OS. This work must be done before you start to configure z/OSMF, as described in this book.
- z/OSMF is installed on the z/OS system and the appropriate program directory jobs have been run.

Before you install z/OSMF, read *Program Directory for z/OS Management Facility*, GI11-2886. This document contains information on high level qualifiers for installation of data sets and product file systems. Make sure that you note these values because they are used later during the configuration process.

Required publications

Before doing the work described in this book, you need to complete the tasks described in the following books:

- *Program Directory for z/OS Management Facility*, GI11-2886, This book describes the material and procedures for installing z/OSMF and for applying the requisite service for this product.
- *IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide, Version 7.0*, GA32-0631. This book provides configuration information for setting up IBM WebSphere Application Server OEM Edition for z/OS as the first part of the configuration process for z/OSMF.

  IBM WebSphere Application Server OEM Edition for z/OS must be configured before you can configure z/OSMF, as described in this book.

z/OS prerequisites for the core functions

The base functions of z/OSMF (referred to as *core functions* in this document) are enabled when you install and configure the z/OSMF product. No additional system customization is needed to use the core functions.

When configured, z/OSMF includes one user ID that is authorized to access z/OSMF as the product administrator. To allow additional 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 execs with RACF commands for authorizing users. More information is provided in Chapter 3, “Configuring z/OSMF,” on page 25.

z/OS prerequisites for the Configuration Assistant task

The Configuration Assistant task is enabled when you install and configure the z/OSMF product. No additional system customization is needed to use this task.

If your installation uses the Windows® desktop version of Configuration Assistant for z/OS Communications Server, you can transfer your existing backing store files into the z/OSMF environment. More information is provided in "Updating z/OS for Configuration Assistant" on page 47.

z/OS prerequisites for the Incident Log task

To use the Incident Log task, you must ensure that a number of z/OS components and facilities are enabled on your system. These functions allow z/OSMF to create diagnostic logs for Incident Log processing.

The setup actions listed in this section are intended for installations that install z/OSMF from a Custom-Built Product Delivery Option (CBPDO) software delivery package, or from a ServerPac order using the software upgrade method of installation. If you install z/OSMF as part of a ServerPac order using the full system replacement method of installation, this setup work is performed for you during the ServerPac post-installation process.

Table 1 summarizes the z/OS system changes that are required or recommended for enabling the Incident Log task.

Table 1. z/OS setup actions for the Incident Log task

	z/OS setup action	Where described	Check when task is completed
1	If your system environment has not been set up with LOGR couple data sets for IBM WebSphere Application Server OEM Edition for z/OS, define these data sets in the sysplex in which z/OSMF is installed.	See "Defining a couple data set for system logger" on page 156.	
2	Define and enable the operations log (OPERLOG) in a system logger log stream.	See "Enabling the operations log (OPERLOG)" on page 158.	
3	Define and enable the LOGREC log stream.	See "Defining and activating the logrec log stream" on page 160.	
4	Define OPERLOG and LOGREC model log streams for diagnostic log snapshots to be obtained by the common event adapter (CEA) component of z/OS.	See "Defining diagnostic snapshot log streams" on page 161.	
5	Set up and configure automatic dump data set allocation (auto-dump).	See "Configuring automatic dump data set allocation" on page 161.	
6	Configure dump analysis and elimination (DAE) to suppress duplicate SVC dumps and use a sysplex-wide scope.	See "Configuring dump analysis and elimination" on page 162.	

Table 1. z/OS setup actions for the Incident Log task (continued)

	z/OS setup action	Where described	Check when task is completed
7	Create a sysplex dump directory.	See "Creating the sysplex dump directory" on page 163.	
8	Ensure that CEA is active.	See "Ensuring that CEA is active" on page 165.	
9	Ensure that System REXX (SYSREXX) is active.	See "Ensuring that System REXX is active" on page 166.	
10	If your installation has chosen to rename a dump data set, ensure that the data set name in the sysplex dump directory is correct.	See "Ensuring that dump data set names are correct" on page 166.	
11	Ensure that SYS1.MIGLIB is APF-authorized.	See "Authorizing the SYS1.MIGLIB data set" on page 167.	

Much of this work might already be done on your system, such as enabling the operations log (OPERLOG) log stream. 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.

Considerations for IBM WebSphere Application Server OEM Edition for z/OS

Before you can configure the z/OSMF product, you must create an instance of IBM WebSphere Application Server OEM Edition for z/OS on your z/OS system. IBM WebSphere Application Server OEM Edition for z/OS is shipped with z/OSMF and provides the application server runtime environment for the product.

For a description of the steps to follow for configuring IBM WebSphere Application Server OEM Edition for z/OS, see *IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide, Version 7.0*, GA32-0631.

When you start z/OSMF for the first time, you might want to have IBM WebSphere Application Server OEM Edition for z/OS configured to use trace options for help with any debugging that might be required. Later, when z/OSMF is functioning correctly, you can deactivate the trace options. For information, see "Enabling trace and logging for z/OSMF" on page 81.

WebSphere administrative console

IBM WebSphere Application Server OEM Edition for z/OS deploys a Web application that is used to configure and manage the WebSphere runtime environment. This application is known as the WebSphere administrative console.

Configuring z/OSMF does not require the use of the WebSphere administrative console. Other tasks related to z/OSMF, however, such as setting the level of logging, will require you to log into the WebSphere administrative console.

The configuration process

The z/OSMF configuration process occurs in three stages:

Configuration stage
During this stage, you run a shell script to create a file of configuration settings for your z/OS system (the configuration file). The script requires that you provide input about your environment and the z/OSMF tasks that you plan to configure. Your can change any values that are not appropriate for your system environment. The script saves your information as variables in a configuration file, which is used as input for subsequent steps in the configuration process. Any settings that you specify in optional override file before invoking the script are incorporated into the resulting configuration file.

Security setup stage
The z/OSMF configuration process generates a REXX exec that contains RACF commands for security definitions and setup. This exec is specific to your system and contains information gathered during the configuration stage. Your security administrator should review and then submit the exec. 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.

Security setup continues with separate script invocations to verify your security setup and initialize or "prime" the z/OSMF data file system.

Deployment stage
The z/OSMF configuration process uses the configuration file that was created in the configuration stage to deploy z/OSMF on your system. The configuration process also verifies your system setup for the tasks that you chose to configure.

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," as you prefer. This script is located in the `/usr/lpp/zosmf/V1R11/bin` directory.

izudflt.cfg
The default configuration file that is provided with z/OSMF. This file contains default configuration values that can be used as a base configuration. This file is located in the `/usr/lpp/zosmf/V1R11/defaults` directory.

izudflt.ovr
The optional override file that is used to replace any of the settings found in the configuration file. Any changes that you make to this file should be completed before you invoke the **izusetup.sh -config** script. A default copy of this file is located in the `/usr/lpp/zosmf/V1R11/defaults` directory, which is read-only. If you use this optional file, you must copy it to a read-write directory, such as `/etc/zosmf`, and modify the file as appropriate for your installation.

Roles and authorities needed during the configuration process

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

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

Table 2 provides an overview of the authorities needed during the z/OSMF configuration process.

Table 2. Authorities needed for configuring z/OSMF on your z/OS system

Action to perform and where described	Invocation	Performed by
"Step 1: Create the initial configuration" on page 27	izusetup.sh -file */etc/zosmf/izuconfig1*.cfg -config [-system *SYSNAME*] *[...other options...]*	Superuser
"Step 2: Run the security commands" on page 31	*/etc/zosmf*/izuconfig1.cfg.rexx	Security administrator
"Step 3: Verify the RACF security setup" on page 33	izusetup.sh -file */etc/zosmf/izuconfig1*.cfg -verify racf	Security administrator
"Step 4: Prime the z/OSMF data file system" on page 34	izusetup.sh -file */etc/zosmf/izuconfig1*.cfg -prime	Superuser
"Step 5: Complete the setup" on page 35	izusetup.sh -file */etc/zosmf/izuconfig1*.cfg -finish	z/OSMF administrator
"Step 6: Access the z/OSMF Welcome task" on page 39	At the end of the z/OSMF configuration process, you can verify the success of your configuration changes by opening your browser to the z/OSMF Welcome task.	

Choosing a script mode: Interactive or fastpath

z/OSMF is configured using a 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 variable settings that are contained in a default configuration file, and can accept an optional override file that contains changes to the default settings that are more appropriate for your environment.

When used in interactive mode, the **izusetup.sh** script presents you with a series of prompts, one for each z/OSMF configuration parameter. All prompts require a response; either an acceptance of the displayed value, or a value that you enter in response to the prompt. If you specify your installation-specific values in an optional override file, the values presented will be those that you have determined to be more appropriate for your environment. Otherwise, you will be presented with the IBM default values (where applicable). Whenever you use the interactive mode, you have an opportunity to change the value in response to the prompt.

When used in fastpath mode, the **izusetup.sh** script runs without any interactive prompting. The script uses the variable values that are specified in the configuration file, with precedence given to any installation-specific values that you supply in the optional override file.

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.

Most installations will find it appropriate to use the **izusetup.sh** script in interactive mode. However, if you prefer to supply the configuration values in a flat file, with no interactive prompting from the script, you should consider using the script in fastpath mode.

Table 3 summarizes the considerations for each mode.

Table 3. 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 all 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 all 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	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 your configuration data is supplied through the configuration file, or the optional override file, or a combination of both files. Or, you need to re-run the configuration process to update an erroneous value in an existing configuration file, and do not want to repeat the prompts.

Considerations for using the script in fastpath mode

Using the fastpath mode requires that you include a configuration file, and, optionally, the override file, **izudflt.ovr**.

If any variables are omitted from the override file, the **izusetup.sh** script checks your specified configuration file for the values. If you omit the override file altogether, the **izusetup.sh** script uses the configuration file only. Here, you must ensure that the configuration file is complete with valid values specified for all of the configuration variables.

You might find the fastpath mode to be useful if you need to re-run the configuration process later to update an erroneous configuration value. Here, instead of repeating the prompts, you can manually update the override file that was used during the previous pass through the process. More information about

this technique is provided in "If you need to repeat Step 1, use the fastpath option" on page 31.

Creating the configuration file

When you run the **izusetup.sh -config** script, you will specify a configuration file to be used for collecting your input values. It is recommended that you name the configuration file `izuconfig1.cfg`. The examples in this document use this name. If you plan to 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 and later for authorizing users to z/OSMF.

If the configuration file already exists, it will be used when you invoke the script. Otherwise, the script creates this file using the values from the default configuration file **izudflt.cfg** as a starting point.

If you retained the configuration file from a previous configuration of z/OSMF, and you wish to re-use some or all of the values for this configuration, you can select that file to use.

For descriptions of the variables provided in the default configuration file, see Appendix D, "Default configuration file, and default override file variables," on page 173.

Using an override file

You can choose to supply your configuration settings in an editable file called the override file. The override file allows you to gather your installation values in one place (the override file) and have this file serve as input to the configuration process. As an added benefit, you might find that having an override file provides you with a convenient means for gathering and reviewing configuration data at your installation before proceeding with the z/OSMF configuration.

During the configuration process, you can specify the override file as input to have your values override the corresponding IBM defaults. The resulting configuration process will present your override values for each of the script prompts. Press Enter to accept each value, or type an alternative value, as needed.

z/OSMF includes a default override file, **izudflt.ovr** in the `/usr/lpp/zosmf/V1R11/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, such as `/etc/zosmf`, and edit the file with an editor of your choice. It is recommended that you name the override file `izudflt.ovr`.

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

For the content of the override file that is supplied with z/OSMF, see Appendix D, "Default configuration file, and default override file variables," on page 173.

Planning worksheets for z/OSMF

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

To save time during the configuration process, have this information at hand when you perform the steps in Chapter 3, "Configuring z/OSMF," on page 25.

The amount of information you need to gather depends on whether your installation plans to configure the Incident Log task in addition to the base functions of z/OSMF (referred to as *core functions* in this document). For systems running z/OS V1R11, configuration of the Configuration Assistant task is included in the process that configures the core functions.

Input for the core functions

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

Configuring the z/OSMF core functions requires that you have the following information available (Table 4). The **izusetup.sh** script saves this input as variables in a configuration file for use throughout the configuration process. Table 4 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.

Table 4. Worksheet for the core functions variables

Input	Description	Variable name	Default value	Your value
System name.	Name of your z/OS system (up to 8 characters)	IZU_SYSNAME_ PREFIX	@SYSNAME, which equates to the value of the *&SYSNAME* symbol for your z/OS system.	
z/OSMF root code directory path.	z/OSMF product file system that was created earlier when you ran the jobs described in the z/OSMF Program Directory.	IZU_CODE_ROOT	`/usr/lpp/zosmf/V1R11`	
Mount point of the z/OSMF data file system.	Mount point (the full pathname) for the z/OSMF data file system.	IZU_DATA_DIR	`/var/zosmf/data`	
The directory for the z/OSMF configuration.	The directory (the full pathname) for the z/OSMF configuration.	IZU_CONFIG_DIR	`/etc/zosmf`	
Name of the z/OSMF data file system.	z/OSMF data file system. For considerations regarding the use of a shared data file system, see "Planning a backup instance of z/OSMF" on page 22. You may pre-create the data file system, but you should ensure that the name is configured for this variable, and that you can mount this file system at the IZU_DATA_DIR mount point.	IZU_DATA _FS_NAME	IZU.SIZUDATA	

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

Input	Description	Variable name	Default value	Your value
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	
Volume name for the z/OSMF data file system, or SMS managed storage.	Volume serial number (VOLSER) of the DASD to be used for creating the z/OSMF data file system. Specify * to let SMS select a 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. If you specify a volume, the volume must be online when you begin the configuration process described in Chapter 3, "Configuring z/OSMF," on page 25.	IZU_DATA_FS_ VOLUME	*	
Allocation size (in cylinders) for the z/OSMF data file system.	Initial space allocation, in cylinders, for the z/OSMF data file system data set. The script uses 90% of this value for the primary allocation and 10% for the secondary allocation. The minimum suggested size (and default) is 100 cylinders, which causes the script to use 90 cylinders for the primary allocation and 10 cylinders for the secondary allocation.	IZU_DATA_FS_SIZE	100	
Group name for the z/OSMF administrator.	Primary group for z/OSMF administrator identity.	IZU_ADMIN_GROUP	ZOSMFGRP	
Group 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 *z/OS Security Server RACF Security Administrator's Guide*.	IZU_ADMIN_GROUP _GID	9003	
z/OSMF administrator user ID.	User ID for the z/OSMF administrator.	IZU_ADMIN_NAME	ZOSMFAD	
z/OSMF administrator UID or AUTOUID.	UID for the z/OSMF administrator. Instead of specifying the UID value, you can enter AUTOUID to have RACF automatically generate a unique ID. For more information about the AUTOUID operand, see *z/OS Security Server RACF Security Administrator's Guide*.	IZU_ADMIN_UID	9001	

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

Input	Description	Variable name	Default value	Your value
z/OSMF administrator home directory.	Home directory for the z/OSMF administrator. Do not specify a home directory to be created under the mount point of the z/OSMF data file system, which by default is `/var/zosmf/data`. The mount point owner and group permissions do not allow the z/OSMF administrator ID access.	IZU_ADMIN_HOME	`/u/zosmfad`	
z/OSMF administrator shell program path.	Program path for the z/OSMF administrator identity for z/OS UNIX system services.	IZU_ADMIN_ PROGRAM	`/bin/sh`	
z/OSMF administrator proc name.	TSO/E logon procedure to be used by the z/OSMF administrator.	IZU_ADMIN _PROC	NO.DEFAULT.VALUE You must provide a value for this.	
z/OSMF administrator account number.	User account number for z/OSMF administrator identity.	IZU_ADMIN_ ACCOUNT	NO.DEFAULT.VALUE You must provide a value for this.	
z/OSMF administrator region size.	Region size for z/OSMF administrator identity.	IZU_ADMIN _REGION	2096128	
Directory path and name of the WebSphere Application Server configuration file.	Full pathname of the WebSphere Application Server response file. Your installation created this file when customizing IBM WebSphere Application Server OEM Edition for z/OS for this system. If you omit this value, the configuration process prompts you for the WebSphere values individually (see Table 6 on page 29.	IZU_WAS_CONFIG _FILE_LOCATION	/etc/ zWebSphereOEM/ V7R0/conf/ CONFIG1/ CONFIG1. responseFile	
Path of the WBEM root directory	Root directory path of the CIM server installation.	IZU_WBEM_ROOT	`/usr/lpp/wbem`	

Input for the Incident Log task

To enable the Incident Log task, you must provide additional information to the **izusetup.sh** script. This process begins with your response to the script prompt "`Do you want to configure the Incident Log task?`". If you reply Y, you are prompted for additional values for setting up your system for the Incident Log task.

For your planning purposes, Table 5 on page 19 shows the information you should have at hand when running the configuration script. Table 5 on page 19 includes the variable names and defaults, if any, for these values.

Table 5. Worksheet for the Incident Log task variables

Input	Description	Variable name	Default value	Your value
Do you want to configure the Incident Log task?	Specify Y or N to indicate whether you require system setup for the Incident Log task. • If you reply Y, you are prompted for additional values for setting up your system for the Incident Log. The system changes include initializing a CEAPRMxx parmlib member with options set for Incident Log processing. • If you reply N, the script will not prompt you for the additional values (below). The Incident Log task will not be usable in z/OSMF.	IZU_INCIDENT_LOG	Y	
Has the Common Information Model (CIM) server been set up? [Y/N]	Specify Y or N to indicate whether you already have a CIM server set up for this system. • If you reply Y, the script will attempt to use your existing CIM server. You are prompted for the CIM administrator user ID for your installation. • If you reply N, you are prompted for additional CIM-related values to configure a CIM server for your installation.	IZU_CIM_SETUP	N	
	CIM administrator user ID for your installation.	IZU_CIM_ADMIN_NAME	ZOSMFAD	
	CIM group name	IZU_CIM_GROUP_NAME	CIMGP	
	CIM group GID for the CIM group admin identity. Instead of specifying the GID value, you can enter AUTOGID to have RACF automatically generate a unique ID. For more information about the AUTOGID operand, see *z/OS Security Server RACF Security Administrator's Guide*.	IZU_CIM_GROUP_ID	5321	
CEA UID or AUTOUID.	Common event adapter (CEA) UID. To find the CEA UID, enter the LISTUSER command in TSO/E, as follows: `LU CEA OMVS` Instead of specifying the GID value, you can enter AUTOUID to have RACF automatically generate a unique ID. For more information about the AUTOUID operand, see *z/OS Security Server RACF Security Administrator's Guide*.	IZU_CEA_UID	9002	

Table 5. Worksheet for the Incident Log task variables (continued)

Input	Description	Variable name	Default value	Your value
Group for accessing CEA resources.	Group name to use for allowing the Incident Log task to access CEA functions.	IZU_CEA _GROUP _NAME	CEAGP	
CEA group GID or AUTOGID.	CEA group GID to use for the CEA group administrator identity. Instead of specifying the GID value, you can enter AUTOGID to have RACF automatically generate a unique ID. For more information about the AUTOGID operand, see *z/OS Security Server RACF Security Administrator's Guide*.	IZU_CEA _GROUP _ID	6321	
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.	IZU_IEA_PARM _NAME	ZM	
Suffix of the CEAPRMxx parmlib member.	Two-character suffix of a new CEAPRMxx parmlib member to be used for enabling captures or "snapshots" of the system logs. Two characters are required. If this member already exists, the script prompts you to choose whether to overwrite the existing member.	IZU_CEA_PARM _NAME	01	
Country code.	IBM-defined country code for your site (3-character numeric).	IZU_COUNTRY _CODE	NO.DEFAULT.VALUE You must provide a value for this.	
Branch.	IBM-defined branch code (or branch office) for your site (3-character alphanumeric).	IZU_BRANCH _CODE	NO.DEFAULT.VALUE You must provide a value for this.	
What STORAGE option do you want to use?	Indicates where CEA is to store the snapshot information. • Enter V to specify one or more volumes. • Enter S to specify one or more SMS storage classes. In response, the script prompts for each volume (up to seven) or a single storage class name. Specify each value on a separate line as prompted.	IZU_STORAGE _VALUE	NO.DEFAULT.VALUE You must provide a value for this.	
Data set name for your parmlib member CEAPRM00.	Source parmlib 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_PARMLIB _SOURCE	SYS1.PARMLIB	

Table 5. Worksheet for the Incident Log task variables (continued)

Input	Description	Variable name	Default value	Your value
Data set name for updated parmlib members.	Target parmlib data set that will contain the newly created members for Incident Log processing (IEADMC*nn* and CEAPRM*nn*).	IZU_PARMLIB	SYS1.PARMLIB	

Using your existing CIM server configuration

If your installation has already configured the CIM server on this system, you can use the existing CIM server configuration rather than allowing z/OSMF to create one. If so, respond `Y` to the script prompt *"Has the Common Information Model (CIM) server been set up? [Y/N]"*; see Table 5 on page 19.

Using your existing CIM server configuration requires that you perform a few additional steps later in the configuration process. The steps, which are summarized below, are described elsewhere in this document:

- Ensure that the CIM administrator and z/OSMF administrator are authorized to the CIM directories; see "Step 2: Run the security commands" on page 31.
- Update the LIBPATH setting to include the directory `/usr/lib`; see "Using your existing CIM server configuration" on page 32.
- Register CIM providers; see "Registering the CIM providers" on page 38.

For information about setting up the CIM server, see z/OS Common Information Model User's Guide, SC33-7998.

Preparing your workstation for z/OSMF

To work with z/OSMF, your workstation requires Microsoft® Windows XP. No other versions of Windows are supported at this time.

The z/OSMF interface is optimized for a screen resolution of 1024 by 768 pixels or higher. Therefore, it is strongly recommended that you set your screen resolution to 1024 by 768 pixels or higher; otherwise, you might experience some clipping of content.

To access z/OSMF on the z/OS system, your workstation requires one of the following Web browsers:

- Mozilla Firefox Version 2 or Version 3.0 (minimum service level 3.0.6).
- Microsoft Internet Explorer Version 6 or Version 7.

For multiple sessions on the z/OS host system, if you are using Internet Explorer, you must launch a new copy of Internet Explorer for each session. If you are using Firefox, create a Firefox profile for each session. For information about creating multiple Firefox profiles, see "Using multiple Mozilla Firefox sessions" on page 22.

z/OSMF includes an environment checker tool to help you verify your browser settings at any time. For more information, including recommendations for specific browsers, see "Verifying your workstation with the environment checker" on page 72.

Using multiple Mozilla Firefox sessions

IBM WebSphere Application Server OEM Edition for z/OS uses session cookies to track which users are logged in from a specific browser. Mozilla Firefox allows for only one session cookie per site and per instance. If you wish to have multiple users logged in from a single location, or if you wish to log into multiple servers at the same host name, you might need to configure your browser to accommodate multiple session cookies.

To create a profile in Firefox, close all existing sessions and do the following:

1. From the Run prompt in Windows, enter: `firefox -p`. A dialog box opens to allow you to Create Profile, Rename a Profile, or Delete a Profile.
2. Select the **Create Profile** option and define a new profile.
3. Repeat this step again to create a second profile.
4. Ensure that the **'Don't ask at startup'** check box is not selected.
5. Select one of the users (user1) and select Start Firefox.
6. To start a second browser with a new profile, enter the following command from the Run prompt: `firefox -p "user2" -no-remote`.

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

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

By default, the z/OSMF administrator home directory is `/u/zosmfad`. If this file system is automount managed, you must pre-create it before running the script described in "Step 4: Prime the z/OSMF data file system" on page 34.

For more information about the automount facility, see *z/OS UNIX System Services Planning*, GA22-7800.

Planning a backup instance of z/OSMF

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

If you plan to create a backup instance of z/OSMF, consider the following when setting up your primary instance of z/OSMF:

- If your primary instance of z/OSMF uses a shared data file system (one that is read/write accessible from other systems in the sysplex), you will have fewer steps to follow to configure a backup instance of z/OSMF and for performing a takeover from the primary instance of z/OSMF to the backup. If you use a shared RACF database, the takeover procedure is further simplified because the backup instance can use the same RACF user IDs and groups as your primary instance.
- If your primary instance of z/OSMF uses a non-shared data file system (one that is read/write accessible from only the host z/OS system), takeover from primary instance of z/OSMF to a backup will require that you unmount the data file system on the host z/OS system and mount it on the backup system. z/OSMF includes a shell script to help you do this work.

For information about creating backup instances of z/OSMF, see Chapter 5, "Creating another instance of z/OSMF," on page 63.

Planning service updates for z/OSMF

As with other IBM software products, IBM ships service for z/OSMF in the form of program temporary fixes or PTFs. Applying service to z/OSMF involves installing new product files in place of your existing product files.

For z/OSMF, a PTF specifies whether any configuration scripts should be run, whether a redeployment of the product Enterprise Archive (EAR) file is required, and whether your installation must restart the IBM WebSphere Application Server OEM Edition for z/OS runtime instance. Any actions that you need to take are documented as a ++HOLD in the PTF.

For example, a PTF might require you to redeploy the z/OSMF EAR file (`izuzosmf.ear`). Here, you must ensure that IBM WebSphere Application Server OEM Edition for z/OS is not running.

Then, run the **izusetup.sh** script to begin the deployment. As supplied by IBM, this script resides in the following directory, which was created when you installed z/OSMF:

```
/usr/lpp/zosmf/V1R11/bin
```

Run the script as follows from a user ID with z/OSMF administrator authority:

```
izusetup.sh -file /etc/zosmf/izuconfig1.cfg –core
```

When used with the `-core` option, the script deploys the z/OSMF core functions into the instance of IBM WebSphere Application Server OEM Edition for z/OS. In this example, and throughout this document, *izuconfig1*.cfg is the name of the file used to save your configuration settings. If you installed z/OSMF as part of a ServerPac order, however, the configuration file is named *serverpac.cfg*.

The configuration file is stored, by default, in the `/etc/zosmf` directory.

Chapter 3. Configuring z/OSMF

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

Attention: It is strongly recommended that you thoroughly review all of the steps in this chapter before the performing the configuration.

Users of this information

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

Follow the steps in this chapter to configure the product. These setup actions are required for installations that install z/OSMF from a Custom-Built Product Delivery Option (CBPDO) software delivery package, or from a ServerPac order for which the software upgrade installation type is used.

If you installed z/OSMF as part of a ServerPac order, and you selected the full system replacement installation type, z/OSMF is configured for you through a ServerPac post-installation job using the IBM-supplied script **izuserverpac.sh** (which is invoked with an argument that represents all of the input variables). The ServerPac post-installation job creates a default instance of z/OSMF that is ready to use. It is recommended that you review the setup actions in this chapter to ensure that they are correct for your environment.

Before you begin

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

1. z/OSMF is installed on your z/OS system and the appropriate program directory jobs have been run. See *Program Directory for z/OS Management Facility*, GI11-2886.
2. IBM WebSphere Application Server OEM Edition for z/OS is installed and configured on your z/OS system but is not currently running. The installation and configuration steps are described in *Program Directory for z/OS Management Facility*, GI11-2886, and *IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide, Version 7.0*, GA32-0631.
3. If your installation plans to set up the Incident Log task at this time, ensure that your z/OS system meets the requirements listed in "z/OS prerequisites for the Incident Log task" on page 10.
4. Ensure that you have collected the list of variables and other information described in "Planning worksheets for z/OSMF" on page 16. You will supply these values as input to the configuration script that you use to set up z/OSMF.

Where to find the script

As supplied by IBM, the **izusetup.sh** script resides in the following directory, which was created when you installed z/OSMF on your z/OS system:

```
/usr/lpp/zosmf/V1R11/bin
```

This script creates a number of REXX execs and report files, which are written to the `/etc/zosmf` directory by default.

This directory is created when you run the **izusetup.sh** script with the -config option.

How to access and run the script

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

To run the script, you must first be able to access it. Ensure that the script directory is specified in your shell environment path. You can do this by adding the directory to your path, or by adding '.' to the path, which indicates that the current working directory is to be used. For example:

```
/usr/lpp/zosmf/V1R11/bin
```

To add the script directory to your path, enter the following command from z/OS UNIX:

```
export PATH=.:/usr/lpp/zosmf/V1R11/bin:$PATH
```

To add the current working directory to your path, enter the following commands from z/OS UNIX:

```
cd /usr/lpp/zosmf/V1R11/bin
export PATH=$PATH:.
```

You can display your PATH variable by running the following command from z/OS UNIX:

```
echo $PATH
```

For more information about the z/OS UNIX shell and how to switch between the shell and TSO/E, see *z/OS UNIX System Services User's Guide*, which is available online in the IBM z/OS Internet Library.

Removing command aliases

The z/OSMF configuration script makes use of the built-in z/OS UNIX shell commands and defaults. If your z/OS UNIX shell profile (.profile) or system profile alters or aliases the shell commands cp, mv, or rm, you must remove the aliases before running the script.

To remove an alias, enter the following command from the z/OS UNIX shell:

```
unalias <alias>
```

Thereafter, for the duration of the session, the shell does not perform alias substitution when you specify the particular shell command.

Step 1: Create the initial configuration

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

About this step

The **izusetup.sh** script uses the input you supply, based on your environment and the z/OSMF tasks that you plan to configure. You gathered these values earlier in "Planning worksheets for z/OSMF" on page 16. The script saves your input in the configuration file, which is used as input to subsequent script invocations.

As described in "Choosing a script mode: Interactive or fastpath" on page 13, you can run the **izusetup.sh** script either interactively or "quietly" (the fastpath option). Usually, you will find it appropriate to use this script in interactive 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, you might prefer to supply the configuration values in a flat file, with no interactive prompting from the script. For more about these considerations, see "Choosing a script mode: Interactive or fastpath" on page 13.

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

- Creates a file for storing your configuration information (the configuration file).

  If you retained the configuration file from a previous configuration of z/OSMF, and you wish to re-use some or all of the values for this configuration, you can select that file to use when you invoke this script.
- If the z/OSMF data file system is not already allocated and mounted, the script allocates the data file system and mounts it at the mount point you specify (see Table 4 on page 16). The default mount point is `/var/zosmf/data`.
- The script creates a REXX exec with RACF commands that your security administrator can use to secure the z/OSMF functions and tasks, and create the z/OSMF administrator user ID (ZOSMFAD, by default). If you specify that the script is to set up the Incident Log task, the generated REXX exec will include the RACF commands that your security administrator can use to create security definitions for the CIM server, CEA, and other system components, and the security definitions that allow the z/OSMF administrator to access and run the Incident Log task.

Before running the script

If you plan to configure the Incident Log task, you should have completed some z/OS system setup tasks before running this script. Use the checklist in "z/OS prerequisites for the Incident Log task" on page 10 to verify that all of these setup tasks have been completed. Information about these tasks is provided in Appendix A, "z/OS system setup for z/OSMF," on page 155.

Running the script

Authority

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

Environment

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

Location

By default, the script resides in the following directory:

`/usr/lpp/zosmf/V1R11/bin`

Invocation

Run the script as follows:

```
izusetup.sh -file <pathname/filename>.cfg -config [-system <SystemName>]
[-overridefile <overridefilename>] [-fastpath]
```

Figure 4. izusetup.sh syntax

Where:

- *pathname/filename*.cfg is the configuration file. By default, the configuration file is created in the directory `/etc/zosmf`.

  If this file exists, the script will use it. Otherwise, the script creates this file (by default, in the directory `/etc/zosmf`).

  You can use an existing configuration file, if you retained one from a previous configuration of z/OSMF, and you wish to re-use some or all of the values for this configuration.
- *SYSNAME* is the system on which z/OSMF is to be configured. If you omit this value, the script will prompt you for it.
- *overridefilename* identifies an optional override file to be used to substitute your installation specific values in place of the IBM default values.

For descriptions of the options that you can specify on izusetup.sh, see Appendix C, "izusetup.sh script," on page 171.

Using the script interactively

When used in interactive mode (that is, without the fastpath option specified), this script prompts you for the installation-specific values that you gathered earlier in "Planning worksheets for z/OSMF" on page 16.

If necessary, you can exit from the interactive session before completing it. To do so, enter the CNTRL-C key combination. The script will save your in-progress configuration file up to the point at which you exited.

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

- The script prompts you for a file name to use for saving your configuration settings. Enter a name for this file, for example: */etc/zosmf/izuconfig1*.cfg. Choose a name that is easy to remember and make note of it. You will need to specify this name several times during the z/OSMF configuration process and later for authorizing users to z/OSMF. You might also need the configuration file again in the future for setting up additional instances of z/OSMF, as described in Chapter 5, "Creating another instance of z/OSMF," on page 63.
- To use an existing configuration file, enter Y in response to the next script prompt to overwrite the existing configuration file. If you choose to overwrite the file, your changes will be stored in that file (you might want to back up the contents of that file before invoking the configuration script in this manner). If you want to create another configuration file, you can specify a new file name when prompted by the "save file" message.
- The script prompts you for a number of installation-specific values needed for configuration, such as the z/OSMF data file system, administrator ID default

group and home directory, root directory path of the application server, and the other values you collected earlier; see "Input for the core functions" on page 16.

Note that the z/OSMF administrator home directory (IZU_ADMIN_HOME) is set to `/u/zosmfad` by default. In many installations, this value should be replaced with an alternative directory.

- Some values require that you provide a unique UID or GID. Instead of specifying these identifiers, you can specify the AUTOUID or AUTOGID operand (as appropriate) to have RACF automatically generate a unique ID for you. For more information about AUTOUID and AUTOGID, see *z/OS Security Server RACF Security Administrator's Guide*.
- The script prompts you for the directory path and name of the WebSphere Application Server response file. Your installation created this file earlier when installing IBM WebSphere Application Server OEM Edition for z/OS. If you cannot supply this value, for example, because the response file is not accessible or no longer exists, the script will prompt you for the following WebSphere values (Table 6).

Table 6. WebSphere response file values

WebSphere value	Description	Variable name	Default
zConfigurationGroup	WebSphere application server group.	IZU_APPSERVER _GROUP	WSCFG1
zConfigMountPoint	WebSphere root directory path of the application server.	IZU_APPSERVER _ROOT	/zWebSphereOEM/ V7R0/config1
zSAFProfilePrefix	WebSphere SAF profile prefix.	IZU_WAS_PROFILE _PREFIX	BBNBASE
zClusterTransition Name	WebSphere cluster transition name.	IZU_CLUSTER _TRANSITION _NAME	BBNC001
zCellShortName	WebSphere application server cell short name.	IZU_CELL_SHORT _NAME	BBNBASE
zServantUserid	WebSphere application server servant region user ID.	IZU_SERVANT _USERID	WSSRU1
zControlUserid	WebSphere application server control region user ID.	IZU_CONTROL _USERID	WSCRU1

The content of the WebSphere Application Server response file is described in *IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide, Version 7.0*, GA32-0631.

- If you want to enable the Incident Log task, reply Y to the prompt that asks whether you want to configure the Incident Log. Then supply the values needed for the Incident Log, such as whether the CIM server is already configured, the suffix of the CEAPRMxx member to be used for Incident Log processing, the volume or SMS STORAGE class to be used for storing diagnosis snapshots, and the other values you collected earlier in "Input for the Incident Log task" on page 18.

- If you choose to bypass the setup of the Incident Log task, understand that adding this task at a later time will require you to repeat the entire z/OSMF configuration process, beginning with this script.
- The script prompts you for a source parmib data set for your existing CEAPRM00 member. Therefore, the user ID that you use to run this script must have READ access to the source parmlib data set.
- The script prompts you for a target parmlib data set to use for creating the new members for Incident Log processing (IEADMCnn and CEAPRMnn). This parmlib data set cannot be edited or allocated to a user or job while this 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. Your installation's system programmer can later manually copy from this interim place into the active parmlib.

Using the script in fastpath mode

To avoid prompting altogether, 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 or the override file (or the combination of both files), are complete and correct for your installation. When you specify the -fastpath option during the configuration process, you are not prompted for new values for the configuration variables.

The -fastpath option assumes that all of your configuration values can be found through the aggregation of the configuration file and your override file (if provided). The script uses these values as you provide them. Omitted values will cause the script to end with errors.

If an override file is used in fastpath mode, you must ensure that the variables specified in the override file are set to valid values for your installation. Some variables are initially set to the following value, which is not a valid setting: `NO.DEFAULT.VALUE`. If these variables are not set to valid values, you must manually update the override file before invoking the **izusetup.sh** script with the -fastpath parameter. If any variables are omitted from the override file, the **izusetup.sh** script checks your specified configuration file for the values.

Results

You can view the script output messages in the following log file:
`/etc/zosmf/izusetup_<date>_<time>.log`

On completion, the **izusetup.sh** script creates an updated configuration file, and saves that file in the directory that is created based on the name you specified for your configuration. For example, if your IZU_CONFIG_DIR variable is set to `/etc/zosmf` and you specified `izuconfig1.cfg` for the name of your configuration file, the updated configuration file is called `izuconfig1.cfg` and is located in the `/etc/zosmf` directory.

The script also creates a REXX exec with RACF commands for creating the necessary security definitions for your installation. The exec name is a concatenation of your configuration file name and ".rexx". If you use "izuconfig1.cfg" as your configuration file name, for example, the rexx exec is created as "izuconfig1.cfg.rexx."

The exec is stored in the following location by default:

/etc/zosmf/

Information about using the **izuconfig1.cfg.rexx** exec is provided in the next step: "Step 2: Run the security commands."

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

If you need to update an erroneous configuration value, you must re-run the izusetup.sh script in -config mode. However, instead of repeating the prompts, you can include the –fastpath option on the **izusetup.sh** invocation. The fastpath version of the **izusetup.sh** script bypasses the prompt session, and uses the updated configuration file and override file (if provided) from the previous pass as input.

To re-run the configuration of z/OSMF using the -fastpath option, enter the following command:

```
izusetup.sh -file /etc/zosmf/izuconfig1.cfg -config
-overridefile /etc/zosmf/izudflt.ovr -fastpath
```

Step 2: Run the security commands

This section describes the REXX exec **izuconfig1.cfg.rexx**. In short, this exec contains RACF commands for securing the z/OSMF core functions and tasks.

About this step

The REXX exec **izuconfig1.cfg.rexx** contains sample RACF commands that your installation's security administrator can use to secure the z/OSMF functions and tasks, and create the z/OSMF administrator user ID (ZOSMFAD, by default).

The contents of the exec depends on whether your installation has selected to configure the Incident Log task, and, if so, whether to configure the CIM server or use an existing CIM server setup. For your reference, Appendix H, "Security exec examples," on page 189 contains the sample REXX output that would be created for each of these possible scenarios. The exec also contains commented sections for additional authorizations that might be useful for your installation. These sections should be reviewed by your security administrator and uncommented as needed.

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

Before running the exec

These commands should be reviewed by your security administrator and modified as needed for your installation's environment. By default, the exec resides in this directory: /etc/zosmf/.

The common event adapter (CEA) component of z/OS has security profiles for protecting different portions of its processing. As supplied by IBM, this exec provides CEA group access to CEA.CEAPDWB* in the SERVAUTH class. For the profiles included in this group, see Appendix F, "Common event adaptor (CEA) security profiles," on page 181.

Running the exec

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

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

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

Location
By default, the exec resides in the following directory:

```
/etc/zosmf/
```

Invocation
From on OMVS session, do the following:

1. Make `/etc/zosmf/` your active directory. For example:

   ```
   cd /etc/zosmf
   ```

2. Run the exec, as follows:

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

Results

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

Using your existing CIM server configuration

If you selected to use your existing CIM server configuration, rather than allow the **izuconfig1.cfg.rexx** exec to configure the CIM server for you (see Table 5 on page 19), you have some additional steps to perform before continuing to the next step.

After the exec completes, do the following:

- Ensure that the CIM administrator user ID and the z/OSMF administrator user ID have write access to the CIM directories and any associated subdirectories. By default, these are the following directories: `/var/wbem` and `/etc/wbem`.
- Start the CIM server. Or, if the CIM server is already running, restart it. Observe the following considerations:
  - If you start the CIM server from MVS as a started task, ensure that the LIBPATH setting defined in the CIM server environment file (by default, `/etc/wbem/cimserver.env`) contains this directory in its path: `/usr/lib`
  - If you start the CIM server from the z/OS UNIX shell, ensure that the LIBPATH setting in the .profile for the CIM administrator contains this directory in its path: `/usr/lib`
- Ensure that your CIM server is started automatically at IPL time, if you have not done so already.

For information about customizing your CIM server start-up procedure, and details on how to set environment variables for the CIM server, see z/OS Common Information Model User's Guide, SC33-7998.

Step 3: Verify the RACF security setup

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

About this step

The **izusetup.sh** script verifies the RACF security setup actions that were performed in the previous steps.

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

Running the script

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

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

Location
By default, the script resides in the following directory:

```
/usr/lpp/zosmf/V1R11/bin
```

Invocation
Run the script as follows:

```
izusetup.sh -file /etc/zosmf/izuconfig1.cfg -verify racf
```

izuconfig1.cfg is the configuration file that you created previously in "Step 1: Create the initial configuration" on page 27. If you omit this value, the script will fail.

Note: You might need your security administrator to run this script.

Results

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

```
/etc/zosmf/izusetup_<date>_<time>.log
```

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

```
/etc/zosmf/izuracfverify.report
```

Have your installation's security administrator review this file for any areas that might require corrective action on your part.

As a possible technique for verifying the completion of the script, you can edit the report file and search for z/OSMF messages (IZU*nnnnn*). Each message should end with a reason code of zero.

Step 4: Prime the z/OSMF data file system

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

About this step

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

- Initializes or "primes" the z/OSMF data file system, which is mounted by default at `/var/zosmf/data`
- Changes the permissions and ownership of the directories and files in `/var/zosmf/data`
- Creates the home directory for the z/OSMF administrator, if one does not already exist. By default, this directory is `/u/zosmfad`
- Changes ownership and permissions for the other directories that z/OSMF uses. For example, if you specified earlier that the CIM server was to be set up for Incident Log task processing, this script changes ownership and permissions for the CIM directories.

Priming the data file system can be done only once.

Before running the script

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

Running the script

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

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

Location
By default, the script resides in the following directory:

```
/usr/lpp/zosmf/V1R11/bin
```

Invocation
Run the script as follows:

```
izusetup.sh -file /etc/zosmf/izuconfig1.cfg -prime
```

izuconfig1.cfg is the configuration file that you created earlier in "Step 1: Create the initial configuration" on page 27. If you omit this value, the script will fail.

Results

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

```
/etc/zosmf/izusetup_<date>_<time>.log
```

On completion, the script primes the z/OSMF data file system, and creates the necessary directories and files, as described previously. The script records the results of this invocation in a log file called **izuprime_*configfilename*.log**, which is stored by default in the `/etc/zosmf/` directory.

Step 5: Complete the setup

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

About the script

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

- Registers z/OSMF with IBM WebSphere Application Server OEM Edition for z/OS, which includes creating a symbolic link "`${IZU_APPSERVER_ROOT}/AppServer/properties/version/zosmf.registrar`" to `/usr/lpp/zosmf/V1R11/bin/zosmf.register`".
- Updates the WebSphere Application Server configuration. For a list of the updates, see Table 19 on page 177.

The script also prepares your z/OS system for running the Incident Log task, if you chose to configure this task earlier. Specifically, the script performs the following z/OS setup actions:

1. If you replied N to the script prompt "Has the Common Information Model (CIM) server been set up [Y/N]?" , the script sets up and starts the CIM server. Otherwise, the script attempts to use your existing CIM server. To ensure that your CIM setup meets the requirements for z/OSMF, see "Using your existing CIM server configuration" on page 21.
2. Copies the IEADMCnn member to the installation parmlib you specified earlier.
3. Copies the IBM-supplied CEAPRM00 member to the installation parmlib you specified earlier and modifies it. The new CEAPRMnn member:
   - Defines HLQ(CEA) and SNAPSHOTS(Y) to enable captures of the system logs
   - Sets the IBM branch and country code values for your installation
   - Defines the storage value for parmlib (SMS class or string of volume names).
4. Activates the new CEAPRMnn member.

Lastly, the script verifies the setup for all z/OSMF functions and tasks. If you configured the Incident Log task, the script runs an installation verification program (IVP) that verifies the setup of z/OS system components such as:

- Sysplex dump directory
- System logger
- Common event adapter (CEA)
- System REXX.

The script checks that all necessary steps were carried out, and creates a report indicating any areas that might require further action on your part.

Before running the script

Before running this script, you must do the following:

1. Ensure that your z/OS system has been properly configured for the Incident Log task; see Table 1 on page 10.
2. Create a password for the z/OSMF administrator user ID. For RACF, you can use a command like the following to assign a password to ZOSMFAD:

   ```
   ALU ZOSMFAD PASSWORD(PutYourPasswordHere) NOEXPIRED
   ```

3. Ensure that IBM WebSphere Application Server OEM Edition for z/OS is **not** running. To do so, try displaying the WebSphere address space; enter a command like the following from System Display and Search Facility (SDSF) on your z/OS system: `d a,bbn*`

   If IBM WebSphere Application Server OEM Edition for z/OS is active, you must shut it down before running the script. To do so, use the STOP command, for example, `P BBN7ACRS`. For more information about starting and stopping IBM WebSphere Application Server OEM Edition for z/OS, see *IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide, Version 7.0*, GA32-0631.

The user ID that runs this script must be authorized on the z/OS system (for example, through RACF) to create members in the target parmlib data set that you specified earlier in "Step 1: Create the initial configuration" on page 27. By default, this data set is SYS1.PARMLIB.

Alternatively, you might have selected an interim or temporary parmlib data set to be used if you did not want your system's active parmlib data set to be updated directly by the script (perhaps in accordance with the change control procedures at your site). If so, your installation's system programmer must manually copy from this interim place into the active parmlib after this script completes.

Optional: For experienced installers of WebSphere Application Server for z/OS, you can update several WebSphere settings if the default values are not acceptable for your environment. For information, see Appendix E, "Modifying values for the WebSphere configuration," on page 177. In most cases, you should not need to change these values.

Running the script

Authority

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

Environment

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

Location

By default, the script resides in the following directory:

```
/usr/lpp/zosmf/V1R11/bin
```

Invocation

Run the script as follows:

```
izusetup.sh -file /etc/zosmf/izuconfig1.cfg -finish
```

izuconfig1.cfg is the configuration file that you created earlier in "Step 1: Create the initial configuration" on page 27. If you omit this value, the script will fail.

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

Results

The script writes output messages to some or all of the following log files, depending on which z/OSMF tasks have been configured:

- `izusetup_<date>_<time>.log`
- `izuadmin_<date>_<time>.log`
- `izucimconfig_<date>_<time>.log`
- `izuincidentlogconfig_<date>_<time>.log`
- `izuincidentlogverify_<date>_<time>.log`

These log files reside in the `/etc/zosmf` directory by default.

If you selected to configure the Incident Log task, the script ran an installation verification program (IVP) to verify the setup of z/OS system components. To see the results of the IVP, check the report file named **izuincidentlogverify.report**. For information about using the **izuincidentlogverify.report** file, see"Reviewing the results of the izuincidentlogverify.report file."

If the script ends with errors, see the troubleshooting actions listed in "Problems during configuration" on page 83.

Reviewing the results of the izuincidentlogverify.report file

Check the **izuincidentlogverify.report** file for potential problems in your system configuration. This file resides in the `/etc/zosmf` directory by default. Table 7 summarizes the potential problems and the recommended corrective actions.

Table 7. 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 "Ensuring that CEA is active" on page 165.
System REXX address space is not running.	Start the System REXX address space; see "Ensuring that System REXX is active" on page 166.
User is not authorized.	Authorize the user to the indicated security class *profile-class*; see "User is not authorized" on page 88
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 89.
Unable to open the sysplex dump directory.	Check the sysplex dump directory setup; see "Unable to open the sysplex dump directory" on page 89.
SYS1.MIGLIB is not APF-authorized.	APF-authorize the SYS1.MIGLIB data set; see "Authorizing the SYS1.MIGLIB data set" on page 167.
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 90.
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 active" on page 166.
User is not SAF authorized.	Grant the user the system authority to view the log files; see "User is not SAF authorized" on page 90.
System logger is not available.	Check the system logger setup; see "System logger not available" on page 91.

Table 7. Responding to system setup errors indicated in the izuincidentlogverify.report file (continued)

Problem indicated by the IVP	Corrective action
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 162.
System REXX environment cannot process the request.	Ensure that runtime support for compiled REXX is set up properly; see "System REXX cannot process cannot process the request" on page 91.
Unable to allocate the prepared data set to be tersed.	The function that prepares an incident's materials to be sent through FTP was not able to allocate the data set to be tersed; see "Unable to allocate the prepared data set to be tersed" on page 91.
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 91.
Sysplex dump directory has no space allocated.	Allow more space for incidents; see "Sysplex dump directory has no space allocated" on page 92.
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.
No diagnostic data available.	Specify a larger time interval for error log snapshots; see "No diagnostic data available" on page 92.
Internal error encountered. CEA return code: *return-code* CEA reason code: *reason-code*	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 92.

"Summary of system changes for z/OSMF" on page 155 contains sections on how to perform each of these z/OS setup tasks manually.

Registering the CIM providers

The script might fail because the z/OSMF CIM providers are not installed. If so, you must register the z/OSMF CIM providers. To do so, run the following commands from your CIM identity (the identity from which CIM was set up and started). In place of the variable `$IZU_WBEM_ROOT`, substitute the name of the CIM root directory in use at your installation.

```
$IZU_WBEM_ROOT/bin/cimmof -n root/cimv2 $IZU_WBEM_ROOT/provider/schemas/os_management/IBMzOS_PDW_IVP.mof
$IZU_WBEM_ROOT/bin/cimmof -n root/PG_InterOp $IZU_WBEM_ROOT/provider/schemas/os_management/IBMzOS_PDW_IVP_R.mof
$IZU_WBEM_ROOT/bin/cimmof -n root/cimv2 $IZU_WBEM_ROOT/provider/schemas/os_management/IBMzOS_PDWLogstream.mof
$IZU_WBEM_ROOT/bin/cimmof -n root/PG_InterOp $IZU_WBEM_ROOT/provider/schemas/os_management/IBMzOS_PDWLogstreamR.mof
$IZU_WBEM_ROOT/bin/cimmof -n root/cimv2 $IZU_WBEM_ROOT/provider/schemas/os_management/IBMzOS_SysplexDumpDirectory.mof
$IZU_WBEM_ROOT/bin/cimmof -n root/PG_InterOp $IZU_WBEM_ROOT/provider/schemas/os_management/IBMzOS_SysplexDumpDirectoryR.mof
```

Figure 5. Registering CIM providers for z/OSMF

If you do not perform this action, running the script might result in errors such as the following:

```
IZUG298E: Provider "IBMzOS_PDW_IVP" not registered with CIM
```

GPMSERVE missing authority

If you have Resource Measurement Facility (RMF) installed on your system, you might notice RACF messages regarding GPMSERVE while running this script. The messages, which are written to both the console and SYSLOG, refer to missing authority to `IRRPTAUTH.GPMSERVE.ZOSMFAS CL (PTKTDATA)`.

You can ignore these messages.

Step 6: Access the z/OSMF Welcome task

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

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

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

  START *appserver_proc_name*,JOBNAME=*server_short_name*,
  ENV=*cell_short_name.node_short_name.server_short_name*

  For example:

  ```
  START BBN7ACR,JOBNAME=BBNS001,ENV=BBNBASE.BBNNODE.BBNS001
  ```

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

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

  For example:

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

Leave the instance running for this step. If you need to shut it down, use the STOP command, for example, `P BBN7ACRS`. For more information about starting and stopping IBM WebSphere Application Server OEM Edition for z/OS, see *IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide, Version 7.0*, GA32-0631.

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

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

where:

- *hostname* is the hostname or IP address of the system in which IBM WebSphere Application Server OEM Edition for z/OS is installed
- *port* is the secure application port for the IBM WebSphere Application Server OEM Edition for z/OS configuration. By default, the port is 32208.

To find the hostname and port number, check the IBM WebSphere Application Server OEM Edition for z/OS response file, which is located by default in the directory `/etc/zWebSphereOEM/V7R0/conf/CONFIG1/CONFIG1.responseFile`. In the response file, see the following fields:

- hostName

- zHttpTransportSslPort

If you encounter errors when opening your Web browser to the z/OSMF Welcome task, you might need to modify your workstation setup. z/OSMF includes a tool that you can run to check your browser settings and workstation configuration. For more information, see "Verifying your workstation with the environment checker" on page 72.

Authorizing more users to z/OSMF

z/OSMF includes scripts for creating RACF commands for authorizing existing z/OS user IDs to z/OSMF.

To create a complete set of RACF commands for authorizing a user ID to all of the z/OSMF functions and tasks, use the script **izuaddloguser.sh** and its associated REXX exec. These programs are described in the following topics:

- "Creating commands to authorize a user to all tasks"
- "Authorizing a user to all tasks" on page 42.

If your installation has chosen not to configure the Incident Log task at this time, you can use the script **izuaddcoreuser.sh** and its associated REXX exec to authorize a user ID to only the z/OSMF core functions and the Configuration Assistant task. These programs are described in the following topics:

- "Creating commands to authorize a user to core functions only" on page 43
- "Authorizing a user to the core functions only" on page 44.

The z/OSMF administrator must later complete this authorization on the product level by adding the user and assigning the appropriate role in z/OSMF through the Users task. For information, see "Establishing security for z/OSMF" on page 55.

Creating commands to authorize a user to all tasks

This section describes script **izuaddloguser.sh**, which allows you to create a REXX exec with sample RACF commands for authorizing a user ID to all of the z/OSMF tasks.

About this script

This script creates a REXX exec with RACF commands for authorizing an existing z/OS user ID to all of the z/OSMF functions and tasks: Core functions, Configuration Assistant task, and the Incident Log task.

If you run this script, you do not need to run the script **izuaddcoreuser.sh**.

Running this script

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

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

Location
By default, the script resides in the following directory:

```
/usr/lpp/zosmf/V1R11/bin
```

Invocation

Run the script as follows:

```
izuaddloguser.sh [-file /etc/zosmf/izuconfig1.cfg] -userid USERID
```

izuconfig1.cfg is the configuration file that you created earlier in "Step 1: Create the initial configuration" on page 27. If you omit this value, the script will prompt you for the following input:

- z/OSMF administrator user ID
- z/OSMF root code directory path
- Mount point (the full pathname) for the z/OSMF data file system
- Mount point (the full pathname) for the z/OSMF configuration file system
- CEA group name
- WebSphere application server servant region user ID
- WebSphere SAF profile prefix
- CIM group name, if you allowed the z/OSMF configuration process to configure the CIM server
- CIM administrator user ID, if you specified that the z/OSMF configuration process is to use your existing CIM server.

You gathered these values earlier in "Planning worksheets for z/OSMF" on page 16.

USERID is the existing user ID for which the RACF commands are to be created.

Note: You might need your security administrator to run this script.

As the script runs, it writes log information to the following file:

```
/tmp/izuaddloguser_<mmddyy>_<hhmmss>.log
```

Results

On completion, this script creates sample RACF commands in the file **izuaddloguser_*USERID*.rexx**, which is stored by default in the following location:

```
/etc/zosmf/izuaddloguser_USERID.rexx
```

Figure 6 on page 42 shows an example of the REXX file created for a sample user ID called ZMAUSR1.

```
/* Connect user to CIM and CEA group */
Call RacfCmd "CONNECT ZMAUSR1 GROUP(CIMGP)"
Call RacfCmd "CONNECT ZMAUSR1 GROUP(CEAGP)"

/* Assumption SURROGAT class is defined and raclisted. */
Call RacfCmd "RDEFINE SURROGAT BPX.SRV.ZMAUSR1 UACC(NONE)"
Call RacfCmd "PERMIT BPX.SRV.ZMAUSR1 CL(SURROGAT) ID(ZOSMFAD) ACCESS(READ)"
/* If SURROGAT was previously RACLISTed use the one below. If not comment the one below and */
/* uncomment the one after */
Call RacfCmd "SETROPTS RACLIST(SURROGAT) REFRESH"
/* Call RacfCmd "SETROPTS RACLIST(SURROGAT)" */

/* Setup z/OSMF user identity to core */
/* Assumption APPL class has been defined, activated, and raclisted as part of WAS OEM setup. */
Call RacfCmd "PERMIT BBNBASE CLASS(APPL) ID(ZMAUSR1) ACCESS(READ)"
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"

/* Assumption EJBROLE is defined, activated, and raclisted. */
Call RacfCmd "PERMIT BBNBASE.izuUsers CLASS(EJBROLE) ID(ZMAUSR1) ACCESS(READ)"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"

/* SyncToOSThread permits */
/* Assume SURROGAT class was defined and raclisted. */
Call RacfCmd "RDEFINE SURROGAT BBO.SYNC.ZMAUSR1 UACC(NONE) "
Call RacfCmd "PERMIT BBO.SYNC.ZMAUSR1 CLASS(SURROGAT) ID(WSSRU1) ACCESS(READ)"
Call RacfCmd "SETROPTS RACLIST(SURROGAT) REFRESH"
```

Figure 6. Sample RACF commands for authorizing a user to all z/OSMF tasks

Authorizing a user to all tasks

This section describes the REXX exec **izuaddloguser_*USERID*.rexx**. In short, this exec contains sample RACF commands for authorizing a user ID to all z/OSMF tasks.

About this exec

This REXX exec contains sample RACF commands that your installation's security administrator can use to authorize an existing z/OS user ID to all of the z/OSMF functions and tasks: Core functions, Configuration Assistant task, and the Incident Log task. For your reference, Figure 6 shows an example of the content in this exec.

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

Running this exec

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

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

Environment
Run the exec from an OMVS session.

Location
By default, the exec resides in the following directory:

```
/etc/zosmf/
```

Invocation
From on OMVS session, do the following:

1. Make `/etc/zosmf/` your active directory. For example:

   ```
   cd /etc/zosmf
   ```

2. Run the exec, as follows:

```
./izuaddloguser_USERID.rexx
```

Results

On completion, this exec creates the security definitions for the user ID on the z/OS system. The z/OSMF administrator must later complete this authorization on the product level by adding the user and assigning the appropriate role in z/OSMF. For information, see "Establishing security for z/OSMF" on page 55.

Creating commands to authorize a user to core functions only

This section describes script **izuaddcoreuser.sh**, which allows you to create a REXX exec with sample RACF commands for authorizing a user ID to the z/OSMF core functions and the Configuration Assistant task.

About this script

This script creates a REXX exec with RACF commands for authorizing an existing z/OS user ID to the z/OSMF core functions and the Configuration Assistant task.

Use this script if your installation has chosen not to configure the Incident Log task.

Running this script

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

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

Location
By default, the script resides in the following directory:

```
/usr/lpp/zosmf/V1R11/bin
```

Invocation
Run the script as follows:

```
izuaddcoreuser.sh [-file /etc/zosmf/izuconfig1.cfg] -userid USERID
```

izuconfig1.cfg is the configuration file that you created earlier in "Step 1: Create the initial configuration" on page 27. If you omit this value, the script will prompt you for the following input:

- z/OSMF root code directory path
- Mount point (the full pathname) for the z/OSMF data file system
- Mount point (the full pathname) for the z/OSMF configuration file system
- WebSphere application server servant region user ID
- WebSphere SAF profile prefix.

You gathered these values earlier in Table 4 on page 16.

USERID is the existing user ID for which the RACF commands are to be created.

Note: You might need your security administrator to run this script.

As the script runs, it writes log information to the following file:

```
/tmp/izuaddcoreuser_<date>_<time>.log
```

Results

On completion, this script creates sample RACF commands in the file **izuaddcoreuser_*USERID*.rexx**, which is stored by default in the following location:

`/etc/zosmf/izuaddcoreuser_USERID.rexx`

Authorizing a user to the core functions only

This section describes the REXX exec **izuaddcoreuser_*USERID*.rexx**. In short, this exec contains sample RACF commands for authorizing a user ID to the z/OSMF core functions and the Configuration Assistant task.

About this exec

This REXX exec contains sample RACF commands that your installation's security administrator can use to authorize an existing z/OS user ID to the z/OSMF core functions and the Configuration Assistant task. Use this exec if your installation has chosen not to configure the Incident Log task.

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

Running this exec

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

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

Environment
Run the exec from an OMVS session.

Location
By default, the exec resides in the following directory:

`/etc/zosmf/`

Invocation
From on OMVS session, do the following:

1. Make `/etc/zosmf/` your active directory. For example:

   ```
   cd /etc/zosmf
   ```

2. Run the exec, as follows:

   ```
   ./izuaddcoreuser_USERID.rexx
   ```

Results

On completion, this exec creates the security definitions for the user ID on the z/OS system.

The z/OSMF administrator must later complete this authorization on the product level by adding the user and assigning the appropriate role in z/OSMF. For information, see "Establishing security for z/OSMF" on page 55.

Using the verify function as needed

After you have configured a working instance of z/OSMF on your system, you can optionally run the **izusetup.sh** script again whenever you want to verify your configuration.

To do so, run the **izusetup.sh** script with the -verify option, as described in "Step 3: Verify the RACF security setup" on page 33. To select the scope of the verification, include one of the options shown in Table 8 with the -verify option.

Table 8. Script options for verification

Script option	Scope of verification
`all`	Verify the RACF security setup and the z/OS system customization for all configured tasks and functions.
`core`	Verify the core functions only.
`log`	Verify the z/OS system customization for the Incident Log task only.
`racf`	Verify the RACF security setup for all configured tasks and functions.

For example:

```
izusetup.sh -file /etc/zosmf/izuconfig1.cfg -verify all
```

where *izuconfig1*.cfg is the configuration file that you created previously in "Step 1: Create the initial configuration" on page 27.

As a result, the script checks that all necessary configuration steps were carried out, and creates a report indicating any areas that might require further action on your part. The report resides in the `/etc/zosmf` directory by default.

If you run the script with the options `all` or `log`, the script runs an installation verification program (IVP) that verifies the setup of z/OS system components. To see the results of the IVP, check the report file named **izuincidentlogverify.report**. For information about using the report file, see "Reviewing the results of the izuincidentlogverify.report file" on page 37.

For more information about the format and options for the **izusetup.sh** script, see Appendix C, "izusetup.sh script," on page 171.

Additional steps for setting up your z/OS system

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

By default, the z/OSMF file systems use the following names:

- **Product file system:** IZU.SIZUHFS is the default file system name for an HFS file system and IZU.SIZUZFS is the default file system name for a zFS file system. This file system is mounted in READ mode at the following location: `/usr/lpp/zosmf/V1R11`.
- **Data file system:** The default name is IZU.SIZUDATA. This file system is mounted in READ/WRITE mode at the following location by default: `/var/zosmf/data`.

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 9 provides sample MOUNT commands.

Table 9. 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') MOUNTPOINT('/usr/lpp/zosmf/V1R11) TYPE(ZFS) MODE(READ)
Data file system	MOUNT FILESYSTEM('IZU.SIZUDATA') TYPE(ZFS) MODE(RDWR) MOUNTPOINT('/var/zosmf/data') UNMOUNT

Automove considerations

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

```
BPXM048I BPXOINIT 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.

Customizing your CIM server startup

If you allowed the script to configure the CIM server for you (that is, you replied N to the script prompt "Has the Common Information Model (CIM) server been set up [Y/N]?"), it is recommended that you now ensure that the CIM server is started automatically at IPL time.

The CIM server can started in either of the following ways:

- As a started task
- From z/OS UNIX.

For information about customizing the CIM server startup, see z/OS Common Information Model User's Guide, SC33-7998.

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 more information about how to configure CEA, see *z/OS Planning for Installation*, which is available online in the IBM z/OS Internet Library.

Using FTP in your network

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

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

Updating z/OS for Configuration Assistant

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

About this task

To use Configuration Assistant in z/OSMF, you must transfer your existing backing store files into the z/OSMF environment.

Procedure

1. Determine the location of your existing backing store files. They might reside on your Windows local drive, a LAN drive, or already on z/OS. Use the **File** → **Properties** menu option from the Windows client to view the location.
2. If the backing store files reside on your Windows local drive or LAN drive, copy them to the z/OS system on which Configuration Assistant is running. Backing store files are binary and can be placed in a data set or in the z/OS UNIX System Services (z/OS UNIX) file system.
3. From Configuration Assistant in z/OSMF, use the **Actions** → **Tools** → **Transfer Backing Store file to z/OSMF** option to perform the transfer.

4. Enter the name and path of your existing backing store file on z/OS. This required value can be a data set or a z/OS UNIX file.
5. Click on **Transfer** to copy the backing store file into z/OSMF.

What to do next

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

Removing the roles for a non-configured task

If your installation has chosen not to configure a task at this time, you should probably remove the task from the z/OSMF navigation area for any roles defined to use it. This action can save users some confusion by removing an inactive link to the task from the z/OSMF navigation area.

Example: To remove the role definitions for the Incident Log task:

1. Log into z/OSMF as the Administrator.
2. In the navigation area, expand the z/OSMF Administration category by clicking on the plus sign (+) to the left of the category.
3. Select the *Roles* task to display the Roles panel.
4. For each role definition, do the following:
   a. Select the role and display its properties.
   b. If Problem Determination is selected for the role, click on the plus sign (+) to the left of this category.
   c. Clear the selection for Incident Log.

If your installation configures the Incident Log task later, you can restore the Incident Log task to the navigation area.

For more information about working with roles, see “Roles in z/OSMF” on page 56.

Chapter 4. Using z/OSMF

This section includes topics designed to help you get started using z/OSMF. Such topics include, for example, navigating, using tables, and accessing the online help.

The user interface of z/OSMF consists primarily of tables and property sheets. You can tailor the values shown with functions such as filtering and sorting, refresh the data displayed with the latest z/OS information, and set preferences to customize your user experience.

Working with the z/OSMF interface

z/OSMF provides a Web-based graphical user interface (GUI) that helps you to complete system management tasks. The user interface consists primarily of tables and property sheets. You can tailor the values shown with functions such as filtering and sorting, refreshing the data displayed with the latest information, and setting preferences to customize your user experience. This section covers topics designed to help you get started using z/OSMF. Such topics include, for example, logging in and navigating in the z/OSMF interface.

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

Understanding the z/OSMF interface layout

To make it easier for you to perform system management tasks, z/OSMF provides a modern, graphical user interface. This section describes the layout of the interface and describes the layout of the tables and wizards displayed within the interface.

z/OSMF interface layout

z/OSMF provides a visual framework surrounding a work area where various panels are displayed. This framework serves to provide the basis for a common look-and-feel and serves as the launch point for the tasks that users need to perform.

Table 10. z/OSMF interface layout

<table>
<tr><td colspan="2">Banner Area. The title for z/OSMF, a welcome message, a Log out link (if you are logged in), and the IBM logo are displayed in the banner area. The banner area is not resizable.</td></tr>
<tr><td rowspan="2">Navigation Area. This area is divided into two sections separated by a horizontal line: log in section and task section.

The log in section (top section) is displayed only when you are not logged into z/OSMF. It contains the User ID and Password or pass phrase fields that you can use to log in.

The task section (bottom section) is always displayed. This area contains the tasks that you are authorized to access in z/OSMF. Most tasks are grouped by category. To display the tasks for a particular category, expand the category.

To change the size of the navigation area, click and drag the divider left (to decrease the size) or right (to increase the size).</td><td>Taskbar. The tab for each active task is shown in the taskbar. To close a tab, click the X that is displayed next to the tab title.</td></tr>
<tr><td>Work Area. The content (including tables, wizards, and property sheets) that you can browse or take an action against is displayed in the work area. When clicked, the Help link (located in the top right corner of the work area) opens a new browser window and displays help information about the panel.</td></tr>
</table>

Considerations for using Configuration Assistant

Configuration Assistant contains a navigation tree as part of its user interface. For optimum viewing, you can increase the size of the Configuration Assistant work area and its navigation tree with respect to the surrounding z/OSMF interface. To do so, reduce the size of the z/OSMF navigation area by dragging it to the left, which helps to avoid horizontal scrolling.

Also, to reduce the scrolling of tables and Web pages in Configuration Assistant, increase your Windows screen resolution above the z/OSMF minimum of 1024 by 768 pixels. For Configuration Assistant, the recommended screen resolution is 1280 by 1024 pixels.

To change the screen resolution, do the following:

1. Right-click on the desktop and select **Properties** → **Settings** tab.
2. Move the slider to select a screen resolution of at least 1280 by 1024 pixels.
3. Click **OK**.

Note: In the Japanese language version of z/OSMF, the term *Configuration Assistant* is not translated.

Logging into z/OSMF

To log into z/OSMF, enter a valid z/OS user ID and password (or pass phrase) in the **log in** section of the navigation area. Logging in requires that your user ID has sufficient authorization on both the z/OS system to be managed (through RACF, for example) and in the z/OSMF product.

About this task

z/OSMF uses the concept of *Roles* to group similar users for managing user access to tasks. Role definitions can be modified at any time by the z/OSMF administrator through the z/OSMF interface. Though any z/OS user with sufficient RACF authorization can log into z/OSMF, a user must be assigned a role of Administrator or User to start working with z/OSMF tasks. For more information, see "Defining z/OSMF users and roles" on page 54.

You can launch multiple instances of z/OSMF using different computers, different browsers, or multiple instances of the same browser. If you use multiple instances of the same browser (new window or tab) and your browser is configured to use the same browser session for each instance, when you log into or log out of one z/OSMF instance, you are automatically logged into or logged out of each instance. If you launched multiple z/OSMF instances using different computers or different browsers or using multiple instances of a browser that is not configured to use the same browser session, you must log into and log out of each z/OSMF instance.

Procedure

1. In the User ID field in the navigation area, enter your z/OS user ID that is specified in the z/OS security management facility (for example, RACF) associated with the z/OSMF host system.
2. In the Password or pass phrase field in the navigation area, enter the password or pass phrase associated with the z/OS user ID.
3. Click the **Log in** button.

Results

If the user ID and password or pass phrase are valid, you are authenticated to z/OSMF. The Welcome guest in the header is changed to Welcome <*your_user_ID*> and the navigation area is updated and lists the tasks you are authorized to access.

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

Re-authenticating in z/OSMF

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

About this task

Your z/OSMF session will expire after a period of time has elapsed. By default, this period is eight hours (480 minutes) from the time you log into z/OSMF. Your installation can choose to modify this setting during the configuration of z/OSMF; see "Step 5: Complete the setup" on page 35.

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; all 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 panels 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 re-logged in. If you click **Log out**, all existing tasks are closed and the *Welcome* task is launched. 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.

Navigating in z/OSMF

There are a number of features (such as links in the navigation area, breadcrumbs, and tabs) that you can use to navigate within z/OSMF.

Note: This section describes elements of the user interface for the Incident Log task. Some descriptions do not apply to Configuration Assistant.

Do not use the Web browser navigation buttons, including Back, Forward, Reload and Stop. Doing so might result in unexpected behavior such as losing your place within the interface or losing selections or changes you made.

Table 11. Navigation features in z/OSMF

Feature	Description
Navigation area	The navigation area provides launch points to various tasks that you can access using z/OSMF. When you click them, tasks that are not links are launched in a tab in the work area. Links that appear under the Links category, however, are always launched in a new browser window. If the selected task is currently open in a tab in the work area, the tab is brought into focus (a new instance is not created). Otherwise, unless the task is a link, the task is launched as a new tab into the work area.
Tabs	z/OSMF tabs are arranged horizontally across the work area in the order in which you launched the tasks. The active tab (tab that has focus) is displayed and has a background color that is different from the background color of the inactive tabs. You can easily navigate between tasks by clicking an inactive tab to bring it into focus. Any changes or selections you make are not lost when switching between tabs.
Links in tables	In most tables in z/OSMF, the first column contains a link. When you click the link, it displays one of the following items: • Items that are subordinate to the selected item. • Properties for the selected item.
Action menus in tables	Actions listed in the *Actions* menu or context menus that have a trailing ellipsis (...) do not run immediately. When you select one of those actions, another panel or dialog box is displayed prompting you to provide additional information or to confirm the action. If a new panel is displayed, it replaces the panel that launched it. You can use breadcrumbs to navigate between the new panel and the launching panel. If a dialog box is launched from a panel, it is displayed on top of that panel. Although, you can see the launching panel, you cannot interact with it until you close the dialog box.
Breadcrumbs (also known as navigation trails)	When you navigate several levels into a hierarchy, you can use breadcrumbs (displayed in the work area above the panel title) to return to any panel you previously visited within that hierarchy. For example, if you launch the Incident Log task and display the diagnostic details for an incident, the following breadcrumbs are displayed: `Incident Log > View Diagnostic Details` Each breadcrumb, except the last, is a link that you can click to return to the associated panel. In this example, you can return to the *Incident Log* panel. When you click the breadcrumb link, if there are any unsaved changes, a message is displayed indicating that those changes will be discarded if you choose to continue.

z/OSMF administration

z/OSMF provides a Web browser interface for performing product administration tasks, such as defining z/OSMF roles and users. z/OSMF also allows your installation to define links for other external Web applications that users can launch. This allows you to have a single launch point for all of your z/OS management Web applications.

Selecting an administration task

To display the z/OSMF administration tasks, expand the z/OSMF Administration category in the navigation area. To perform an administration task, select the appropriate task from the following list:

- **z/OSMF Links.** Select this task to manage your links.
- **z/OSMF Roles.** Select this task to view and modify z/OSMF roles.
- **z/OSMF Users.** Select this task to define new z/OSMF users and to modify or delete existing z/OSMF users.

Defining z/OSMF users and roles

To perform work in z/OSMF, a user requires sufficient authority on both the z/OS system to be managed and in the z/OSMF product. With the necessary permissions established in both areas, users can begin using z/OSMF to perform system management tasks on z/OS.

The process of authorizing a user for z/OSMF work begins with the z/OS system. Because z/OS resources are accessed on behalf of z/OSMF users, access to these resources must be defined through the security management product in use at your installation. Usually, this work is performed by your installation's security administrator, who ensures that all users are defined in accordance with the security policies in use at your installation.

z/OSMF includes scripts for authorizing user IDs to the required resources on your z/OS system (through RACF commands). Your installation's security administrator can refer to these RACF commands as examples for creating the required security product settings for a new user. The scripts are further described in "Assistance for security administrators" on page 56.

In the z/OSMF product, authorizing a user means defining the user to z/OSMF and associating the user with a z/OSMF role, based on the type of work the user is expected to perform.

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

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

z/OSMF also includes options for managing the access of guest users, that is, users who enter z/OSMF without an explicitly assigned role, or users who do not log in. Depending on how a guest user enters z/OSMF, a guest user is considered either authenticated or non-authenticated.

Though your installation can modify these roles, it is recommended that you use the roles as provided, and reserve the administration tasks for users assigned to the z/OSMF Administrator role.

More information:

- For more information about security in z/OSMF, see "Establishing security for z/OSMF"
- For information about defining roles, see "Roles in z/OSMF" on page 56.
- For information about defining users and guest users, see "Defining users in z/OSMF" on page 57.

Establishing security for z/OSMF

Establishing a secure environment for z/OSMF begins with your installation's security administrator. This person is responsible for ensuring that the security policies for users and resources on the z/OS system are followed with z/OSMF. Your installation's security administrator must grant the proper security product access to users before they can use z/OSMF to work with the z/OS system.

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

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

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

When defining roles and users to z/OSMF through the z/OSMF administration tasks, the z/OSMF administrator must ensure that a user's authority on z/OSMF is sufficient within the user's existing authority on the z/OS host system. If not, the user's authorization on the z/OS system takes precedence over the user's authorization in z/OSMF.

On a system with RACF, for example, the RACF database contains profiles for all of the users, groups, data sets, and other resources that have been defined to RACF. When a z/OSMF user attempts to access a protected resource, RACF verifies the user's identity (by checking the user profile in the RACF database) and performs authorization checking to ensure that the user may access the requested resource.

If a z/OSMF user attempts to access a resource without sufficient authority on the z/OS host system, the user's request is rejected with an error message (insufficient authorization).

Assistance for security administrators

z/OSMF includes scripts for authorizing user IDs to the required resources on your z/OS system (through RACF commands). Your installation's security administrator can refer to these RACF commands as examples for creating the required security product settings for a new user.

To create the required security authorizations, use the appropriate configuration script that is supplied with z/OSMF. The script creates a REXX exec with RACF commands for the core functions, such as creating the z/OSMF administrator identity. IBM recommends that you work with your installation's security administrator to review the RACF commands, modify them as necessary, and run the script to issue them.

The z/OSMF configuration scripts are described in Chapter 3, "Configuring z/OSMF," on page 25.

Roles in z/OSMF

In z/OSMF, a *role* represents the ability to perform one or more tasks. These tasks include both general administrative actions for z/OSMF and task-specific actions for the z/OS system to be managed. Your installation can modify the tasks for a role through the *Roles* task.

The process of defining a role in z/OSMF involves the separate actions of selecting tasks for the role (through the Roles task) and assigning users to the role (through the Users task).

z/OSMF filters the list of tasks shown in the navigation area to match the authorization of the assigned role for the current user. If a role is not authorized to work with certain tasks, those tasks are not displayed in the navigation area for users assigned to the role.

To work with roles for z/OSMF, your user ID must be assigned to a z/OSMF role that is permitted to the Roles task. By default, only the z/OSMF Administrator role can work with roles.

When defining roles in z/OSMF through the z/OSMF administration tasks, the z/OSMF administrator must ensure that a user's authority in z/OSMF is sufficient within the user's authority on the z/OS host system. If not, the user's authorization on the z/OS system takes precedence over the user's authorization in z/OSMF.

Understand that z/OSMF does not prevent you from modifying the role or the user definition with which you are currently logged on to z/OSMF. If you remove the Roles task from the role definition to which your user id is assigned, for example, you lose the authority to continue working with the Roles task. Here, z/OSMF performs the change and issues messages to:

- Confirm the modification of the role definition
- Indicate that you are not authorized to use the Roles task.

To work with roles in z/OSMF, expand the z/OSMF Administration category in the navigation area and select Roles. Doing so will begin a sequence of steps for defining which tasks are assigned to a z/OSMF role. For assistance with this task, see the online help for the *Roles* task.

Managing guest users

z/OSMF includes options for managing the access of *guest users*, that is, users who enter z/OSMF without an explicit role assignment. 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 whose user ID is not assigned to a z/OSMF role.
- **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 an explicit role assignment. It is not possible to designate a user as a non-authenticated or authenticated guest user, for example, through the *Users* task.

Your installation can manage the access of guest users to z/OSMF tasks through the *Roles* task by modifying the roles z/OSMF Guest and z/OSMF Authenticated Guest.

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

Defining users in z/OSMF

To perform work in z/OSMF, a user must be defined to z/OSMF. With the appropriate authorization established in both z/OSMF and on the z/OS system to be managed, a z/OSMF user can select one or more tasks from the navigation area and advance through a guided sequence of panels for performing each task.

On the *Users* panel, you define a user by specifying the user ID and user name. You also select a role for the user: z/OSMF User or z/OSMF Administrator. By specifying a role for the user, you authorize this person to perform the tasks that are associated with that role.

To define users for z/OSMF, your user ID must be assigned to a z/OSMF role that is permitted to the Users task. By default, only the z/OSMF Administrator role can define users.

For any new users to be added, verify that your installation's security management product (for example, RACF) will permit the user to access the system resources needed to perform a particular task. If necessary, contact your installation's security administrator to authorize the user.

For help with establishing the required security setup for the user, your installation's security administrator can refer to the configuration scripts that are provided with z/OSMF. The scripts contain sample RACF commands for authorizing users and groups to system resources. For information about the z/OSMF configuration process, see Chapter 3, "Configuring z/OSMF," on page 25.

The z/OSMF configuration process creates an initial administrator user ID. With this user ID, the administrator can log into z/OSMF and add more users and administrators as needed, through the *Users* panel.

To work with user definitions in z/OSMF, click on the z/OSMF Administration category in the navigation area and select Users. Doing so will begin a sequence a steps for defining one or more users to z/OSMF.

For more assistance with this task, see the online help for the *Users* panel.

Defining links for z/OSMF

Your installation can customize z/OSMF with links to external sites for system management tools and information.

The process of defining a link to z/OSMF includes specifying the link and its location (a URL) and selecting which z/OSMF roles can access the link. Depending on the user's Web browser settings, the link opens as either a new browser window or a new browser tab.

To define links for z/OSMF, your user ID must be assigned to a z/OSMF role that is permitted to define links. By default, only the z/OSMF Administrator role can define links.

To display the *Links* panel, expand the z/OSMF Administration category in the navigation area and select *Links* to begin a sequence of steps for defining links for z/OSMF.

For more assistance with this task, see the online help for the *Links* task.

Note: Some useful links were provided with the installation of z/OSMF. In the Japanese language version of z/OSMF, these links are not translated.

System management with z/OSMF

z/OSMF V1R11 provides the following system management tasks:
- Configuration Assistant (for z/OS V1R11 systems and later)
- Incident Log
- Links.

Configuration Assistant task overview

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

To use the Configuration Assistant task in z/OSMF, your system must be running z/OS V1R11 or later.

Figure 7 on page 59 shows the main page for the Configuration Assistant task.

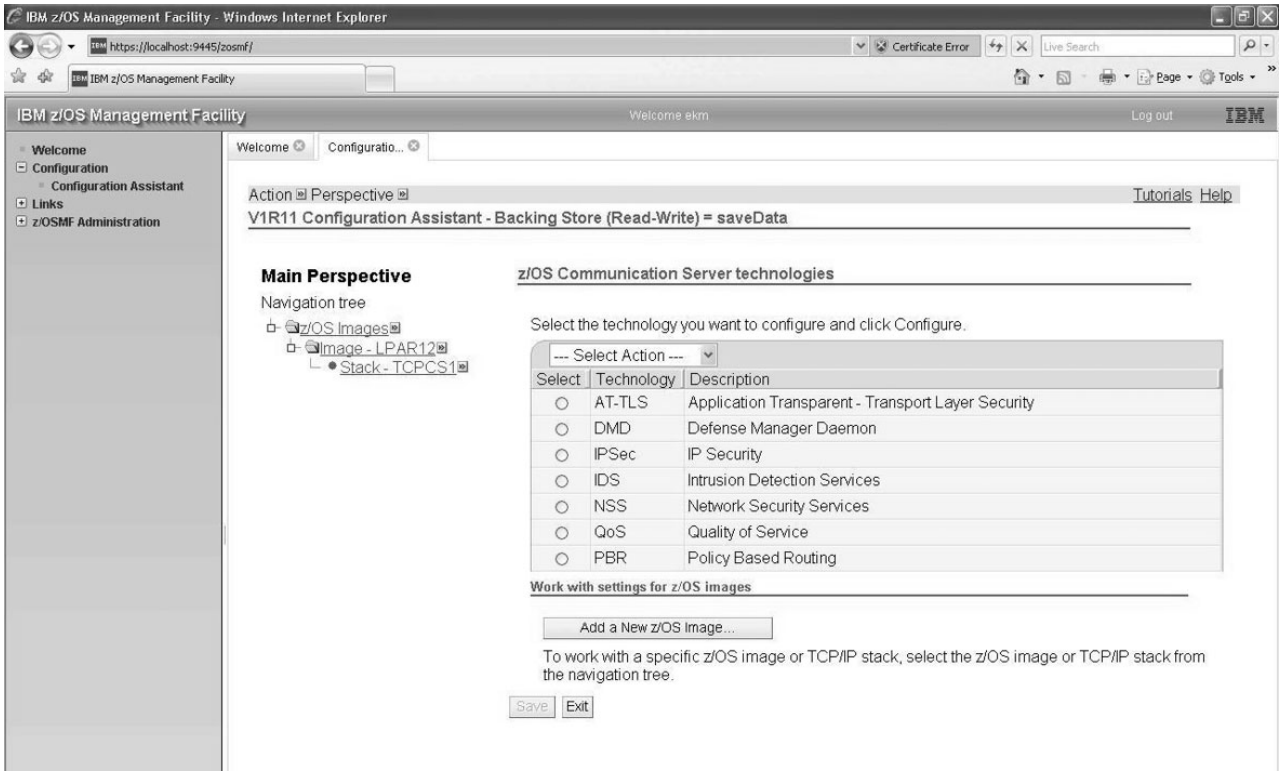


Figure 7. Configuration Assistant task main page

Through the Configuration Assistant task, you can:

- Configure new policies for the following TCP/IP, policy-based networking disciplines:
  - IP Security, including IKE
  - Network Security Services (NSS)
  - Defense Manager daemon (DMD)
  - Application Transparent TLS (AT-TLS)
  - Intrusion Detection Services (IDS)
  - Policy-based Routing (PBR)
  - Quality of Service (QoS).
- Import previously defined policies for IP Security, AT-TLS, IDS, and PBR.
- Review Application Setup Tasks containing detailed instructions for getting a supported policy discipline up and running.

For information about getting started, see the Welcome page within the Configuration Assistant task. Here you can find extensive help, which you can reference at any time.

On the Web, you can find information about the Configuration Assistant at the z/OS Communications Server Web site: http://www.ibm.com/software/network/commserver/zos/support/.

Note: In the Japanese language version of z/OSMF, the term *Configuration Assistant* is not translated.

Incident Log task overview

The Incident Log task in z/OSMF simplifies the management of supervisor call (SVC) dumps that have occurred on a system or in a sysplex. The Incident Log task offers a browser-based user interface for viewing and managing system detected and user-initiated incidents and their associated diagnostic data. Using this interface reduces the possibility of errors while obtaining, aggregating and sending the collection of diagnostic data to IBM or an independent software vendor (ISV). The Incident Log task is available for systems running z/OS V1R10 or later.

An incident is an occurrence that is not part of the standard operation of a service and can cause a disruption to, or a reduction in, the quality of service and productivity. Incidents are identified by the occurrence of an SVC dump. SVC dumps that an authorized program or an operator initiates (using DUMP or SLIP commands) are related to *User Initiated* incidents. SVC dumps initiated by the system on behalf of abend recovery result in *ABEND* incidents.

When an incident occurs, the system creates diagnostic log snapshots of the operations log, error and error log summary (that is, logrec detail and logrec summary), based on the settings specified in your installation's CEAPRMxx parmlib member.

Some of the key functions available in the Incident Log task in z/OSMF V1R11 follow.

- **Display list of incidents.** The Incident Log task provides a consolidated list of problems along with the details and the diagnostic data captured and saved with each problem. By default, only incidents that have occurred in the past three days are displayed. A maximum of 500 incidents are displayed in the log.
- **Set properties.** The Incident Log task provides the ability to correlate an incident with a problem number or tracking ID. The problem number allows you to associate an incident with an IBM problem number (such as a PMR or an ETR number) or an ISV problem number. With the tracking ID, you can associate an incident with a problem record in your installation's problem management system.
- **Display properties.** The Incident Log task allows you to view additional information about an incident, such as the symptom string, reason code, or list of collected diagnostic data.

  An incident can represent a multi-system SVC dump, which consists of a primary dump and multiple secondary dumps taken on other systems in the sysplex. If so, the Incident Log task shows all of the SVC dumps associated with the incident, with a single set of diagnostic snapshot files.
- **Send diagnostic data.** The Incident Log task provides a *Send Diagnostic Data* wizard that you can use to send diagnostic data to IBM or another FTP destination. Here, z/OSMF gathers the diagnostic data, compresses it, and uses FTP to send it to an FTP destination. The FTP destination can be any destination you choose including the IBM Support Center or an ISV.
- **Manage FTP job status.** The Incident Log task allows you to view or delete the status of an FTP job or to cancel an FTP job.
- **Allow next dump.** 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 that is being suppressed by DAE (with the same MVS symptom string).

- **Delete incident.** The Incident Log task allows you to simultaneously delete an incident, all of its FTP job status information, and all associated diagnostic data (such as the operations log, error log, and SVC dumps).
- **Manage FTP destinations and profiles.** To send diagnostic data in z/OSMF, the destination to where the data is being sent and the firewall or proxy the data crosses must be defined. The Incident Log task allows you to define the destinations on the *FTP Destinations* panel and the firewalls or proxies on the *FTP Profiles* panel. The Incident Log task provides substitution variables that you can use when specifying the information required by your firewall or proxy. For a list of the substitution variables, see the *FTP profile substitution variables* help topic provided in the z/OSMF online help. To access the help, click the Help link, which is located in the upper right-hand corner of each panel.

Figure 8 is a view of the Incident Log task summary, which lists all incidents in the sysplex meeting your specified filter criteria. The summary list provides a consolidated view of all incidents occurring on all participating systems in the sysplex (those that communicate through the same sysplex dump directory). You can then drill down to view the details of any given incident.

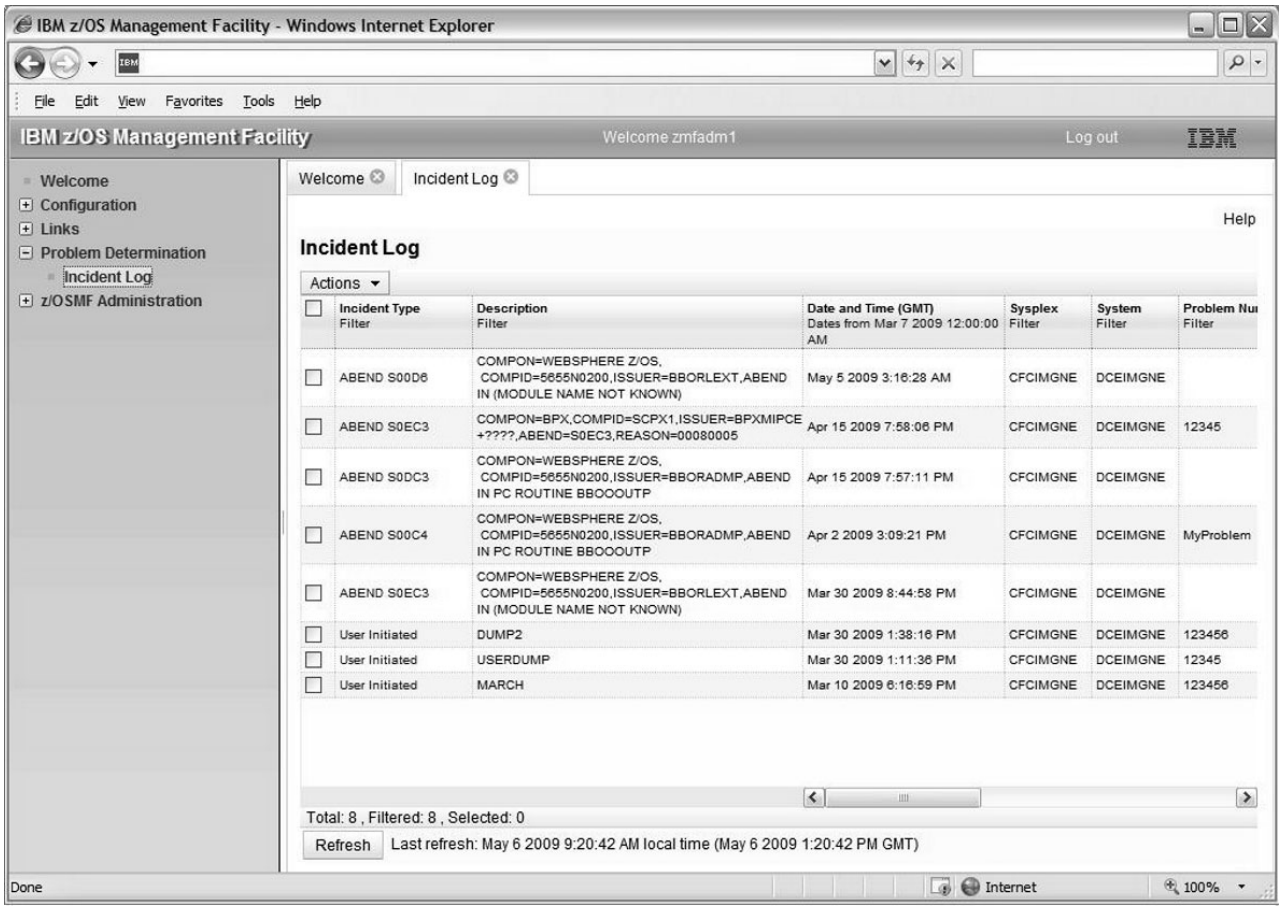


Figure 8. Incident Log task

Chapter 5. Creating another instance of z/OSMF

You can have only one active instance of z/OSMF in a sysplex at any given time. You might choose, however, to create a backup instance of z/OSMF for failover (or takeover) or for testing purposes. This topic provides information about setting up a backup instance of z/OSMF.

Planning for a backup instance of z/OSMF

Before creating a backup instance of z/OSMF, you should have already created primary instances of IBM WebSphere Application Server OEM Edition for z/OS and z/OSMF, as described in the book *IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide, Version 7.0*, GA32-0631, and in Chapter 3, "Configuring z/OSMF," on page 25.

Consider the following:

- If your primary instance of z/OSMF uses a shared data file system (one that is read/write accessible from other systems in the sysplex), you will have fewer steps to follow to configure a backup instance of z/OSMF and to perform a takeover from the primary instance of z/OSMF to the backup. If you use a shared security database, the takeover procedure is further simplified because the backup instance can use the same user IDs and groups as your primary instance.
- If your primary instance of z/OSMF uses a non-shared data file system (one that is only read/write accessible from only the host z/OS system), takeover from the primary instance of z/OSMF to the backup will require that you unmount the data file system on the host z/OS system and mount it on the backup system. z/OSMF includes shell scripts to help you do this work, which are described in this topic.

After a takeover from the host z/OS system, users must log into z/OSMF again on the backup system to resume using z/OSMF.

- If you use a shared z/OSMF data file system, you must stop the instance of IBM WebSphere Application Server OEM Edition for z/OS before you can create the backup instances of IBM WebSphere Application Server OEM Edition for z/OS and z/OSMF.
- If you use a non-shared z/OSMF data file system, you do not need to stop IBM WebSphere Application Server OEM Edition for z/OS before you create the backup instances. In this case, your backup instance of z/OSMF will use a different data file system.

For information about creating multiple instances of IBM WebSphere Application Server OEM Edition for z/OS, see *IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide, Version 7.0*, GA32-0631.

Restrictions on using additional instances of z/OSMF

Observe the following restrictions for using additional instances of z/OSMF in your environment:

- You can have only one instance of z/OSMF per instance of IBM WebSphere Application Server OEM Edition for z/OS.

- Only a single instance of z/OSMF in the sysplex can use the z/OSMF data file system at a given time.

  To prevent the same z/OSMF data file system from being accessed by more than one instance of z/OSMF at a time, z/OSMF locks the data file system through a global resource serialization ENQ with QNAME ZOSMF. If you start a second instance of z/OSMF using the same data file system, that z/OSMF will become active but will not be usable. Any users who attempt to access the second instance of z/OSMF will encounter a z/OSMF error Web page. Further, all log messages from the second instance of z/OSMF are routed to the WebSphere log, rather than to the z/OSMF 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.
- Do not run multiple instances of z/OSMF simultaneously in a sysplex, even if using different z/OSMF data file systems. 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.
- The z/OSMF data file system can be used by only a single instance of z/OSMF in a sysplex at a given time.

Steps for configuring a backup instance of z/OSMF

This procedure assumes that you have an initial instance of IBM WebSphere Application Server OEM Edition for z/OS and z/OSMF in the same sysplex, including the necessary security authorizations for z/OSMF users.

Step 1: Create an additional instance of IBM WebSphere Application Server OEM Edition for z/OS.

When creating an additional instance of IBM WebSphere Application Server OEM Edition for z/OS, use the same values (user IDs, groups, and so on) that you used to configure your initial instance of z/OSMF. These values are contained in the IBM WebSphere Application Server OEM Edition for z/OS response file.

For more information, see *IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide, Version 7.0*, GA32-0631,

Step 2: Copy your z/OSMF configuration settings to the backup instance.

When you created your initial instance of z/OSMF — either by installing z/OSMF through the configuration scripts described in Chapter 3, "Configuring z/OSMF," on page 25 or as part of performing a ServerPac full system replacement— you saved a copy of your settings in a configuration file. To save time, you can use a copy of that configuration file to set up a backup instance of z/OSMF. If so, you must verify and update as necessary any values that are different on the new system from your original setup.

By default, the configuration file is stored in the `/etc/zosmf` directory on the system. The configuration file has an installation-specific name, such as **izuconfig1.cfg**, if created through the **izusetup.sh** script or **serverpac.cfg** if supplied with a ServerPac order.

Copy the configuration file and, if used, the override file (`/etc/zosmf/izudflt.ovr`) from your initial z/OSMF instance to the system on which you are configuring the backup instance.

Then, run the following script from a user ID with superuser authority:

```
izusetup.sh -file /etc/zosmf/izuconfig1.cfg -config [–system SYSNAME]
```

SYSNAME is the system on which the backup instance of z/OSMF is to be configured. If you omit this value, the script will prompt you for it.

Specify the configuration file from your initial instance of z/OSMF as a source file (`/etc/zosmf/izuconfig1.cfg`), but when prompted by the "save file" message, specify `/etc/zosmf/izuconfig2.cfg`. This action provides a unique configuration file for the backup system.

The script prompts you for z/OSMF data file system. Note the following:

- If your initial instance of z/OSMF uses a shared z/OSMF data file system, specify the same data file system for your backup instance.
- If your initial instance of z/OSMF does not share its data file system, you must specify a different data file system for your backup instance. During takeover, you will switch the backup system to the data file system used by the initial instance (as described in "Performing a takeover from the primary instance of z/OSMF to a backup" on page 66).

If you installed z/OSMF as part of a ServerPac order, the security was set up through the ServerPac post-installation job, RACFTGT. In this case, not all configuration values are saved in the ServerPac configuration file **serverpac.cfg**.

Step 3: Authorize users for the backup instance of z/OSMF.

This step assumes that your installation uses RACF as its security management system.

Your work for this step depends on whether your installation shares its RACF database between systems, as follows.

- **RACF database is not shared:** When you set up your initial instance of z/OSMF, the configuration process (the **izusetup.sh -config** script or ServerPac) created a REXX exec with RACF commands to be used for securing the z/OSMF functions and tasks. By default, that exec is named **izuconfig1.cfg.rexx**, and is stored in the directory `/etc/zosmf`. To recreate the same security setup on another system, you can run the **izusetup.sh -config** script again, plus the optional scripts for adding additional users to the core functions and, if applicable, the Incident Log task. Or, you can rerun the RACF commands on the backup z/OS system.
- **RACF database is shared:** Setting up another instance of IBM WebSphere Application Server OEM Edition for z/OS might include using a different cell short name and cluster transition name. If so, you must re-run some RACF commands to authorize users to the new instance of IBM WebSphere Application Server OEM Edition for z/OS. To find the cell short name and cluster transition name values for your installation, check the IBM WebSphere Application Server OEM Edition for z/OS response file.

Considerations for running the REXX exec are provided in "Step 2: Run the security commands" on page 31.

Step 4: Prime the data repository for backup instance.

This step primes the data repository with the z/OSMF administrator user ID (ZOSMFAD, by default). Note the following:

- If your initial instance of z/OSMF uses a shared z/OSMF data file system that has already been primed, this step is not necessary.
- If your initial instance of z/OSMF does not share its data file system, you must run the script to prime the repository.

  To use the configuration file from your initial instance of z/OSMF and your existing z/OSMF administrator identity name (assuming that your security database is shared), run the following script from a user ID with superuser authority:

  ```
  izusetup.sh -file /etc/zosmf/izuconfig2.cfg –prime
  ```

  Considerations for running this script are provided in "Step 4: Prime the z/OSMF data file system" on page 34.

Step 5: Complete the configuration.

This step completes the configuration of z/OSMF and deploys it into a backup instance of IBM WebSphere Application Server OEM Edition for z/OS. Run this script from the z/OSMF administrator user ID that you created previously (ZOSMFAD, by default):

```
izusetup.sh -file /etc/zosmf/izuconfig2.cfg –finish
```

If your installation uses the same parmlib members across the sysplex, respond N to the script prompts that ask you whether to override your existing CEAPRMxx and IEADMCxx members.

Considerations for running this script are provided in "Step 5: Complete the setup" on page 35.

Performing a takeover from the primary instance of z/OSMF to a backup

If you have a shared data file system: Follow these steps:

1. Stop the initial instance of IBM WebSphere Application Server OEM Edition for z/OS
2. Start the backup instance of IBM WebSphere Application Server OEM Edition for z/OS.

If you have a non-shared data file system: Follow these steps:

1. Stop your existing instance of IBM WebSphere Application Server OEM Edition for z/OS and the backup instance, if it is active.
2. From a user ID with superuser authority, run the following script to unmount the primary data file system on your system and to mount it on the backup system. In these examples, the term *primary data file system* refers to the data file system that is to be moved.

```
izusetup.sh -file configfilenamebackup -sourcefile configfilenameprimary -move
```

   If another data file system is currently mounted at mount point IZU_DATA_DIR on the backup system, that data file system is unmounted before the primary data file system is mounted. The name and type of the primary data file system are taken from your configuration file

(*configfilenameprimary*) for the primary instance of z/OSMF. The mount point (IZU_DATA_DIR) is taken from the backup configuration file (*configfilenamebackup*). On completion of the script, the backup configuration file (*configfilenamebackup*) is updated with the name and type of the data file system specified in the configuration file (*configfilenameprimary*) for the primary instance of z/OSMF.

For descriptions of the script options, see "Options for moving the z/OSMF data file system."

3. If z/OSMF was deployed on the backup system using another data file system mount point, you must run the following script to set the value for IZU_DATA_DIR to the mount point where the primary data file system has been mounted in Step 2. From the z/OSMF administrator user ID (ZOSMFAD by default) run the script as follows:

```
izusetup.sh -file configfilenamebackup -core
```

4. Start the backup instance of IBM WebSphere Application Server OEM Edition for z/OS.

Because the script **izusetup -move** moves the z/OSMF data file system, the log messages are not written to the logs directory of the data file system. Instead, the script creates log files in the configured directory for temporary files.

Options for moving the z/OSMF data file system

The script **izusetup.sh** offers several options for moving a z/OSMF data file system to another system, as shown in the examples that follow.

- **Example 1: Using the configuration file from your primary system.** To use the data file system name (IZU_DATA_FS_NAME) and type (IZU_DATA_FS_TYPE) from your existing configuration file *configfilenametarget*, invoke the script, as follows:

```
izusetup.sh –file configfilenametarget -move
```

  The mount point (IZU_DATA_DIR) is taken from the *configfilenametarget* file.

  You might use this invocation if your configuration file already contains the correct name and type of the data file system to move, for example, when you move a data file system from a backup system to the primary system and use the configuration file for your primary instance of z/OSMF.

- **Example 2: Using the configuration file from another system.** To use the data file system name (IZU_DATA_FS_NAME) and type (IZU_DATA_FS_TYPE) from another configuration file *configfilenamesource*, invoke the script, as follows:

```
izusetup.sh –file configfilenametarget –sourcefile configfilenamesource -move
```

  The mount point (IZU_DATA_DIR) is taken from the *configfilenametarget* file. When the move of the data file system is completed, the *configfilenametarget* file is updated with the name and type of the data file system from *configfilenamesource*.

You might use this invocation if the configuration file of the target z/OSMF instance does not contain the correct name and type of the data file system to move, for example, if you want to move your existing z/OSMF data file system to a backup system that previously used another data file system.

- **Example 3: Using the configuration file from another system.** This invocation is similar to the previous example, except that the name and type of the data file system are specified explicitly, as shown:

```
izusetup.sh –file configfilenametarget –datafilesystem MVSDS
                  –datafilesystemtype HFS|ZFS -move
```

The mount point (IZU_DATA_DIR) is taken from the *configfilenametarget* file. When the move of the data file system is completed, the *configfilenametarget* file is updated with the specified name and type of the data file system.

You might use this invocation if a configuration file with the correct name and type of the data file system to move is not available.

Setting up a dynamic VIPA for z/OSMF

To help ensure the availability of IBM WebSphere Application Server OEM Edition for z/OS running z/OSMF, you can use the z/OS Communications Server TCP/IP sysplex networking dynamic VIPA (DVIPA) function. This section provides a sample scenario for how you might do so.

To enable IBM WebSphere Application Server OEM Edition for z/OS for DVIPA, you use an application-defined DVIPA. This work involves setting the VIPARANGE statement in the TCP/IP configuration profile. Use of the VIPARANGE requires that the DVIPA be activated by the application; in the case of WebSphere, activation can be done by binding to an IP address within the VIPARANGE.

Assume that your installation has a primary z/OSMF instance and a backup, with both host systems defined on the same VIPARANGE statement. If the primary z/OSMF instance becomes unavailable, you can start the backup instance. With DVIPA activated by IBM WebSphere Application Server OEM Edition for z/OS, your installation can move the WebSphere application to a backup system. This action allows IBM WebSphere Application Server OEM Edition for z/OS to bind again to the same DVIPA address and resume operation, remaining available for workloads throughout the failover.

Sample TCP/IP configuration profiles: In the following samples, the IP addresses are examples; the actual addresses will be specific to your installation.

Figure 9 on page 69 shows the statements for the TCP/IP configuration profile for the primary system on which IBM WebSphere Application Server OEM Edition for z/OS and z/OSMF is used.

```
IPCONFIG
  DYNAMICXCF 9.42.100.1

 VIPADYNAMIC
  VIPARANGE DEFINE MOVEABLE NONDISRUPT 255.255.255.0 10.25.101.1

ENDVIPADYNAMIC

/* End Tcp/Ip profile for Primary z/OSMF system */
```

Figure 9. TCP/IP configuration profile for the primary system

Figure 10 shows the statements for the TCP/IP configuration profile for the system on which the backup z/OSMF is to be started.

```
IPCONFIG
  DYNAMICXCF  9.42.100.2

VIPADYNAMIC
  VIPARANGE DEFINE MOVEABLE NONDISRUPT 255.255.255.0 10.25.101.1
ENDVIPADYNAMIC

/* End of Tcp/Ip profile for Backup z/OSMF system   */
```

Figure 10. TCP/IP configuration profile for the system on which the backup z/OSMF is to be started

For an overview of TCP/IP sysplex networking, see *z/OS Communications Server IP Configuration Guide*. For a description of TCP/IP profile statements, see *z/OS Communication Server IP Configuration Reference*.

Chapter 6. Troubleshooting

This chapter provides troubleshooting tips for common problems. Included are procedures and methods for performing problem determination and for determining the status of the different components.

This chapter is organized into major topics, as follows:
- "Resources for troubleshooting"
- "Tools and techniques for troubleshooting" on page 72
- "Common problems and scenarios" on page 83.

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 12 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 12. 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 72.	N/A
Core functions and the Incident Log task	• The About page • z/OSMF log files and tracing.	• "Accessing the About page" on page 80 • "Working with z/OSMF runtime logs" on page 80.	Chapter 7, "Messages for z/OSMF," on page 107.
Configuration Assistant	Various.	"Problems when using Configuration Assistant" on page 99.	Supplied with the Configuration Assistant task as messages and pop-ups.
IBM WebSphere Application Server OEM Edition for z/OS	• WebSphere FFDC log files (sysout, HFS) • WebSphere tracing.	"Enabling trace and logging for z/OSMF" on page 81.	*IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide, Version 7.0*, GA32-0631.
CIM server and CIM providers	• CIM server logging • CIM server trace • CIM provider trace.	These options are defined in the CIM server configuration properties and set through the cimconfig command; see z/OS Common Information Model User's Guide.	z/OS Common Information Model User's Guide.
Common event adapter (CEA)	System commands: • MODIFY CEA • MODIFY AXR • TRACE CT.	*z/OS MVS System Commands*,which is available online in the IBM z/OS Internet Library.	*z/OS MVS System Messages* for information about: • WTO messages • CTRACE • Reason codes.

For information about resolving problems with IBM WebSphere Application Server OEM Edition for z/OS, see *IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide, Version 7.0*, GA32-0631.

Tools and techniques for troubleshooting

This section describes the tools and techniques available for troubleshooting problems with z/OSMF.

This section is organized into the following major topics:
- "Verifying your workstation with the environment checker"
- "Working with z/OSMF runtime logs" on page 80
- "Enabling trace and logging for z/OSMF" on page 81.

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.

Running the tool

The environment checker tool inspects your Web browser and workstation operating system for compliance with z/OSMF requirements and recommended settings.

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. By default, this is port 32208.
2. Follow the instructions for your particular browser in the online help for the tool.

Figure 11 on page 74 shows an example of the environment checker report for a Firefox browser.

Understanding the results of the tool

Table 13 describes the layout of the environment checker report.

Table 13. Columns in the environment checker tool results panel

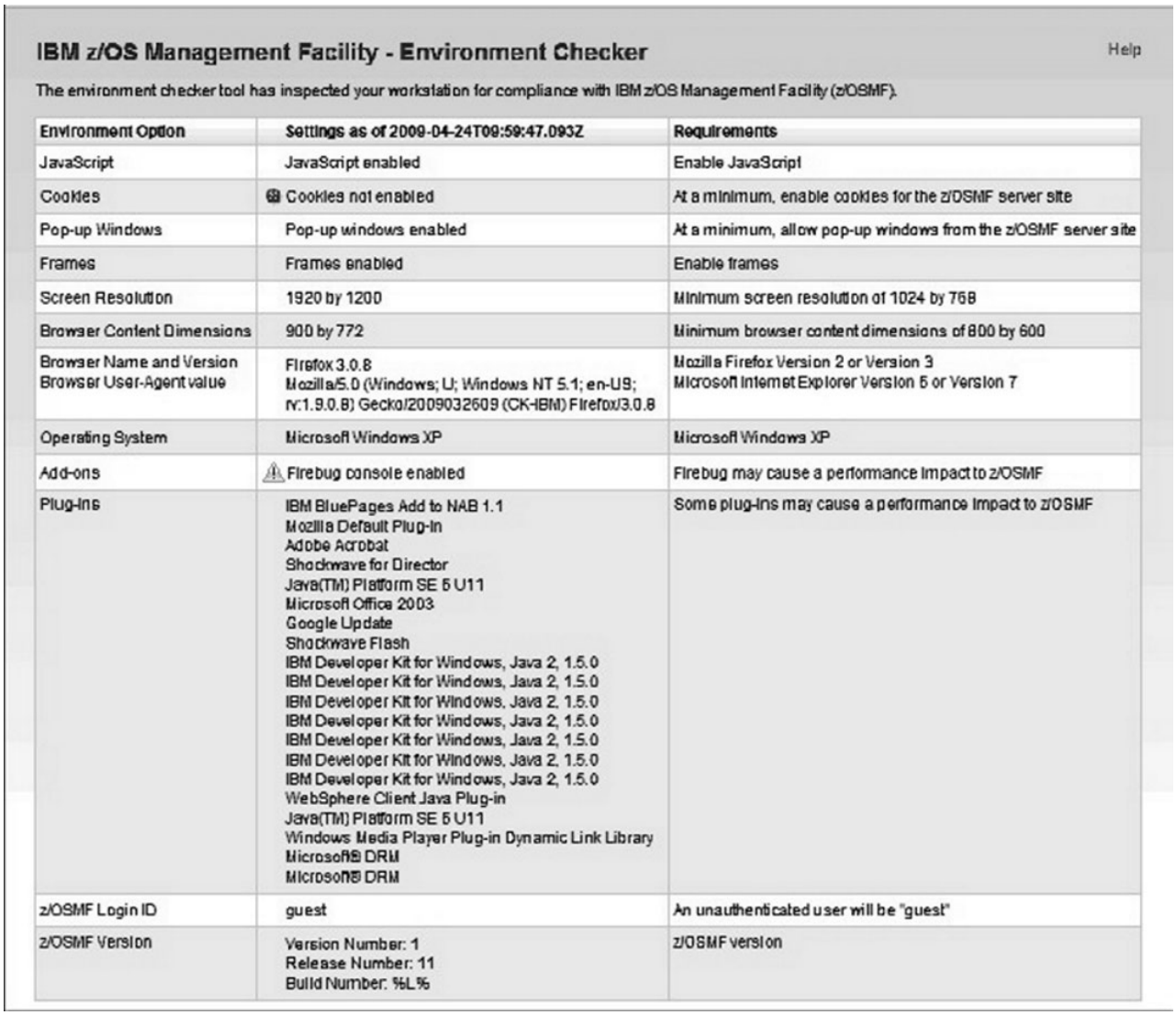
Column	Description
Environment Option	Browser setting that was examined by the environment checker tool.

Table 13. Columns in the environment checker tool results panel (continued)

Column	Description
Settings as of *date-time*	Findings from the most recent invocation of the tool. This column indicates potential problems with your browser. In the column heading, the date and time (*date-time*) is represented in ISO 8601 format, a standard provided by the International Organization for Standardization (ISO). In this format: • Calendar date is represented in year-month-day format (*yyyy-mm-dd*) . • Time of day (*T*) is based on the 24-hour clock: *hh:mm:ss:mmm*. • *Z* indicates zero offset from coordinated universal time (UTC). In the report, the status of each setting is indicated, as follows: **Items marked with a critical icon X** Setting is not correct for z/OSMF. You must fix this problem before continuing with z/OSMF. **Items marked with a warning symbol !** Setting is not optimal for z/OSMF. It is recommended that you update the setting before continuing with z/OSMF. **No error indication** Setting is correct for z/OSMF.
Requirements	Recommended setting for your environment.

For the steps to resolve a problem, see the appropriate entry in the tool's online help. After updating a setting, use the browser reload button to run the environment checker again. Repeat this process until you have resolved all of the errors and warnings.

Figure 11 on page 74 shows an example of the environment checker report for a Firefox browser. Here, the tool detected that the browser is not enabled for cookies as required. The tool also found that the Firebug add-on is enabled in the browser, which could affect the performance of the browser session.



IBM z/OS Management Facility - Environment Checker Help

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

Environment Option	Settings as of 2009-04-24T09:59:47.093Z	Requirements
JavaScript	JavaScript enabled	Enable JavaScript
Cookies	Cookies not enabled	At a minimum, enable cookies for the z/OSMF server site
Pop-up Windows	Pop-up windows enabled	At a minimum, allow pop-up windows from the z/OSMF server site
Frames	Frames enabled	Enable frames
Screen Resolution	1920 by 1200	Minimum screen resolution of 1024 by 768
Browser Content Dimensions	900 by 772	Minimum browser content dimensions of 800 by 600
Browser Name and Version Browser User-Agent value	Firefox 3.0.8 Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.8) Gecko/2009032609 (CK-IBM) Firefox/3.0.8	Mozilla Firefox Version 2 or Version 3 Microsoft Internet Explorer Version 6 or Version 7
Operating System	Microsoft Windows XP	Microsoft Windows XP
Add-ons	Firebug console enabled	Firebug may cause a performance impact to z/OSMF
Plug-ins	IBM BluePages Add to NAB 1.1 Mozilla Default Plug-in Adobe Acrobat Shockwave for Director Java(TM) Platform SE 6 U11 Microsoft Office 2003 Google Update Shockwave Flash IBM Developer Kit for Windows, Java 2, 1.5.0 IBM Developer Kit for Windows, Java 2, 1.5.0 IBM Developer Kit for Windows, Java 2, 1.5.0 IBM Developer Kit for Windows, Java 2, 1.5.0 IBM Developer Kit for Windows, Java 2, 1.5.0 IBM Developer Kit for Windows, Java 2, 1.5.0 IBM Developer Kit for Windows, Java 2, 1.5.0 WebSphere Client Java Plug-in Java(TM) Platform SE 6 U11 Windows Media Player Plug-in Dynamic Link Library Microsoft® DRM Microsoft® DRM	Some plug-ins may cause a performance impact to z/OSMF
z/OSMF Login ID	guest	An unauthenticated user will be "guest"
z/OSMF Version	Version Number: 1 Release Number: 11 Build Number: %L%	z/OSMF version

Figure 11. Example of an environment checker tool report

Using a supported operating system

To work with z/OSMF, your workstation requires Microsoft Windows XP. No other versions of Windows are supported at this time.

For optimal viewing with z/OSMF, your workstation requires a minimum screen resolution of 1024 by 768 pixels.

Using a supported Web browser

To access z/OSMF on the z/OS system, your workstation requires one of the following Web browsers:

- Mozilla Firefox Version 2 or Version 3.0 (minimum service level 3.0.6)
- Microsoft Internet Explorer Version 6 or Version 7.

Recommended settings for the Mozilla Firefox browser

Table 14. Recommended settings for Firefox

Environment Option	Response
JavaScript	To work with z/OSMF, your browser must have JavaScript enabled. To enable JavaScript, do the following: 1. From the *Tools* menu, click **Options** → **Content** tab. 2. Ensure that the JavaScript check box is selected. 3. Click **OK**.
Cookies	To work with z/OSMF, your browser must have cookies enabled—if not for all sites, then at least for the z/OSMF site at your installation. To enable cookies for use by any site, do the following: 1. From the *Tools* menu, click **Options** → **Privacy** tab. 2. Ensure that the **Accept cookies from sites** check box is selected. 3. Click **OK**. To enable cookies for only the z/OSMF site, clear the **Accept cookies from sites** check box. Then, do the following: 1. Click **Exceptions**. 2. Enter the URL for the z/OSMF site at your installation. 3. Click **Enable** → **Close** → **OK**.
Pop-up Windows	For proper functioning with z/OSMF, your browser must be enabled for pop-up windows. To enable your browser for pop-up windows, do the following: 1. From the *Tools* menu, click **Options** → **Content** tab. 2. Clear the **Block pop-up windows** check box. 3. Click **OK**. To enable pop-up windows for the z/OSMF site only, ensure that the **Block pop-up windows** check box is selected. Then, do the following: 1. Click **Exceptions**. 2. Enter the URL for the z/OSMF site at your installation. 3. Click **Allow** → **Close** → **OK**.
Frames	To work with z/OSMF, your browser must have frames enabled. To enable your browser for frames, do the following: 1. In the browser input area, enter the following URL: `about:config`. 2. If a warranty warning message appears, click the **I'll be careful, I promise!** button to continue. 3. In the **Filter** field, enter `frames`. 4. Click `browser.frames.enabled` to set the **Value** field to `true`. 5. Close the browser to save the changes.

Table 14. Recommended settings for Firefox (continued)

Environment Option	Response
Screen Resolution	For optimal viewing with z/OSMF, your workstation requires a minimum screen resolution of 1024 by 768 pixels. To increase the screen resolution, do the following: 1. Right-click on the desktop and select **Properties** → **Settings** tab. 2. Move the slider to select a screen resolution of at least 1024 by 768 pixels. 3. Click **OK**.
Browser Content Dimensions	For optimal viewing with z/OSMF, your browser requires a usable content display area of at least 800 by 600 pixels. A number of factors can affect the size of your browser's usable content display area, such as Windows desktop appearance settings and the inclusion of toolbars for browser plug-ins. To check the desktop appearance settings, do the following: 1. Right-click on the desktop and select **Properties** to open the *Display Properties* dialog box. 2. Click the **Appearance** tab. 3. Click **Advanced**. 4. From the **Item** list, select **Active Title Bar** and verify that it is no larger than necessary (the default is 25 pixels). Similarly, check the setting for **Scrollbar** (the default is 17 pixels). 5. Click **OK** → **OK**. To remove unnecessary toolbars, do the following: 1. From the *View* menu in Firefox, click **Toolbars**. 2. For any unnecessary toolbars, clear the associated check box. As an alternative, you can maximize the browser window, thus eliminating the toolbars, by pressing the F11 function key. To restore the window to its previous size, press F11 again.
Add-ons	For optimal performance with z/OSMF, disable the Firebug add-on in your browser settings. To disable the Firebug add-on, do the following: 1. From the *Tools* menu, click **Add-ons** → **Extensions** tab. 2. Select the Firebug add-on and click the **Disable** option. 3. Restart the browser to have the changes take effect.

Table 14. Recommended settings for Firefox (continued)

Environment Option	Response
Plug-ins	Some plug-ins, such as JavaScript debuggers, can affect browser performance. For optimal performance with z/OSMF, include only required plug-ins with your browser. In the environment checker report, the **Settings** column shows the installed plug-ins for your browser. To verify this list, do the following: 1. In the browser input area, enter the following URL: `about:plugins`. 2. Compare the list of installed plug-ins to the list shown in the environment checker report to determine whether any add-ons should be disabled. To disable a plug-in, do the following: 1. From the *Tools* menu, click **Add-ons** → **Plugins** tab. 2. Scroll down the list to locate the plug-in. 3. Select the plug-in and click the **Disable** option. 4. Restart the browser to have the changes take effect.

Recommended settings for the Windows Internet Explorer browser

Table 15. Recommended settings for Internet Explorer

Environment Option	Response
JavaScript	To work with z/OSMF, your browser must have JavaScript enabled. To enable JavaScript, do the following: 1. From the *Tools* menu, click **Internet Options** → **Security** tab. 2. Click **Custom Level**. 3. Scroll down to *Scripting*, then *Active Scripting*. 4. Click **Enable**. 5. Click **OK** → **OK**.

Table 15. Recommended settings for Internet Explorer (continued)

Environment Option	Response
Cookies	To work with z/OSMF, your browser must have cookies enabled—if not for all sites, then at least for the z/OSMF site at your installation. To enable cookies for use by any site, do the following: 1. From the *Tools* menu, click **Internet Options** → **Privacy** tab. 2. Click **Advanced**. 3. Select the **Override automatic cookie handling** check box. 4. Select **Accept** for *First-party Cookies* and *Third-party Cookies*. 5. Click **OK** → **OK**. To enable cookies for only the z/OSMF site, clear the **Override automatic cookie handling** check box and select **Block** for *First-party Cookies* and *Third-party Cookies*. Then, do the following: 1. From the *Tools* menu, click **Internet Options** → **Privacy** tab. 2. Click **Sites**. 3. Enter the URL for the z/OSMF site at your installation. 4. Click **Allow**. 5. Click **OK** → **OK**.
Pop-up Windows	For proper functioning with z/OSMF, your browser must be enabled for pop-up windows. To enable your browser for pop-up windows, do the following: 1. From the *Tools* menu, click **Internet Options** → **Privacy** tab. 2. Clear the **Turn on Pop-up Blocker** check box. 3. Click **OK**. To enable pop-up windows for the z/OSMF site only, ensure that the **Turn on Pop-up Blocker** check box is selected. Then, do the following: 1. Select **Settings** 2. Enter the URL for the z/OSMF site at your installation. 3. Click **Add**. 4. Click **Close** → **OK**.
Frames	To work with z/OSMF, your browser must have frames enabled. To enable your browser for frames, do the following: 1. From the *Tools* menu, click **Internet Options** → **Security** tab. 2. Click **Custom Level**. 3. Scroll down to *Miscellaneous*, then *Launching programs and files in an IFRAME*. 4. Click **Enable**. 5. Click **OK**.

Table 15. Recommended settings for Internet Explorer (continued)

Environment Option	Response
Screen Resolution	For optimal viewing with z/OSMF, your workstation requires a minimum screen resolution of 1024 by 768 pixels. To increase the screen resolution, do the following: 1. Right-click on the desktop and select **Properties** → **Settings** tab. 2. Move the slider to select a screen resolution of at least 1024 by 768 pixels. 3. Click **OK**.
Browser Content Dimensions	For optimal viewing with z/OSMF, your browser requires a usable content display area of at least 800 by 600 pixels. A number of factors can affect the size of your browser's usable content display area, such as Windows desktop appearance settings and the inclusion of toolbars for browser plug-ins. To check the desktop appearance settings, do the following: 1. Right-click on the desktop and select **Properties** to open the *Display Properties* dialog box. 2. Click the **Appearance** tab. 3. Click **Advanced**. 4. From the **Item** list, select **Active Title Bar** and verify that it is no larger than necessary (the default is 25 pixels). Similarly, check the setting for **Scrollbar** (the default is 17 pixels). 5. Click **OK** → **OK**. To remove unnecessary toolbars, do the following: 1. From the *View* menu, click **Toolbars**. 2. For any unnecessary toolbars, clear the associated check box. As an alternative, you can maximize the browser window, thus eliminating the toolbars, by pressing the F11 function key. To restore the window to its previous size, press F11 again.
Add-ons	For optimal performance with z/OSMF, it is recommended that you include only required add-ons with your browser. To disable an add-on, do the following: 1. From the *Tools* menu, click **Manage Add-ons** → **Enable or Disable Add-ons**. 2. Scroll down the list to view the add-ons. 3. To disable an add-on, select it and click the **Disable** button. 4. Click **OK**. 5. Restart the browser to have the changes take effect.

Table 15. Recommended settings for Internet Explorer (continued)

Environment Option	Response
Plug-ins	Some plug-ins, such as JavaScript debuggers, can affect browser performance. For optimal performance with z/OSMF, it is recommended that you include only required plug-ins with your browser. In the environment checker report, the **Settings** column shows the installed plug-ins for your browser. To verify this list, do the following: 1. From the *Tools* menu, click **Manage Add-ons > Enable or Disable Add-ons**. 2. Scroll down the list to view the add-ons. 3. To disable an add-on, select it and click the **Disable** button. 4. Click **OK**. 5. Restart the browser to have the changes take effect.

Accessing the About page

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 panel for z/OSMF, do the following:

Procedure

1. Open a Web browser to the z/OSMF Welcome task.
2. Click the **About** link located in the upper right-hand corner of the Welcome task. Details about the product build level are displayed in a new browser window.

Working with z/OSMF runtime logs

During normal operations, z/OSMF writes runtime log data to files in the product logs directory. By default, this is `/var/zosmf/data/logs`. If a problem occurs with the logs directory, for example, the directory is not writable or z/OSMF encounters an error on initialization, z/OSMF includes its log data with the WebSphere servant log instead.

z/OSMF log and trace messages can be generated on the server (*server side*) or transmitted to the server by the client (*client side*). Both types of messages are written to the z/OSMF logs.

z/OSMF runtime logs are written in English only. z/OSMF log files are written in the ISO8859-1 code page (ASCII). To activate automatic conversion, you can set the environment variable _BPXK_AUTOCVT to "ON". Tools such as vi, emacs, and grep will display the text correctly.

To work with the logs, you require a user ID with superuser authority.

For examples of z/OSMF runtime log data, and a description of the log file format, see Appendix B, "Viewing z/OSMF runtime logs," on page 169.

During the configuration of the z/OSMF product, log data is written to a file in the z/OSMF configuration file system: `/etc/zosmf`. If a problem occurs with the log file, the log data is written, instead, to the directory specified by $TMPDIR, if this environment variable is set. Otherwise, the log data is written to the `/tmp` directory.

Maintaining the runtime logs directory

Check the z/OSMF runtime logs directory periodically and clean up files that are no longer needed.

You might also need to inspect the logs directory if Websphere Application Server ends abnormally. See "Managing log lock files"

Managing log lock files

When z/OSMF initializes, the log file handler creates a file named IZUG0.log.lck. This file represents a "lock" on the log data. Usually, lock files are cleaned up automatically as part of application shutdown. If Websphere Application Server ends abnormally, however, the lock files might remain. If so, the log file handler 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.

Changing the log level

Changing the level of logging and activating trace are performed by the same operation. For the steps, see "Enabling trace and logging for z/OSMF."

When 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.

Enabling trace and logging for z/OSMF

For diagnostic purposes, you might be asked by IBM Support to enable trace or logging for z/OSMF. This section provides instructions for performing these actions.

Enabling the trace for z/OSMF is done while the IBM WebSphere Application Server OEM Edition for z/OS server process runs. You can configure the server to start in a trace-enabled state, or change dynamically by setting the appropriate configuration properties, as described in the following sections:

- "Enabling trace and logging at server startup" on page 82
- "Enabling trace and logging on a running server" on page 82.

z/OSMF trace output is written to files in the z/OSMF logs directory.

Understand that trace carries a performance cost. Do not activate trace for z/OSMF unless directed to do so by IBM Support.

For more information about setting and analyzing trace data, see WebSphere Application Server for z/OS Information Center.

Enabling trace and logging at server startup

The diagnostic trace configuration settings for the IBM WebSphere Application Server OEM Edition for z/OS process determines the initial trace state. The configuration settings are read at IBM WebSphere Application Server OEM Edition for z/OS startup and used to configure the trace service. You can also change many of the trace service properties or settings while IBM WebSphere Application Server OEM Edition for z/OS is running.

The following are the steps for this task:

1. Log on to the WebSphere administrative console:

   ```
   https://hostname:port/ibm/console
   ```

   where:

   - *hostname* is the hostname or IP address of the system in which IBM WebSphere Application Server OEM Edition for z/OS is installed
   - *port* is the secure application port for the IBM WebSphere Application Server OEM Edition for z/OS configuration.
2. Select **Troubleshooting > Logs and Trace** in the console navigation area.
3. From the Logging and Tracing table, choose your server.
4. Click "**Change Log Detail Levels**".
5. Click the **Configuration** tab if it is not already selected.
6. Expand the * [All Components] tree.
7. Scroll down to **com.ibm.zoszmf.*** and select this. (If you are working with IBM Support, you might be directed to activate only a sub-package of this, such as **com.ibm.zoszmf.util.***.)
8. In the popup menu, hover on **Message and Trace Levels**, and select the "**finest**" option.
9. Click **Apply** and then **OK** to save the changed configuration.
10. Re-start the server.

Enabling trace and logging on a running server

You can modify the trace state for IBM WebSphere Application Server OEM Edition for z/OS and z/OSMF dynamically for a running server by using the following procedure.

The following are the steps for this task:

1. Log on to the WebSphere administrative console:

   ```
   https://hostname:port/ibm/console
   ```

   where:

   - *hostname* is the hostname or IP address of the system in which IBM WebSphere Application Server OEM Edition for z/OS is installed
   - *port* is the secure application port for the IBM WebSphere Application Server OEM Edition for z/OS configuration.
2. Select **Troubleshooting > Logs and Trace** in the console navigation area.

3. From the Logging and Tracing table, choose your server.
4. Click "**Change Log Detail Levels**".
5. Click the **Runtime** tab.
6. Expand the * [All Components] tree.
7. Scroll down to **com.ibm.zoszmf.*** and select this. (If you are working with IBM Support, you might be directed to activate only a sub-package of this, such as **com.ibm.zoszmf.util.***.)
8. In the popup menu, hover on **Message and Trace Levels**, and select the "**finest**" option.
9. Click **Apply** and then **OK** to save the changed runtime settings.

Your changes take effect immediately. Your changes are discarded when the server is restarted.

Common problems and scenarios

z/OSMF is based on a stack of components, starting with the application running in the user's workstation internet browser and extending to the lower level z/OS functions and components that deliver much of the underlying function. This section discusses troubleshooting topics, procedures and tools for recovering from a set of known issues.

Troubleshooting topics are included for the following problems and scenarios:

- "Problems during configuration"
- "Problems identified by the installation verification program (IVP)" on page 86
- "Problems when accessing the user interface" on page 92
- "Problems when using Configuration Assistant" on page 99
- "Problems when using the Incident Log task" on page 100
- "Problems when attempting to send data" on page 105.

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:

- "Incident Log setup script cannot locate CEAPRM00 member" on page 84
- "CEA parmlib member activation fails" on page 84
- "Failure in Incident Log setup script or verify script, or CIM server abends" on page 85
- "Failure of an operator command, such as DUMP" on page 85
- "Verify script fails with an authorization failure for the z/OSMF administrator" on page 86
- "Verify script fails when creating the IVP report" on page 86.

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 G, "Common event adapter (CEA) reason codes," on page 183.

Incident Log setup script cannot locate CEAPRM00 member

Symptom: While performing "Step 5: Complete the setup" on page 35, the script **izusetup.sh** 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 parmlib data set (*source parmlib*) that you specified earlier as input (see "Step 1: Create the initial configuration" on page 27). However, the source parmlib data set is:

1. Missing or is not cataloged
2. Missing the CEAPRM00 member
3. Protected through a RACF data set profile (for example, SYS1.*), but the z/OSMF administrator identity is not permitted to the profile.

By default, the source parmlib data set is SYS1.PARMLIB.

Corrective Actions: Ensure that the parmlib data set:

1. Exists and is cataloged
2. Contains the IBM-supplied member CEAPRM00
3. If protected through a RACF data set profile, the z/OSMF administrator identity is permitted to the data set profile. To grant this permission, use the following command, where ZOSMFAD is the user ID to be authorized to the data set profile SYS1.*:

   ```
   PERMIT SYS1.* ID(ZOSMFAD) ACCESS(READ)
   ```

CEA parmlib member activation fails

Symptom: When performing "Step 5: Complete the setup" on page 35, the script **izusetup.sh** 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*nn* parmlib member (by default, CEAPRM01). This error can occur if the configuration script copied the CEAPRMxx member to a target parmlib data set that is not in your installation's parmlib concatenation. You specified the target parmlib data set earlier when you ran the script described in "Step 1: Create the initial configuration" on page 27. By default, this is data set SYS1.PARMLIB.

Corrective Action: To resolve the problem, copy the CEAPRMxx member to your parmlib concatenation. Then, enter the following command to activate the new CEAPRMxx member, where *xx* represents the member suffix:

```
MODIFY CEA,CEA=xx
```

To verify that the new CEAPRMxx parmlib member is in effect, enter the MODIFY command, as follows:

```
MODIFY CEA,DISPLAY,PARMS
```

Ensure that the new member:

- Defines HLQ(CEA) and SNAPSHOTS(Y) to allow CEA to create diagnostic snapshots of the system logs
- Sets the IBM branch and country code values for your installation
- Defines the storage value for parmlib (an SMS class or a string of volume names).

It is recommended that you edit your active IEASYSxx parmlib member to identify the CEAPRMxx parmlib member to use for the next IPL of the system. Specify the CEAPRMxx member suffix on the CEA=xx statement of IEASYSxx.

For more information about the CEAPRMxx parmlib member, see *z/OS Initialization and Tuning Reference*, which is available online in the IBM z/OS Internet Library.

Failure in Incident Log setup script or verify script, or CIM server abends

Symptoms:

- While performing "Step 5: Complete the setup" on page 35, the script **izusetup.sh** fails.
- 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`.

Failure of an operator command, such as DUMP

Symptom: When performing "Step 5: Complete the setup" on page 35, the script **izusetup.sh** fails. SYSLOG contains messages related to authorization errors.

Possible Cause: The z/OSMF administrator lacks OPERCMDS access.

Corrective Action: If your installation protects MVS commands with the RACF class OPERCMDS, you must grant the proper authority to the z/OSMF administrator user ID.

- To grant DUMP command access to the z/OSMF administrator, enter the PERMIT command as follows. This authorization is required for the Incident Log verify step to complete.

  ```
  PERMIT MVS.DUMP CLASS(OPERCMDS) ID(ZOSMFAD) ACCESS(CONTROL)
  ```

- To allow the z/OSMF administrator to use all operator commands, enter the PERMIT command as follows:

  ```
  PERMIT MVS.** CLASS(OPERCMDS) ID(ZOSMFAD) ACCESS(CONTROL)
  ```

- To grant the z/OSMF administrator access to particular operator commands, enter the PERMIT command with one or more of the profiles shown in Table 16 on page 86, as appropriate for your installation.

Table 16. Authorizing the z/OSMF administrator 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

Verify script fails with an authorization failure for the z/OSMF administrator

Symptom: While performing "Step 5: Complete the setup" on page 35, the script **izusetup.sh** fails with an authorization failure message for the z/OSMF administrator identity.

Possible Cause: Your installation uses the RACF PROTECT-ALL option to protect its data sets, but you did not define the CEA.* RACF profile.

Corrective Action: If your installation uses PROTECT-ALL, you must define a CEA.* data set profile to RACF and permit CEA and the z/OSMF administrator identity. For example:

```
ADDSD 'CEA.*' UACC(NONE)
PERMIT 'CEA.*' ID(CEA) ACCESS(ALTER)
PERMIT 'CEA.*' ID(ZOSMFAD) ACCESS(ALTER)
```

Verify script fails when creating the IVP report

Symptom: While performing "Step 5: Complete the setup" on page 35, the script **izusetup.sh** fails with a message indicating that no z/OS UNIX processes are available for the z/OSMF administrator identity.

Possible Cause: When the z/OSMF administrator user ID is created, it uses the MAXPROCUSER setting specified in your installation's BPXPRMxx member. MAXPROCUSER specifies the maximum number of processes that a single user can have active concurrently. You might need to increase this value for the z/OSMF administrator user ID.

Corrective Action: Use the RACF ALTUSER command to specify a larger number of z/OS UNIX processes (at least 1000) for the z/OSMF administrator. To set this value in the OMVS segment of the user ID, enter the following command, where `ZOSMFAD` is the user ID of the z/OSMF administrator:

```
ALTUSER ZOSMFAD OMVS(PROCUSERMAX(1024))
```

Problems identified by the installation verification program (IVP)

This topic provides troubleshooting tips for system setup problems identified by the Incident Log installation verification program (IVP). Included are procedures

and methods for performing problem determination and for troubleshooting the status of the different system components.

Using the installation verification program

The Incident Log installation verification program (IVP) checks the z/OS system setup to determine actions that might have been missed during z/OSMF configuration.

About the installation verification program

The IVP checks for the following conditions, all of which are required for successful operation of the Incident Log task:

- CEA component is available
- System REXX component is available
- User is authorized for the Incident Log resources associated with CEA and CIM
- Sysplex dump directory is available and accessible
- AMATERSE program is enabled to run
- System REXX execs are available and operational
- System Logger is available
- Operations log (OPERLOG) and logrec snapshots are accessible
- Dump analysis and elimination (DAE) is active and its symptom data set is available.

Running the installation verification program

To run the Incident Log IVP, your user ID must be permitted to enter operator commands. To add this authority, enter the RACF PERMIT command, as follows:

```
PERMIT MVS.** CLASS(OPERCMD) ID(userid) ACCESS(CONTROL)
```

To invoke the IVP program in a z/OS UNIX shell environment, enter the following command:

```
/usr/lpp/wbem/bin/cimcli ei IBMzOS_PDW_IVP -niq
```

Alternatively, you can invoke the IVP 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 12. Invoking the Incident Log IVP as a batch job

Reviewing the results of the installation verification program

On completion, the IVP writes the results to the file **izuincidentlogverify.report**, which resides in the following directory: `/etc/zosmf`

Corrective actions for identified problems are provided in "Resolving problems identified by the installation verification program."

Resolving problems identified by the installation verification program

This topic provides corrective actions for system setup problems identified by the Incident Log installation verification program (IVP).

Troubleshooting topics are included for the following problems and scenarios:

- "CEA address space is not running"
- "System REXX address space is not running"
- "User is not authorized"
- "Unable to locate an incident in the sysplex dump directory" on page 89
- "Unable to open the sysplex dump directory" on page 89
- "SYS1.MIGLIB is not APF-authorized" on page 90
- "Another resource is using the sysplex dump directory" on page 90
- "Unable to generate prepared data set" on page 90
- "User is not SAF authorized" on page 90
- "System logger not available" on page 91
- "Unable to find the active DAE data set name" on page 91
- "System REXX cannot process cannot process the request" on page 91
- "Unable to allocate the prepared data set to be tersed" on page 91
- "Unable to find the OPERLOG snapshot" on page 91
- "Sysplex dump directory has no space allocated" on page 92
- "Unable to allocate new data set" on page 92
- "No diagnostic data available" on page 92
- "Internal error encountered. CEA return code: CEA reason code: " on page 92

CEA address space is not running

Possible Cause: CEA address space is not active.

Corrective Action: Start the CEA address space. For information, see "Ensuring that CEA is active" on page 165.

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 active" on page 166

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 **izuaddloguser.sh** script, which is used to authorize the user; see "Creating commands to authorize a user to all tasks" on page 40. Ensure that the user has the appropriate permission to the CEA classes required for using the Incident Log task; see Appendix F, "Common event adaptor (CEA) security profiles," on page 181.

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 13 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=*
 //SYSTSIN  DD *
 IPCS
 LISTDUMP SYMPTOMS
 END
 /*
```

Figure 13. Checking the sysplex dump directory—sample job for creating an IPCS report

Unable to open the sysplex dump directory

Possible Causes:

- 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 165.
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 163.

SYS1.MIGLIB is not APF-authorized

Possible Cause: The SYS1.MIGLIB data set, which contains the AMATERSE program, is not APF-authorized.

Corrective Action: APF-authorize the SYS1.MIGLIB data set. For information, see "Authorizing the SYS1.MIGLIB data set" on page 167.

Another resource is using the sysplex dump directory

Possible Cause: Another program is accessing the sysplex dump directory (by default SYS1.DDIR) exclusively and must free it. Programs that obtain exclusive (ENQ) access to the data set include DUMPSRV post-dump processing and common event adapter (CEA) when using IPCS service routines.

Corrective Actions: Check the sysplex dump directory usage:

1. Enter the command `D GRS` and check for contention on the sysplex dump directory data set.
2. If an IPCS user is holding the ENQ exclusively, consider cancelling that user's TSO session.
3. If CEA is holding the ENQ exclusively, enter the following command to end the CEA usage of the directory data set: `MODIFY CEA,DROPIPCS`
4. Try the request again later.

For more information, see "Creating the sysplex dump directory" on page 163.

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 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 active" on page 166.

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 common event adapter (CEA) component cannot access the OPERLOG or logrec snapshot log stream when preparing incident data to be sent.

Corrective Action: Enter the command `D LOGGER` and verify that system logger is active. For information about system logger and the log streams, see:
- "Defining a couple data set for system logger" on page 156
- "Enabling the operations log (OPERLOG)" on page 158
- "Defining and activating the logrec log stream" on page 160.

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 162.

System REXX cannot process cannot process the request

Possible Cause: The System REXX environment cannot process an exec. This problem usually indicates that the runtime support for compiled REXX has not been set up.

Corrective Action: The REXX library or the REXX Alternate library data set must be added to the LINKLIST concatenation or LPA. For more information, see *IBM Compiler and Library for REXX on zSeries: User's Guide and Reference*, which is available online in the IBM z/OS Internet Library.

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 *MVS System Messages*, which is available online in the IBM z/OS Internet Library.

Unable to find the OPERLOG snapshot

Possible Cause: The OPERLOG snapshot was not created. When accessing the OPERLOG snapshots, the system logger service IXGCONN received a bad return or reason code, indicating that the OPERLOG snapshot does not exist. It is possible that system logger is not active.

Corrective Action: Check the system logger setup:

1. Verify that the user has authorization to the OPERLOG DASD log stream.
2. Enter the command `DISPLAY LOGGER,LOGSTREAM` and verify the name of the OPERLOG snapshots (defined when configuring the DASD log streams).

For more information, see "Enabling the operations log (OPERLOG)" on page 158.

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 165.

Unable to allocate new data set

Possible Cause: When preparing incident materials to be sent through FTP, z/OSMF could not allocate a new data set to contain the tersed diagnostic snapshot.

Corrective Action: Look for system messages indicating why the failure occurred in the CIM trace associated with the failed return code. For assistance, contact IBM Support.

No diagnostic data available

Possible Cause: The prepare error log did not accumulate any data within the current time interval.

Corrective Action: To specify a larger time interval for error log snapshots, modify the CEAPRMxx member statements as shown in Figure 14:

```
DUMPCAPTURETIME
(
SLIP(OPERLOG(01:00:00) LOGREC(01:00:00)
LOGRECSUMMARY(24:00:00))
DUMP(OPERLOG(01:00:00) LOGREC(01:00:00)
LOGRECSUMMARY(24:00:00))
ABEND(OPERLOG(01:00:00) LOGREC(01:00:00)
LOGRECSUMMARY(24:00:00))
)
```

Figure 14. 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 Table 21 on page 183. 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" on page 93

Browser cannot connect to z/OSMF

When logging into z/OSMF for the first time, your browser either does not connect, or waits indefinitely. Verify that the browser has network connectivity to the host on which the IBM WebSphere Application Server OEM Edition for z/OS instance is running. If your network connectivity is functioning properly, there might be an issue with the digital certificates used for SSL connections.

For more information on working with certificates, see *IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide, Version 7.0*, GA32-0631, and WebSphere Application Server for z/OS Information Center.

Missing initialization message or JSP processing error when attempting to use z/OSMF from browser

Symptoms: The following symptoms occur in this sequence:

1. You start IBM WebSphere Application Server OEM Edition for z/OS on the system where z/OSMF is installed, but see no message on the operator log about whether z/OSMF started successfully or failed.
2. You attempt to access the z/OSMF URL but encounter a "JSP Processing Error" with HTTP code 500, along with some text like the following with supporting messages:

   ```
   JSPG0049E: /NavigationTree.jsp failed to compile
   ```

3. You examine z/OSMF logs, find that they are empty or have no new messages since starting IBM WebSphere Application Server OEM Edition for z/OS. No .lck file exists either, which suggests that the logs are not active.
4. You examine IBM WebSphere Application Server OEM Edition for z/OS servant logs and search for "IZUG" looking for message codes. While none exist, you notice that the search reveals the following:

   ```
   UTLS0002E: The shared library IzuSrvLibs contains a classpath entry
   which does not resolve to a valid jar file, the library jar file is
   expected to be found at /usr/lpp/zosmf/V1R11/lib/izugjni.jar.

   UTLS0002E: The shared library IzuAppLibs 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/V1R11/lib/izug.jar.
   ```

Possible Cause: A failure of the JSP to compile typically means that one or more of the required classes could not be found. Most likely, this is a problem with a referenced shared library. The errors in the Websphere logs support this possibility.

Failures with the shared libraries typically mean either of two things:
- Shared libraries class path entries are incorrect.
- Class path entries point to missing JAR files.

In this situation, the WebSphere message shows which paths were not found.

Investigation:

1. Examine the contents of the directory where the JARs are supposed to exist:

   ```
   # ls /usr/lpp/zosmf/V1R11/lib
   ls: FSUM6785 File or directory "/usr/lpp/zosmf/V1R11/lib" is not found
   ```

2. The directory does not exist, so inspect which file systems are mounted. Figure 15 shows an example.

```
# df
Mounted on     Filesystem                Avail/Total    Files      Status
/u/tt          (/SY1/tt)                 2097040/2097152 262130     Available
/SY1/dev       (/SY1/dev)                2096968/2097152 262121     Available
/SY1/tmp       (/SY1/tmp)                2097008/2097152 262126     Available
/SY1/var       (/SY1/var)                2027464/2097152 253433     Available
/u/wasoemcfg   (IBMUSER.CONFIG.FS)       446176/921600  4294924496 Available
/VRA/usr/lpp/zWebSphereOEM/V7R0 (WAS.HBBN700.DRIVER2.MAR27)
185540/3456000 4294940390 Available
/VRA/usr/lpp/java (MVSBUILD.ZFSVIC.JAVA531) 48808/1094400  4294964768 Available
/ict           (CIMPROV.PEV078.ZFS)      16634/36000    4294967229 Available
/SY1/etc       (ZOS111.SY1.ETC.ZFS)      2926/4320      4294967044 Available
/VRA           (ZOS111.ROOT.ZFS)         84546/286560   4294966025 Available
/SY1           (ZOS111.SY1.ZFS)          1124/1440      4294967283 Available
/              (CIMPROV.SYSPLEX.ROOT.ZFS) 1120/1440      4294967276 Available
/u/zodirm      (PEVID.ZODIRM.HFS)        3928/11520     4294967272 Available
/u             (IBMUSER.WORK.HFS)        173848/432000  4294966640 Available
/VRA/usr/lpp   (ZOS111.LPP.HFS)          826352/2662560 4294956529 Available
/VRA/usr/lib/nls (ZOS111.NLS.HFS)          73496/2374560  4294964743 Available
/VRA/usr/man   (ZOS111.MAN.HFS)          6752/20160     4294967192 Available
```

Figure 15. Determining which files systems are mounted

In Figure 15, notice that the display is missing the file system that should be mounted at the location `/usr/lpp/zosmf/V1R11`.

Corrective Action: Mount the necessary file system in the correct location and restart IBM WebSphere Application Server OEM Edition for z/OS.

Certificate error in Mozilla Firefox Version 3

When logging into z/OSMF for the first time, you might notice that the Mozilla Firefox Version 3 browser displays the error message: `Secure Connection Failed` (Figure 16 on page 95).

Figure 16. Connection failure message in Firefox Version 3

The error message occurs because the browser does not recognize the self-signed Certificate Authority (CA) certificate configured in the application server hosting the z/OSMF application.

To resolve the certificate error message, you can use either of the following methods:

- "Adding the CA certificate to the security exceptions list"
- "Importing the CA certificate into your browser" on page 96.

These methods are described in the sections that follow.

Adding the CA certificate to the security exceptions list

You can allow your browser to bypass the Secure Connection Failed message for z/OSMF.

Do the following:

1. On the error page, click **Or you can add an exception**.
2. Click **Add Exception**. The *Add Security Exception* dialog is displayed.
3. Click **Get Certificate**.
4. Click **View** to display a window that describes the problem with your z/OSMF site. Figure 17 on page 96 shows an example.

Figure 17. Connection failure message in Firefox Version 3

Examine the *Issued To* fields. Verify that the information identifies the WebSphere application server that is hosting z/OSMF. The value for *Common Name (CN)* should match the host name for your installation of z/OSMF.

Examine the *Issued By* fields. Verify that the certificate was issued by the certificate authority (CA) that was used to generate the server certificate. By default, IBM WebSphere Application Server OEM Edition for z/OS uses the certificate authority *WAS CertAuth for Security Domain*.

To see the other fields of the certificate, select the *details* tab.

5. After you have verified the certificate, close the dialog. If you leave the **Permanently store this exception** check box selected, Firefox stores the certificate information to prevent the error from being displayed again for the z/OSMF site.
6. Click **Confirm Security Exception** to trust the z/OSMF site.

Your browser will now connect to the z/OSMF application.

Importing the CA certificate into your browser

You can import the CA certificate into your browser. Doing so involves exporting the IBM WebSphere Application Server OEM Edition for z/OS certificate from RACF, transferring the CA certificate to your workstation, and importing the CA certificate into your browser.

The CA certificate is determined by the WebSphere configuration file that you used to create the IBM WebSphere Application Server OEM Edition for z/OS instance. The file provides the controller id (zControlUserid=WSCRU1) and the SAF keyring name (zDefaultSAFKeyringName=WASKeyring.BBNBASE).

To import the CA certificate into your browser, do the following:

1. List the keyring for the controller user ID using the RACDCERT command, for example:

```
RACDCERT ID(WSCRU1) LISTRING(*)
```

Figure 18 shows an example of the output from the RACDCERT command.

```
Digital ring information for user WSCRU1:

  Ring:
       >WASKeyring.BBNBASE<
  Certificate Label Name              Cert Owner     USAGE      DEFAULT
  --------------------------------    ------------   --------   -------
  WebSphereCA                         CERTAUTH       CERTAUTH     NO
  Verisign Class 3 Primary CA         CERTAUTH       CERTAUTH     NO
  Verisign Class 1 Primary CA         CERTAUTH       CERTAUTH     NO
  RSA Secure Server 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
  Verisign International Svr CA       CERTAUTH       CERTAUTH     NO
  DefaultWASCert.BBNBASE              ID(WSCRU1)     PERSONAL     NO
  DefaultDaemonCert.BBNBASE           ID(WSCRU1)     PERSONAL     YES

  Ring:
       >WASKeyring.BBNBASE.Root<
  Certificate Label Name              Cert Owner     USAGE      DEFAULT
  --------------------------------    ------------   --------   -------
  WebSphereCA                         CERTAUTH       CERTAUTH     NO
```

Figure 18. Digital ring information for the controller user ID

Verify that the configured SAF keyring is shown for the controller user ID. Note the keyring name and the certificate label (WebSphereCA, in this case).

2. Export the CA certificate using the RACDCERT command, for example:

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

3. Transfer this file in binary format to your workstation. Keep the `.der` extension when you transfer the file.
4. To import the certificate into the Firefox browser, do the following:
   a. From the *Tools* menu, click **Options** → **Advanced** tab.
   b. Click **View Certificates**.
   c. Select the *Authorities* tab.
   d. Click **Import**.
   e. From the *Select File* menu, navigate to the folder to which you transferred the CA certificate.
   f. Select the certificate file and click **Open**.
   g. In the dialog box, select the *Trust this CA to identify web sites* check box. You can also click **View** to examine the certificate.
   h. To import the certificate to your browser, click **OK**.

Your browser will now open to the z/OSMF interface.

Cannot log into z/OSMF

If you receive an error while attempting to log into z/OSMF, try troubleshooting with the following steps.

Procedure

1. Verify that your user ID is correct and then try logging in. If you are still not able to log in, continue to the next step.

2. Ensure that the password associated with your user ID is correct. If you are still not able to log in, continue to the next step.
3. It is possible that the password for your user ID has expired. Try creating a new password for the user ID and then log in.
4. If you are attempting to log in with a password phrase (pass phrase), your installation's security product might need to be updated to allow mixed case passwords. In a system with RACF, for example, your security administrator can use the SETROPTS PASSWORD(MIXEDCASE) option to allow mixed-case passwords at your installation. After this change is made, your installation must restart IBM WebSphere Application Server OEM Edition for z/OS. For more information, see *z/OS Security Server RACF Security Administrator's Guide*, which is available online in the IBM z/OS Internet Library. Also, see the WebSphere Application Server for z/OS Information Center.
5. Ensure that the appropriate script has been run for your user ID; see "Authorizing more users to z/OSMF" on page 40.

What to do next

If none of these steps resolve the problem, contact your system programmer for assistance.

End user messages for authentication errors are often general by design, to avoid providing malicious users with valuable information, such as whether a particular user ID is valid. More specific information about this error might be available to your system programmer in the form of messages written to the operator console or to the operator log. Typically, these problems are caused by incorrect passwords or user IDs that have been revoked.

Message or help information is not available

Symptom: Help information for messages or panels is not available.

Possible Cause: The associated help files are missing, are not readable, or new files were installed and z/OSMF was not restarted.

Corrective Action:

1. Verify that the following file is present and readable: `/usr/lpp/zosmf/V1R11/helps/plugins/zosmf.properties`. Note that all help files are stored at `/usr/lpp/zosmf/V1R11/helps/plugins`
2. To use any changes to the help files, you must restart the Enterprise Archive (EAR) file or IBM WebSphere Application Server OEM Edition for z/OS.

Security prompt when accessing help

Symptom: When using Windows Internet Explorer Version 6, a security prompt is displayed when you access the z/OSMF help information. The prompt is a pop-up window that displays the following message:

```
This page contains both secure and nonsecure items.
Do you want to display the nonsecure items?
```

You can ignore this prompt. To clear it, click **Yes**.

Corrective Action: If it is acceptable for the browser to display mixed content, you can disable the security prompt.

To disable the security prompt in Windows Internet Explorer, do the following:

1. From the *Tools* menu, click **Internet Options** → **Security** tab.
2. Click **Custom Level**.
3. Scroll down to *Miscellaneous*, then *Display mixed content*.
4. Click **Enable**.
5. Click **OK** → **Yes** → **OK**.

This is a browser-wide setting. If you disable the security prompt, it is no longer displayed for Web sites with mixed content.

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 Info**. A zip file of troubleshooting information is created.

2. Send the zip file to IBM Support.

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

Symptom: On selecting the Incident Log task, the user receives an error message indicating a lack of authorization to CEA.

Probable cause: During the configuration of z/OSMF, the configuration script defines the resource CEA.CEAPDWB*. However, the resource CEA.* was already defined by your installation. Because CEA.CEAPDWB* takes priority over CEA.* no z/OSMF users are authorized to make CIM requests.

Corrective Action: Give z/OSMF users access to CEA.CEAPDWB*. If you have CEA security definitions configured, you might already have the CEA.* resource defined.

Incidents have only dumps associated with them, no other diagnostic logs

Possible Causes:
1. System on which the incident occurred is earlier than z/OS V1R10.
2. The system ran out of space when gathering diagnostic snapshots.

Corrective Actions:

1. None. This processing is normal when the detecting system is at a lower level. A subset of the properties are captured, but not all of them.
2. Rerun the Incident Log task IVP. Check SYSLOG for message CEA600I and resolve the issue. The "additional message text" identifies the problem that was detected. Examples include CDS out of space, no data within specified time range, and other system logger error conditions. Also, if SNAPSHOT(Y) is specified in your CEAPRMxx member, ensure that the sysplex dump directory, log stream, OPERLOG in log stream, logrec in log stream, volume or STORAGE class have sufficient space. Check SYSLOG for CEA600xI messages.

Contents of Diagnostic Data do not show the entire interval, only 10 minutes. The logrec summary is missing.

Possible Cause: When CEA detects that ABEND SVC dumps are occurring frequently (within 10 minutes of each other), the amount of data collected is reduced on each subsequent dump encountered. This behavior protects the system from collecting inordinate amounts of duplicate data in a recurring dump situation.

Corrective Action: None; the system behavior is normal.

Incident information does not match the dump content

When a dump is opened, its information does not match the information in the Incident Log task. For example, the incident is identified as a GRS dump, but the associated dump is for a BPX incident.

Possible Causes:

1. Your installation has not configured automatic dump data set allocation. CEA expects that automatic dump data set allocation is in use, and that data set names are created dynamically based on a specified naming convention. If your installation uses pre-allocated dump data sets (SYS1.DUMPxx) instead of automatic dump data set allocation, it is possible that the Incident Log task has accessed a dump data set that has been reused.
2. The dump was copied to another data set and was renamed, for example, through an installation-supplied automation program.
3. The dump was copied to an uncataloged data set. If so, the system cannot locate the dump, which results in the following problems:
   - CEA cannot locate the dump
   - Incident Log task cannot identify the dump data set
   - Incident Log Send Diagnostic Data wizard cannot include the dump with the other diagnostic materials.

Corrective Actions:

1. Configure automatic dump data set allocation. See "Configuring automatic dump data set allocation" on page 161. If your installation uses pre-allocated dump data sets (SYS1.DUMPxx), modify your dump data set copy job to invoke the MODSDDIR program, as described in "Ensuring that dump data set names are correct" on page 166. This job modifies the sysplex dump directory to refer to the new dump data set name.
2. If your installation has automation that copies the dump to another data set with a different name, the automation must also invoke a program that modifies the sysplex dump directory to use the new dump data set name. For information, see "Ensuring that dump data set names are correct" on page 166.

3. If dumps are being copied to an uncataloged data set, modify the data set to be cataloged.

Logrec summary report missing from diagnostic data, but the other diagnostic data is available

Possible Cause: ABEND dumps that occur within a small time window (10 minutes) do not result in the system creating a logrec summary report. This is a self-protecting feature of the system to prevent inordinate amounts of duplicate data from being collected.

Corrective Actions:
1. If the dumps are being collected within minutes of each other, the system is working as designed.
2. If the SVC dump occurred in isolation and the logrec summary information is missing, check SYSLOG for message CEA0600I or CEA0602I.

User encounters message ICH408I

```
ICH408I USER(user ) GROUP(group ) NAME(user ) 031
CATALOG.SYVPLEX.MASTER CL(DATASET ) VOL(volser)
INSUFFICIENT ACCESS AUTHORITY
FROM CATALOG.*.MASTER (G)
ACCESS INTENT(UPDATE ) ACCESS ALLOWED(NONE )
```

Possible Cause: A user with insufficient authority is attempting to update the master catalog while creating the data diagnostic files. As a result, an Incident Log task request to FTP materials cannot compress (terse) the diagnostic snapshot data set.

Corrective Action: Allow the user to create catalog entries, as follows:

- To authorize a user to create entries in the master catalog:

```
RALTER GLOBAL DATASET ADDMEM('CATALOG.**'/UPDATE)
ADDSD  'CATALOG.**' UACC(UPDATE)
SETR   GLOBAL(DATASET) REFRESH
```

- To authorize a user to create entries in a user catalog:

```
DEFINE ALIAS(NAME(CEA) RELATE(<usercatalog name>))
```

Incidents not appearing in the Incident Log task

The corresponding dump-related incident is not part of the Incident Log task display.

Possible Causes: This problem can occur for a number of reasons:
1. The z/OS system is not configured to write dumps to data sets.
2. An error occurred when the dumping services address space (DUMPSRV) attempted to write information about the SVC dump to the sysplex dump directory. DUMPSRV makes several attempts to update the sysplex dump directory with information describing the dump. If these attempts fail, no entry is made and no information about the dump incident is retrieved.
3. The sysplex dump directory contains more than 500 incidents, however, z/OSMF searches a maximum of 500 of the incidents that are stored in the

dump directory to retrieve the set of incidents that match the date and time filter criteria. Other incidents that match the date and time filter criteria, if any, are not included in the log. The Incident Log task can display no additional incidents while the directory contains more than 500 incidents.

Corrective Actions:

1. Ensure that dump data set handling has been configured for the z/OS system. See "Configuring automatic dump data set allocation" on page 161.
2. If you know the dump data set name, you can add it to the sysplex dump directory by running a job that issues the IPCS ADDDUMP command. Also, Figure 13 on page 89 shows a job you can use to create a report of the contents of the sysplex dump directory.

   Attention: Never access the sysplex dump directory from an IPCS user session. Doing so ties up DUMPSRV and CEA. Always use a batch job to perform this operation. See "Establishing a larger sysplex dump directory" on page 165.
3. Delete incidents from the log (which removes them from the sysplex dump directory). Check with your system programmer to determine whether older dumps can be deleted from the sysplex dump directory.

Only the dump data set name is provided for an incident

Possible Causes:

1. System on which the incident occurred is earlier than z/OS V1R10.
2. SVC dump was not cataloged when the system programmer added it to the sysplex dump directory through the ADDDUMP IPCS command.

Corrective Actions:

1. None. This processing is normal when the detecting system is at a lower level.
2. Catalog the data set on the system and run the IPCS ADDDUMP job to add information about the dump to the sysplex dump directory.

Never access the sysplex dump directory from an IPCS user session. Doing so will tie up DUMPSRV and the Incident Log task. Always use a batch job to perform this operation as quickly as possible.

Allow Next Dump is not operational

Possible Cause: TSO/E is not configured to support DAE.

Corrective Action: Check that the active IKJTSOxx parmlib member includes the program name ADYOPCMD in the AUTHCMD NAMES section. For more information, see the topic on accessing the DAE data set in *Diagnosis: Tools and Service Aids*, which is available online in the IBM z/OS Internet Library.

Logrec report is not created because of authorization error

Symptom: User receives the following authorization error message:

```
- SY1  CEA0602I The z/OS Diagnostic Snapshot option failed.
- SNAPSHOT TYPE:LOGREC DETAIL REPORT
- DIAG1 = 12 DIAG2 = ALLOC DD DIAG3 = 12
- SOURCE NAME: CEA.L00.C3EEE2D2.P0C75366
- TARGET NAME: CEA.L00.C3EEE2D2.P0C75366.X00.TRS
```

Diagnostic messages:

```
- IKJ56893I DATA SET CEA.L00.C3EEE2D2.P0C75366.X00.TRS.TOURIST NOT
-  ALLOCATED+
- IGD17012I USER NOT AUTHORIZED TO DEFINE DATA SET
```

Possible Cause: The user is not authorized to define CEA data sets.

Corrective Actions:

1. Authorize the user to access CEA data sets. For example:

   ```
   PERMIT 'CEA.*' CLASS(DATASET) ID(ZOSMFAD) ACCESS(ALTER)
   ```

2. If errors continue, check for message CEA0602I in SYSLOG. The diagnostic message area contains the original error messages issued as part of the request. Review the messages to understand the problem and determine a solution.

Dump incident occurs in the sysplex, but only OPERLOG snapshot data is collected. Logrec snapshot is not collected.

Possible Cause: Logrec is setup to use a data set instead of a log stream.

Corrective Action:

1. Define the logrec log stream by using the system logger program IXCMIAPU.
2. Switch logrec to using the log stream by entering the command `SETLOGR LOGSTREAM`

For more information, see "Defining and activating the logrec log stream" on page 160.

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 UI 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 from the installation doing maintenance on the sysplex dump directory data set.

Corrective Action: Use the `F CEA,DROPIPCS` command to disconnect CEA from the IPCS sysplex dump directory data set. Use this command if you are locked out from performing the maintenance of the 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))
```

When deleting an incident, user is asked whether to mark the corresponding symptoms as eligible to take the next dump. Should the user say "yes"?

Background: The "Take Next Dump" option allows another dump to be taken after the problem is corrected. The function provides an alternative to doing this step manually through IPCS 3.6 (or ADYDSP). The system prompts the user in case your installation would prefer to continue suppressing such symptoms. Note that marking a symptom in the DAE table to allow the next dump to be taken requires recycling DAE, which is done automatically by the IPCS exec after modifying the symptom entry in the DAE data set.

Corrective Action: Respond Yes. The corresponding processing determines if DAE is active, and if the symptom string is indeed in the DAE table. If neither is the case, no action is taken.

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 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.

After deleting an incident with multi-system dumps, only the primary dump was deleted and the remote dumps are not deleted

Possible Cause: Dump storage is not set up to be shared across the systems in the sysplex.

Corrective Action: Delete the remote dumps manually. Then, define the dump storage using an SMS storage class or a shared volume that is managed through a shared catalog in the sysplex.

Problems when attempting to send data

When you invoke the Send Diagnostic Data wizard from the Incident Log task, the information supplied in the panel is used to produce one FTP job for each

diagnostic data file being sent. Thus, if an incident has a dump data set and three log snapshot files, four FTP jobs are created (and the FTP Job Status table will have four entries). To debug the FTP jobs, you need access to the job output. This is most often obtained by using SDSF to examine the spooled output from the job.

FTP job status codes and other information

The Incident Log allows you to display the status of the FTP jobs. On the *FTP Job Status* panel, 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* panel.

Chapter 7. Messages for z/OSMF

Messages play a major role in problem determination and error recovery. This topic describes the messages produced by z/OSMF.

z/OSMF displays messages from the product interface, from tasks performed by z/OSMF users, and from programs running on the z/OS host system.

Information about other messages

Information about other messages you might encounter while using z/OSMF is provided in the following documents:

- Messages for IBM WebSphere Application Server OEM Edition for z/OS are prefixed by `BBN`. See *IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide, Version 7.0* GA32-0631.
- 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.
- 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.

For information about other z/OS messages, use LookAt, the online facility that lets you look up message explanations and some system abends and codes. You can access the message explanations directly from the LookAt Web site at http://www.ibm.com/eserver/zseries/zos/bkserv/lookat/.

IZUG100E Unable to register provider *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.

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 issuing the `cimserver -s` command. Then, re-run the script.

User response: No action is required.

IZUG104I Provider *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.

System programmer response: No action is required.

User response: No action is required.

IZUG105W Provider *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.

System programmer response: No action is required.

User response: No action is required.

IZUG106I **The provider** *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.

System programmer response: No action is required.

User response: No action is required.

IZUG107E **Unable to register provider** *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.

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.

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.

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 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.

System programmer response: Issue 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** *minimum-maximum* **characters.**

Explanation: The value specified for the variable is not valid.

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** *reason-code***.**

Explanation: The specified script returned with the specified 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** *command-output*

Explanation: The output of the command that was passed to the specified script is displayed.

System programmer response: No action is required.

User response: No action is required.

IZUG114I **Command** *command* **was passed to script** *script-name***.**

Explanation: The specified command was passed to the specified 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.

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-id* does not exist.**

Explanation: The specified user does not exist.

System programmer response: Provide a valid user name and try your request again.

User response: No action is required.

IZUG117I **A *create-or-delete* 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.

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.

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.

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.

System programmer response: Review the specified report.

User response: No action is required.

IZUG122E **Verification failed for *verification-item*.**

Explanation: Verification failed because an error occurred while the specified item was 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.

System programmer response: No action is required.

User response: No action is required.

IZUG126E **An error occurred. Variable *variable-name* is set to value *value-1*. The expected value is *value-2*.**

Explanation: The specified variable is set to the specified value (*value-1*). The variable must be set to the expected value (*value-2*).

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-id* not connected to group *group-name*.**

Explanation: The specified user is not connected to the specified 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-id* not permitted to RACF class *class-name*.**

Explanation: The specified user or group name is not permitted to the specified 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.

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 WebSphere Application 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 WebSphere Application Server, or press enter to accept the default *cluster-transition-name*:**

Explanation: Indicate the cluster transition name to be used.

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.

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 *directory-file directory-file-name* was created.**

Explanation: The specified file or directory has been created.

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.

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.

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** *cim-setup-option-value***:**

Explanation: The message prompts to determine if the Common Information Model (CIM) server has been setup. A default value is provided.

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** *default-data-directory* **as the data directory.**

Explanation: The message indicates that no data directory was specified and that the default data directory will be used.

System programmer response: Ensure the default data directory use is correct to the configuration.

User response: No action is required.

IZUG142I **Enter the target parmlib data set in which the IBM-supplied** *ceaprm-parmlib-member* **and** *ieadmc-parmlib-member* **are to be saved, or press enter to accept the default** *parmlib-name***:**

Explanation: The message prompts for the parmlib data set where the CEAPRM and IEADMC members are to be saved. A default is provided.

System programmer response: Enter the parmlib name to store the updated parmlib members, or accept the default.

User response: No action is required.

IZUG143I **Enter the target parmlib data set in which the IBM-supplied** *ceaprm-parmlib-member* **and** *ieadmc-parmlib-member* **are to be saved, or press enter to use SYS1.PARMLIB:**

Explanation: The message prompts for the parmlib data set where the CEAPRM and IEADMC members are to be saved.

System programmer response: Enter the parmlib name to store the updated parmlib members, or accept the default.

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** *data-filesystem-directory***:**

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.

IZUG146I **Invoking script** *script-name-options***.**

Explanation: The message displays 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.

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.

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.

IZUG152I Enter the directory path and name of the WebSphere Application Server configuration file:

Explanation: This message prompts for the name and location of the WebSphere Application Server configuration file.

System programmer response: Enter the directory path and name of the WebSphere Application Server configuration file.

User response: No action is required.

IZUG153I Enter the directory path and name of the WebSphere Application Server configuration file, or press enter to accept *configuration-file***:**

Explanation: This message prompts for the name and location of the WebSphere Application Server configuration file. A default value is provided.

System programmer response: Enter the directory path and name of the WebSphere Application Server configuration file.

User response: No action is required.

IZUG154I The WebSphere Application Server configuration values have been read.

Explanation: This message indicates that the required configuration values were retrieved from the WebSphere Application Server configuration file.

System programmer response: No action is required.

User response: No action is required.

IZUG155E The WebSphere Application Server configuration file *configuration-file* **does not exist. Enter ″1″ to specify the WebSphere Application Server values, or press enter to respecify the file:**

Explanation: This message indicates that the specified configuration file was not found. Enter ″1″ to configure the WebSphere Application Server values. Prompts will be displayed for you to enter the configuration properties. If you enter any other value you will be prompted for the WebSphere Application Server configuration file.

System programmer response: Enter ″1″ to display prompts for the configuration properties. Enter any other value to respecify the directory path and name of the WebSphere Application Server configuration file.

User response: No action is required.

IZUG156E The WebSphere Application Server configuration file *configuration-file* **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.

System programmer response: Ensure that the specified property exists in the specified configuration file.

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.

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. If you enter an asterisk (*), it indicates that you want the z/OS storage management subsystem (SMS) to manage the storage. A default value is provided.

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.

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.

System programmer response: Provide a fully-qualified path.

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.

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 action failed for the specified user with the specified return code.

System programmer response: For more information, review the log file created for the error.

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.

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.

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.

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.

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 exit.

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.

System programmer response: Issue 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 supported input options for the specified script are displayed. For more information about the script or the input options, see *IBM z/OS Management Facility User's Guide*, SA38-0652, in the IBM z/OS Internet Library.

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.

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.

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.

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.

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.

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.

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.

System programmer response: Reissue 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 reissue 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.

System programmer response: Verify that the correct argument is being used. Ensure that it is spelled correctly. Correct any errors and reissue the command.

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: Issue 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.

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.

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.

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.

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.

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.

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.

System programmer response: No action is required.

User response: No action is required.

IZUG228I **Enter the name of the z/OSMF** *z/OSMF-file-system-type* **file system:**

Explanation: Indicate the name you want to be used for the file system.

System programmer response: Enter the name of the file system.

User response: No action is required.

IZUG229I **Enter the name of the z/OSMF** *z/OSMF-file-system-type* **file system or press enter to accept the default** *z/OSMF file-system-type* **file system name** *value***:**

Explanation: Indicate the name you want to use for the file system. A default is provided.

System programmer response: To use the default file system name, press enter without entering a value. Otherwise, enter the name of the file system.

User response: No action is required.

IZUG230E **The value** *value* **is incorrect.**

Explanation: The specified value is incorrect.

System programmer response: Correct the value.

User response: No action is required.

IZUG231W **A file system with the name** *file-system-name* **already exist. Do you want to use the existing file system as the z/OSMF** *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.

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** *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.

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.

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** *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.

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.

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.

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.

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 **Filename** *file-name* **already exists: Overwrite (Y|N)?**

Explanation: The specified file name already exists. The message prompts the user to overwrite it.

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.

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.

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.

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.

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.

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 value provided for the size of the volume is less than 10 cylinders.

System programmer response: Provide a volume that is greater than 10 cylinders in size.

User response: No action is required.

IZUG250I **The allocation size for the z/OSMF data file system** *file-system-name* **with primary/secondary cylinder allocation** *primary-secondary* **is** *cylinder-size***.**

Explanation: The specified file system was allocated the specified number of cylinders for the primary or secondary extent.

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.

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.

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.

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.

System programmer response: Make sure 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.

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** *attribute-name-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.

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.

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.

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.

System programmer response: Specify the value within the correct range or size.

User response: No action is required.

IZUG262I **Enter the WebSphere Application Server** *attribute-name***:**

Explanation: The message prompts for the name of the application server attributes.

System programmer response: Enter the application server attribute name.

User response: No action is required.

IZUG263I **Enter the WebSphere Application Server** *attribute-name***, or press enter to accept the default** *attribute-name-value***:**

Explanation: The message prompts for the application server attributes. A default value is provided.

System programmer response: Enter the requested information, or accept the default.

User response: No action is required.

IZUG264E *attribute-name* **must be alphanumeric and must be** *attribute-size* **characters.**

Explanation: The value provided for the application server is incorrect or outside the expected range or size for that attribute.

System programmer response: Specify with the correct range or size.

User response: No action is required.

IZUG265I **Enter the root directory path of the WebSphere Application Server:**

Explanation: The message prompts for the root directory path for the application server.

System programmer response: Enter the root directory.

User response: No action is required.

IZUG266I **Enter the root directory path of the WebSphere Application Server, or press enter to accept the default** *application-server-directory***:**

Explanation: The message prompts for the root directory path for the application server. Default value is provided.

System programmer response: Enter the root directory or accept the default.

User response: No action is required.

IZUG267I **Enter the SAF profile prefix (case sensitive) for the WebSphere Application Server:**

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 the WebSphere Application Server, or press enter to accept the default** *saf-profile***:**

Explanation: The message prompts for the SAF profile prefix. A default value is provided.

System programmer response: Enter the SAF profile prefix, or accept the default.

User response: No action is required.

IZUG269I **Enter the path of the root WBEM directory:**

Explanation: The message prompts for the path for Common Information Model (CIM) or WBEM root directory.

System programmer response: Enter the path of the root WBEM directory.

User response: No action is required.

IZUG270I **Enter the path of the root WBEM directory, or press enter to accept the default** *wbem-root***:**

Explanation: The message prompts for the path for Common Information Model (CIM) or WBEM root directory. A default value is provided.

System programmer response: Enter the path for Common Information Model (CIM) or WBEM root directory, or accept the default.

User response: No action is required.

IZUG271I **Do you want to configure the Incident Log task? For yes, enter Y. For no, enter N:**

Explanation: The message prompts to determine if the Incident Log 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 configure the Incident Log task? For yes, enter Y. For no, enter N. Or press enter to accept the default** *value***:**

Explanation: The message prompts to determine if the Incident Log 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 the GUI; 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, 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.

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.

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.

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. Default is provided.

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.

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* numeric characters.**

Explanation: The value specified for the branch or country code does not conform to guidelines.

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.

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 source parmlib data set in which the parmlib member CEAPRM00 is located, or press enter to accept the default *parmlib-name*:**

Explanation: The message prompts for the parmlib data set where the CEAPRM00 member is located. A default is provided.

System programmer response: Enter the parmlib name, or accept the default.

User response: No action is required.

IZUG285I **Enter the source parmlib data set in which the parmlib member CEAPRM00 is located, or press enter to use SYS1.PARMLIB:**

Explanation: The message prompts for the parmlib data set where the CEAPRM00 member is located.

System programmer response: Enter the name of the parmlib data set, or accept the default.

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.

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.

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.

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.

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.

System programmer response: Review log file for details.

User response: No action is required.

IZUG296I Verification process *ivp-name* has completed.

Explanation: The specified verification process has completed.

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).

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).

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).

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.

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.

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.

System programmer response: No action is required.

User response: No action is required.

IZUG303I **Environment name and value being used are** *en-var***.**

Explanation: The name and value for an environment setting is provided.

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.

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 named script failed. Reason codes and meaning for **izuadmin.sh** are as follows:

- 1 Usage error.
- 2 Problem with log directory.
- 3 Error writing to log file.
- 4 Problem related to environment variable.
- 5 Error with an environment file setting.
- 6 Verification failed.
- 7 Incorrect z/OS Version for z/OSMF.

Reason codes and meaning for **izuprime.sh** are as follows:

- 1 Usage error.
- 2 Problem with log directory.
- 3 Error writing to log file.
- 4 Error running command.
- 5 A repository already exists.
- 6 User ID does not exist.

System programmer response: Check the log file for messages that describe the error. After correcting the error, run the script again.

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.

System programmer response: No action is required.

User response: No action is required.

IZUG307I **The script wsadmin.sh is being called to invoke script** *script***.**

Explanation: The message indicates that wsadmin.sh is being called to invoke an administration script in the wsadmin environment.

System programmer response: No action is required.

User response: No action is required.

IZUG308I **Processing of script** *script-name* **has completed at** *date-and-time***.**

Explanation: This message indicates that processing has completed for the script without errors. The script name, data, and time are provided.

System programmer response: No action is required.

User response: No action is required.

IZUG309I **The wsadmin.sh environment is being established.**

Explanation: The wsadmin.sh environment is being set up.

System programmer response: No action is required.

User response: No action is required.

IZUG311E **IZU_APPSERVER_ROOT** *application-server-root-directory* **is not valid: exiting script.**

Explanation: The application server root directory is not valid. The processing for the script stops.

System programmer response: Set IZU_APPSERVER_ROOT to the valid application server 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.

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.

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:** *en-var***.**

Explanation: A problem exists with a setting in the environment file. Context of the error is provided.

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 **IZU_WBEM_ROOT** *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.

System programmer response: Set IZU_WBEM_ROOT to the valid Common Information Model (CIM) server WBEM root directory and run 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.

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.

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.

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* **supported by z/OSMF.**

Explanation: z/OSMF cannot be launched when it is installed on a system that is running a z/OS level that is earlier than the minimum supported z/OS level.

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/OS level** *installed-z/OS-level* **is later than the maximum supported z/OS level** *maximum-z/OS-level***.**

Explanation: z/OSMF is installed on a system that is running a z/OS level that is later than the maximum z/OS level supported by z/OSMF.

System programmer response: Upgrade to a z/OSMF that supports the z/OS level installed on the host system.

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.

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.

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.

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.

System programmer response: No action is required.

User response: No action is required.

IZUG345I **Application** *application-name* **is being removed.**

Explanation: The specified application is being removed from the application server.

System programmer response: No action is required.

User response: No action is required.

IZUG346I **Application** *application-name* **from location** *file-location* **is being installed.**

Explanation: The application is being installed to the application server from the specified location.

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.

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 application server is being updated to the specified value.

System programmer response: No action is required.

User response: No action is required.

IZUG358E **Server** *application-server-name* **does not exist.**

Explanation: The specified application server does not exist.

System programmer response: Specify a valid application server and run again.

User response: No action is required.

IZUG360I **Process** *process-name* **environment entry property** *property-name* **that has a value of** *value* **is being deleted.**

Explanation: The specified property for the named process is being removed.

System programmer response: No action is required.

User response: No action is required.

IZUG361I **Process** *process-name* **environment entry property** *property-name* **that has a value of** *value* **is being created.**

Explanation: The specified property for the named process is being added.

System programmer response: No action is required.

User response: No action is required.

IZUG362I **An application server class loader is being created.**

Explanation: An application server class loader is being created. Shared libraries referenced by this class loader are visible to all applications in the application server.

System programmer response: No action is required.

User response: No action is required.

IZUG363I **Reference to shared library** *shared-library-name* **with scope** *scope* **is being deleted.**

Explanation: The specified shared library reference is being removed.

System programmer response: No action is required.

User response: No action is required.

IZUG365I **Process** *process-name* **with start command arguments is being updated to include value** *value-1*. **New value of the arguments is** *value-2*.

Explanation: The specified argument is being added to the start command arguments for the specified process.

System programmer response: No action is required.

User response: No action is required.

IZUG366I **Tuning parameter** *parameter-name* **is being updated with value** *parameter-value*.

Explanation: The tuning parameter in the application server is being updated with the specified value.

System programmer response: No action is required.

User response: No action is required.

IZUG367I **Log detail level settings are being updated with value** *value*.

Explanation: The log detail level settings are being updated with the specified value.

System programmer response: No action is required.

User response: No action is required.

IZUG368I **Process** *process-name* **environment entry property** *property-name* **is being updated with value** *value*.

Explanation: The specified property for the specified process is being updated.

System programmer response: No action is required.

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.

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.

System programmer response: No action is required.

User response: No action is required.

IZUG372E **Command** *command* **returned an error. Command return code is** *return-code*.

Explanation: An error was received from a command invocation.

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* **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.

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.

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** *verification-item***.**

Explanation: Verification has completed for the specified item.

System programmer response: No action is required.

User response: No action is required.

IZUG376E **Verification failed for** *verification-item* **because of the following reason:** *reason*

Explanation: Verification failed for the item because of the specified reason. Context of the error is provided.

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.

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.

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.

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.

System programmer response: For more information, review 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.

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.

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.

System programmer response: No action is required.

User response: No action is required.

IZUG400I **z/OSMF core functions have been initialized.**

Explanation: z/OSMF core functions have been initialized.

System programmer response: No action is required.

User response: No action is required.

IZUG402W **You are about to close the tab for task** *task-name***. Any changes you made since you last clicked OK or Apply will be discarded. Do you want to continue?**

Explanation: Confirm whether to cancel your request. If you continue, the changes you entered will be discarded.

System programmer response: No action is required.

User response: Click **OK** to close the tab. All progress

information and any data you might have entered will be lost. Click **Cancel** to leave the tab open and retain all progress information and data.

IZUG410E The user ID, password, or pass phrase is not valid. Enter the correct values for your security management product.

Explanation: Typically, this error occurs when the combination of the user ID and password or pass phrase is not valid for the z/OS security product at your installation. It can also occur when the user does not have read access to the WebSphere SAF profile prefix profile in the APPL class.

System programmer response: Grant the user read access to the WebSphere SAF profile prefix profile in the APPL class. The IBM-supplied RACF command template does not allow users to access the profile.

User response: Enter a valid user ID and password or pass phrase (A-Z, a-z, 0-9, #, $, and @). If the problem persists, contact your z/OSMF administrator or system programmer.

IZUG414W An error occurred during the log out of user *user-id*.

Explanation: An error has occurred on the server when attempting to log out the user.

System programmer response: Examine the WebSphere Application Server logs for more information about why the user had trouble logging out. If the problem persists, contact the IBM Support Center.

User response: No action is required.

IZUG415E The user ID, password, or pass phrase are required fields. Enter the correct values for your security management product.

Explanation: A valid user ID and password or pass phrase are required. The fields cannot be blank.

System programmer response: No action is required.

User response: Enter a valid user ID and password or pass phrase.

IZUG416E Password or pass phrase is a required field. Enter a valid value.

Explanation: A valid password or pass phrase is required. The field cannot be blank.

System programmer response: No action is required.

User response: Enter a valid password or pass phrase.

IZUG417E An error occurred when retrieving navigation area content.

Explanation: This general error message occurs when one or more errors are encountered during the creation of the navigation area. Any detailed error messages will be logged on the server.

System programmer response: Examine the z/OSMF and WebSphere Application Server logs to determine if any previously reported failures have occurred. If the previous messages do not help explain the cause of the problem, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG418E The language resource bundle *bundle-link* cannot be retrieved or the property for the task *task-name* does not exist.

Explanation: Either the link for the language resource bundle does not exist or the task name property is not found in the bundle file.

System programmer response: Examine the z/OSMF or WebSphere Application Server logs to determine if any previously reported failures have occurred. If the earlier messages do not help to explain the cause of the problem, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG419E An error occurred during the log in of user *user-id*: reason code: *rsn-code*

Explanation: An error occurred when attempting to log in the user. For reason code, one of the following values is provided:

- Reason code 1 means the LTPA token returned from the LoginContext was not a valid token.
- Reason code 2 means the LTPA token returned from the LoginContext was an expired token.

System programmer response: Examine the z/OSMF or WebSphere Application Server logs for more information about why the reported failures have occurred. If the previous messages do not help explain the cause of the problem, contact the IBM Support Center.

User response: Try again. If the problem persists, contact your administrator or system programmer.

IZUG421I One or more users *user-id* have been created.

Explanation: The request to create a new user has completed.

System programmer response: No action is required.

User response: No action is required.

IZUG422I **User *user-id* was deleted.**

Explanation: The request to delete one or more users has completed.

System programmer response: No action is required.

User response: No action is required.

IZUG427I **User *user-id* was modified.**

Explanation: The request to modify the properties for the user ID has completed.

System programmer response: No action is required.

User response: No action is required.

IZUG433I **Role *role* was created.**

Explanation: The request to create a new role has completed.

System programmer response: No action is required.

User response: No action is required.

IZUG435I **Role *role* was modified.**

Explanation: The request to modify the properties for the named role has completed.

System programmer response: No action is required.

User response: No action is required.

IZUG436E **The link location is not valid. A valid link location consists of 1-4096 ASCII characters.**

Explanation: The link location is not valid because it is missing, too long, or does not contain ASCII characters.

System programmer response: No action is required.

User response: Enter a valid link location.

IZUG437E **The link name is not valid. A valid link name consists of 1-25 characters.**

Explanation: The link name is not valid because it is missing or too long. A valid link name consists of 1-25 characters.

System programmer response: No action is required.

User response: Enter a valid link name.

IZUG438I **Link *link-name* was created.**

Explanation: The specified link was created.

System programmer response: No action is required.

User response: No action is required.

IZUG439E **Your changes to link *link-name* were not saved. Error: *error***

Explanation: An error occurred while attempting to save the link. Context of the error is provided.

System programmer response: This failure might be due to any of the following causes:

- Insufficient disk space
- Memory shortage
- z/OSMF setup
- Program error

Examine the logs to determine if any previously reported failures have occurred. If the previous messages do not help explain the cause of the problem, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG440W **You are about to cancel the operation. Your changes will be discarded. Do you want to continue?**

Explanation: Confirm whether to cancel your current operation. If you continue, the changes you entered will be discarded.

System programmer response: No action is required.

User response: Click **OK** to cancel the operation; otherwise, click **Cancel** to continue.

IZUG441W **You are about to delete one or more links. Do you want to continue?**

Explanation: Confirm whether you want to delete one or more of the links.

System programmer response: No action is required.

User response: Click **OK** to delete the links; otherwise, click **Cancel**.

IZUG442I **One or more links *link-name* have been deleted.**

Explanation: One or more links have been deleted.

System programmer response: No action is required.

User response: No action is required.

IZUG443E The attempt to delete one or more links *link-name* failed. Error: *error*

Explanation: An error occurred while attempting to delete one or more named links. Context of the error is provided.

System programmer response: Causes for this failure might be any of the following:

- Link was already deleted by another user
- Insufficient disk space
- Memory shortage
- z/OSMF setup
- Program error

Examine the logs to determine if any previously reported failures have occurred. If the previous messages do not help explain the cause of the problem, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG444E Failed to delete one or more of the links *link-name*. Check the server log.

Explanation: An error occurred while attempting to delete one or more of the links. Some links were not deleted.

System programmer response: Causes for this failure might be any of the following:

- Link was already deleted by another user
- Insufficient disk space
- Memory shortage
- z/OSMF setup
- Program error

Examine the logs to determine if any previously reported failures have occurred. If the previous messages do not help explain the cause of the problem, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG445E Valid values have to be specified for all required fields.

Explanation: Not all required fields have valid values.

System programmer response: No action is required.

User response: Enter valid values for all required fields and click **OK**. If you click **Cancel**, any changes that you entered are not saved.

IZUG446I Link *link-name* was modified.

Explanation: The specified link was modified.

System programmer response: No action is required.

User response: No action is required.

IZUG560W No tasks are registered for the task group *task-group*.

Explanation: The named task group was not found in the task repository. Authorization data is not available.

System programmer response: Check the z/OSMF logs for warnings or failures. If a failure occurred, try reinstalling the task group. Also, check the runtime log for startup failures.

User response: Contact your z/OSMF administrator or system programmer.

IZUG565E The program attempted to register tasks out of sequence.

Explanation: Attempts to register tasks must be done between the start and end of a registration sequence, the boundaries of which are indicated by the appropriate context invocations.

System programmer response: Contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG566E The user *user-id* is not authorized to use task *task*.

Explanation: The user is not assigned to a role that is permitted to perform the named task. If user ID is "null," it indicates a guest user.

System programmer response: Determine whether the user requires this authorization, and if so, add the user to the appropriate role.

User response: Contact your z/OSMF administrator or system programmer to request authorization.

IZUG570W You are about to delete the selected users. Do you want to continue?

Explanation: When you select the Delete action, the selected users are removed from the z/OSMF Users table. This dialog box allows you to confirm whether you want to delete the selected users.

System programmer response: No action is required.

User response: Click **OK** to delete the selected users. You cannot undo this action. If you do not want to delete the selected users, click **Cancel**.

IZUG573E A user name must be at least one character, but not more than 40 characters.

Explanation: The user name is not valid because it is missing or too long. A valid user name consists of 1-40 characters.

System programmer response: No action is required.

User response: Enter a valid name from 1-40 characters.

IZUG575E Your changes to user *user-id* were not saved. Error: *error*

Explanation: An error occurred while attempting to save the user record. Context of the error is provided.

System programmer response: Causes for this failure might be any of the following:

- Insufficient disk space
- Memory shortage
- z/OSMF setup
- A program error.

Examine the z/OSMF logs to determine if any previously reported failures have occurred. If the earlier messages do not explain the cause of the problem, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG576E The attempt to delete user *user-id* failed. Error: *error*

Explanation: An error occurred while attempting to delete the user record. Context of the error is provided.

System programmer response: Causes for this failure might be any of the following:

- Insufficient disk space
- Memory shortage
- z/OSMF setup
- A program error.

Examine the logs to determine if any previously reported failures have occurred. For information about the logs, see "Working with z/OSMF runtime logs" on page 80. If the previous messages do not help explain the cause of the problem, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG577E The description must be at least one character, but not more than 100 characters.

Explanation: The description is not valid because it is missing or too long. A valid description consists of 1-100 characters.

System programmer response: No action is required.

User response: Enter a valid description from 1-100 characters.

IZUG579E Your changes to role *role* were not saved. Error: *error*

Explanation: An error occurred while attempting to save the named role record. Context of the error is provided.

System programmer response: Causes for this failure might be any of the following:

- Insufficient disk space
- Memory shortage
- z/OSMF setup
- A program error.

Examine the logs to determine if any previously reported failures have occurred. For information about the logs, see "Working with z/OSMF runtime logs" on page 80. If the previous messages do not help explain the cause of the problem, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG620E The required environment variable *en-var* is missing or blank.

Explanation: A required environment variable was not detected or does not contain a valid value. This value is needed in order to continue processing, so the facility will not function properly until the issue is resolved. A blank value only contains white space characters.

System programmer response: Set the required environment entry for one or more of the servant processes, and restart the server.

User response: Contact your z/OSMF administrator or system programmer.

IZUG621I The data registry was started by class *class-name*.

Explanation: The data registry has been initialized for the named class.

System programmer response: No action is required.

User response: No action is required.

IZUG622I **The data registry class** *class-name* **was shut down.**

Explanation: This message is usually issued to the log during normal shutdown for the named data registry class.

System programmer response: No action is required.

User response: No action is required.

IZUG623W **Class** *class-name-1* **attempted to start as the data registry, but class** *class-name-2* **is already performing this function.**

Explanation: While the data registry was already active, an attempt to start another instance of a data registry was made; only one data registry can be active.

System programmer response: Contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG624E **An attempt to use the data registry failed because it is not started.**

Explanation: An exploiter of the data registry attempted to obtain or write data, but it is not currently available.

System programmer response: Ensure that the navigation services module is present in the enterprise application. Check the logs to ensure that the startup of the navigation services module has completed.

User response: Contact your z/OSMF administrator or system programmer.

IZUG625E **An internal error occurred while attempting to serialize file** *file-path***.**

Explanation: The utilities used to write the named file failed because of unexpected causes.

System programmer response: Examine the logs for the attached exceptions to ensure that all of the proper permissions are in effect and that adequate space is available in the file system. For information about the logs, see "Working with z/OSMF runtime logs" on page 80.

User response: Contact your z/OSMF administrator or system programmer.

IZUG626E **An internal error occurred while attempting to read file** *file-path***.**

Explanation: The utilities used to read the file failed because of unexpected causes.

System programmer response: Examine the logs for the attached exceptions to ensure that all of the proper permissions are in effect and that adequate space is available in the file system.

User response: Contact your z/OSMF administrator or system programmer.

IZUG627W **Data registry processing encountered an ownership or permission mismatch for the file or directory** *file-path***. Directory owner** *dir-name-1* **with permissions** *perms-1* **was expected, but directory owner** *dir-name-2* **with permissions** *perms-2* **was found.**

Explanation: The named file does not have the expected owner and permission settings.

System programmer response: Correct the ownership, file permissions, or both to protect data.

User response: Contact your z/OSMF administrator or system programmer.

IZUG628E **Class** *class-name* **attempted to reserve a name space with task group name** *task-group-name* **and user name** *user-id***, but this object is already reserved.**

Explanation: A function made a claim to task group data, but another function has previously claimed the data.

System programmer response: Ensure that Web modules are not installed twice. If the problem persists, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG629E **The specified root directory** *root-directory* **in variable** *en-var* **does not exist or cannot be accessed.**

Explanation: The name of the directory is specified by an environment variable. The name and value of the variable are logged when the system is unable to use the named directory.

System programmer response: Ensure the variable is pointing to the correct location. Ensure that this location exists and that WebSphere Application Server can write to it.

User response: Contact your z/OSMF administrator or system programmer.

IZUG633E **An error occurred while attempting to create directory** *directory-path***.**

Explanation: The specified directory was not found but was needed in order to store the directory data. The facility attempted to create the directory but a failure occurred.

System programmer response: Ensure that the parent directories have the appropriate ownership and permissions set. Also, ensure that there is adequate storage space in order to create and populate the new directory. Finally, ensure that the parent directory of the specified directory-path has write authority for its owner.

User response: Contact your z/OSMF administrator or system programmer.

IZUG634E **Path** *path-name* **exists, but it is not a directory.**

Explanation: The specified path is expected to be a directory, but was found to be another type of object, such as a file or symbolic link that points to a nonexistent location.

System programmer response: Ensure that the path name is a directory.

User response: Contact your z/OSMF administrator or system programmer.

IZUG635E **Path** *path-name* **exists, but it is read only.**

Explanation: The specified path must be in read/write mode in order to be used for storing data.

System programmer response: Modify the permissions, ownership, or both of the path as needed.

User response: Contact your z/OSMF administrator or system programmer.

IZUG636E **An error occurred while attempting to parse file** *file-path***. The file might be corrupted.**

Explanation: The data in the specified file failed to be read because of an incorrect internal format. Errors can occur if the file is incompletely written to disk or if a file is manually edited and corrupted as a result.

System programmer response: Ensure that the file system has not run out of space, which can cause files to be incompletely written. If necessary, expand the amount of storage; otherwise, determine whether a superuser has manually changed the data.

User response: Contact your z/OSMF administrator or system programmer.

IZUG638E **An error occurred while attempting to create or initialize the file** *file-path***.**

Explanation: The facility encountered an internal error while attempting to create the named file, or initialize the file. This error can occur if there are problems with the file system during startup or when a specific set of properties are first accessed.

System programmer response: Examine the logs, and correct the problem described. Ensure that there is adequate storage to create the file.

User response: Contact your z/OSMF administrator or system programmer.

IZUG639W **File** *file-path* **uses the newer version** *version-1* **while the current version is** *version-2***.**

Explanation: The version found in the file is newer than the version of the currently running facility. The currently running version might not support functions that are available in the newer version of the product.

System programmer response: Consider applying the latest service to z/OSMF.

User response: Contact your z/OSMF administrator or system programmer.

IZUG640I **File** *file-path* **uses the older version** *version-1* **while the current version is** *version-2***. The data format will be upgraded to the current version.**

Explanation: The version found in the file is older than the version of the currently running facility. This normally happens when z/OSMF is upgraded; you can ignore this message if you have applied the latest service to z/OSMF.

System programmer response: If found during the processing of an upgrade, you do not need to take any action; otherwise, ensure that the data directory is correct and that it has not reverted to an older level of data.

User response: Contact your z/OSMF administrator or system programmer.

IZUG641E **The following z/OSMF internal facility is not started:** *class-name***. Check the log file for initialization failures.**

Explanation: Certain facilities of the application are started dynamically during initialization. If a problem occurred during initialization, one or more of these shared instances might be missing when called. This message might indicate that another problem has been encountered earlier.

System programmer response: Check earlier in the logs for other failures that might have occurred, and correct the problem.

User response: Contact your z/OSMF administrator or system programmer.

IZUG642W An internal error occurred while attempting to open the z/OSMF log file.

Explanation: The z/OSMF log facilities failed to create or open the file where log records could be written. Messages will be redirected to the WebSphere Application Server servant logs.

System programmer response: Examine the logs for additional information. Ensure that the location for the logs has the appropriate ownership and permissions. Also, ensure that there is adequate storage space.

User response: Contact your z/OSMF administrator or system programmer.

IZUG643E Class *class-name-1* attempted to provide the services of the base class *base-class*, but class *class-name-2* is already performing this function.

Explanation: A dynamically-allocated class was created, but the reference to the instance is already occupied by another instance. These instances could be of the same or different types, but only one is permitted to be active at any given time within the same class loader.

System programmer response: Examine both the z/OSMF and Websphere application server logs to determine if a failure occurred during the shutdown of a Web module that might prevent cleanup of an instance. If this is the case, restart WebSphere Application Server.

User response: Contact your z/OSMF administrator or system programmer.

IZUG645W The directory *log-directory* to be used for logs is not accessible, not a directory, or read only.

Explanation: The directory where logs are written was found to be incorrectly configured. Messages will be redirected to the WebSphere servant logs.

System programmer response: Ensure that the specified location exists. Also, ensure that the appropriate permissions and ownership are set. Finally, ensure that the path is a directory and not some other type like a file.

User response: Contact your z/OSMF administrator or system programmer.

IZUG646E An error occurred while attempting to create the data registry.

Explanation: The facility could not be started because of an unrecoverable error that occurred during initialization. This message indicates that a failure occurred earlier.

System programmer response: Check the logs for information regarding the earlier failure that disrupted startup.

User response: Contact your z/OSMF administrator or system programmer.

IZUG660W No tasks for task group *task-group* are registered.

Explanation: The specified task group does not have any tasks registered.

System programmer response: No action is required.

User response: No action is required.

IZUG664W An operation requiring an authenticated user was attempted, but the current context indicates a guest user.

Explanation: Certain operations are not valid or permitted to guests. If such an operation is attempted while the current context indicates a guest, the operation fails with this message.

System programmer response: No action is required.

User response: This error occurs when an unauthenticated browser session attempts to access content that requires an authenticated user. Ensure that you have the proper permissions to access z/OSMF, or see your z/OSMF administrator.

IZUG669E Task registration failed. Task *task-name* is already registered for task group *task-group-name*.

Explanation: The tasks cannot be registered because tasks with the same IDs are already registered for other task groups.

System programmer response: Contact the IBM Support Center.

User response: No action is required.

IZUG670E User *user-id* already exists.

Explanation: An attempt to create a new user failed because a user with the same user ID already exists. The user ID must be unique.

System programmer response: No action is required.

User response: Specify a unique user ID that does not already exist.

IZUG671E User *user-id* does not exist. The request could not be completed.

Explanation: The request failed because the requested user is not defined to z/OSMF. The user might have been removed by another z/OSMF administrator.

System programmer response: No action is required.

User response: Click **Refresh** to update the z/OSMF Users table.

IZUG672E **User *user-id* cannot be removed because it is the last user with the role z/OSMF Administrator.**

Explanation: At least one user must be defined to z/OSMF in the assigned role of z/OSMF Administrator to ensure that a user can perform the administration tasks for z/OSMF. The user was not removed because it is the last user assigned to this role.

System programmer response: No action is required.

User response: If you need to understand more about the assigned role of the user, see your z/OSMF administrator.

IZUG673E **User *user-id* cannot be switched to another role because it is the last user with the role z/OSMF Administrator.**

Explanation: At least one user must be defined to z/OSMF in the assigned role of z/OSMF Administrator to ensure that a user can perform the administration tasks for z/OSMF. The user was not switched to another role because it is the last user assigned to this role.

System programmer response: No action is required.

User response: If you need to understand more about the assigned role of the user, see your z/OSMF administrator.

IZUG674E **Role *role* already exists.**

Explanation: Your attempt to create a new role failed because a role with that name already exists. Each role name must be unique.

System programmer response: No action is required.

User response: Enter a unique role name that does not already exist.

IZUG675E **Role *role* was not found.**

Explanation: Your request failed because the requested role is not defined to z/OSMF. The role might have been removed by another z/OSMF administrator.

System programmer response: No action is required.

User response: Click **Refresh** to update the roles table.

IZUG676E **Link *link* already exists.**

Explanation: The attempt to create a new link failed because a link with that name already exists. The name of all links must be unique.

System programmer response: No action is required.

User response: Enter a unique link name that does not already exist.

IZUG677E **Link *link* was not found.**

Explanation: Your request failed because the requested link is not defined to z/OSMF. The link might have been removed by another z/OSMF administrator.

System programmer response: No action is required.

User response: Click **Refresh** to update the link table.

IZUG678E **Link *link* was not saved. The specified link name is reserved.**

Explanation: The link cannot be saved because the specified link name is already in use.

System programmer response: No action is required.

User response: Specify another link name.

IZUG680E **A z/OSMF instance using the z/OSMF data file system *data-file-system-name* is already running in the sysplex.**

Explanation: A z/OSMF data file system can only be used by one z/OSMF instance at a time. A z/OSMF instance that has locked the z/OSMF data file system is already running in the sysplex.

System programmer response: To start z/OSMF with the specified z/OSMF data file system, stop the z/OSMF instance currently using the data file system. If the z/OSMF instance is not running, the lock (global resource serialization ENQ) for the z/OSMF data file system might not have been released when z/OSMF was stopped. If so, stop IBM WebSphere Application Server OEM Edition for z/OS to release the lock, and start z/OSMF.

User response: Contact your z/OSMF administrator or system programmer.

IZUG681E **The request to release the lock for the z/OSMF data file system *data-file-system-name* failed with reason code *reason-code*.**

Explanation: An error occurred releasing the lock (global resource serialization ENQ) for the specified z/OSMF data file system. The global resource serialization ENQ service failed with the indicated reason code. For more information, see *z/OS MVS Programming: Assembler Services Reference, Volume 2 (IARR2V-XCTLX))* in the IBM z/OS Internet Library. You might not be able to restart z/OSMF with that z/OSMF data file system.

System programmer response: Check the logs for more information about the failure. Check the status of z/OS global resource serialization (GRS) on your system. If a new start of z/OSMF fails with message

IZUG680E, stop and restart IBM WebSphere Application Server OEM Edition for z/OS to release the lock (global resource serialization ENQ). If the issue persists, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG682E The request to lock the z/OSMF data file system *data-file-system-name* **failed with reason code** *reason-code***.**

Explanation: An error occurred obtaining the lock (global resource serialization ENQ) for the specified z/OSMF data file system. The global resource serialization ENQ service failed with the indicated reason code. For more information, see *z/OS MVS Programming: Assembler Services Reference, Volume 2 (IARR2V-XCTLX))* in the IBM z/OS Internet Library.

System programmer response: Check the logs for more information about the failure. Check the status of z/OS global resource serialization (GRS) on your system. Restart IBM WebSphere Application Server OEM Edition for z/OS and restart z/OSMF. If the failure persists, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG683E The request to launch z/OSMF failed. The installed z/OS level *installed-z/OS-level* **is earlier than the minimum supported z/OS level** *minimum-z/OS-level***.**

Explanation: z/OSMF is not accessible because it is installed on a system that is running a z/OS level that is earlier than the minimum z/OS level supported by z/OSMF.

System programmer response: Upgrade to a z/OS level that is supported by z/OSMF.

User response: Contact your z/OSMF administrator or system programmer.

IZUG684W The installed z/OS level *installed-z/OS-level* **is later than the maximum supported z/OS level** *maximum-z/OS-level***.**

Explanation: z/OSMF is installed on a system that is running a z/OS level that is later than the maximum z/OS level supported by z/OSMF.

System programmer response: Upgrade to a z/OSMF that supports the z/OS level installed on the host system.

User response: No action is required.

IZUG685E Initialization of z/OSMF failed.

Explanation: The initialization of z/OSMF failed.

System programmer response: Verify that z/OSMF is configured properly. Check the z/OSMF logs for more details. For information about setting up z/OSMF, see Chapter 3, "Configuring z/OSMF," on page 25. For information about the logs, see "Working with z/OSMF runtime logs" on page 80. If the problem persists, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG686E An error occurred while priming the z/OSMF repository. Check the server log.

Explanation: The prime action failed. The error might be due to one of the following reasons:

1. The prime script did not run successfully.
2. The persistence file system failed to mount.

System programmer response: Examine the z/OSMF log or WebSphere Application Server log to determine if the prime script did not run successfully. If the script properly primed the necessary repository, make sure the persistence file system is mounted.

User response: No action is required.

IZUG700E An error occurred while attempting to load the native library.

Explanation: The required shared object could not be loaded. This can happen if the native library path is incorrect or missing or if the shared object has incorrect permission settings or incorrect format.

System programmer response: Contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG701E The native library version *version-1* **does not match the application library version** *version-2***.**

Explanation: The native library contains version information that does not match the version of the application library.

System programmer response: Ensure that your configuration and deploy scripts have run correctly; otherwise, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG702I **The native utility library with version *version* was loaded.**

Explanation: The native utility library was loaded with the reported version.

System programmer response: No action is required.

User response: No action is required.

IZUG703E **An error occurred while attempting to allocate memory. The attempted allocation size was *num-bytes*.**

Explanation: The application server is running out of memory. The native code could not allocate the requested amount of memory. The requested allocation size is provided in bytes.

System programmer response: Contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG704E **The file system encountered error *error* while reading or modifying path *path-name*.**

Explanation: An internal error has occurred; the values for *error* can be as follows:

- UNKNOWN_OWNER indicates that the requested owner name could not be converted to a numeric ID.
- UNKNOWN_GROUP indicates that the file group name could not be converted to a numeric ID.
- AEMODESWITCH_FAILURE indicates that the thread-level setting for ASCII/EBCDIC mode could not be saved, set, or restored.

System programmer response: Do the following:

- For UNKNOWN_OWNER, check the configuration for user names that might have been recently deleted.
- For UNKNOWN_GROUP, check the configuration for group names that might have been recently deleted.
- For AEMODESWITCH_FAILURE, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG705E **The errno value *errno* and errnojr value *errnojr* were returned by z/OS Language Environment while attempting to read or modify the properties of path *path-name*.**

Explanation: An unexpected response from the language environment method caused a failure when reading or modifying the owner or access permissions of a file. An *errno* and *errojr* value are provided by z/OS Language Environment®.

System programmer response: For information about the error codes, see *C/C++ Run-Time Library Reference*, SC41-5607, in the IBM z/OS Internet Library.

User response: Contact your z/OSMF administrator or system programmer.

IZUG707E **The attempt to submit JCL indicated an error with return code *return-code*, reason code *reason-code*, and errno value *errno*. The failing subroutine was *subroutine-name*. The first line of the submitted JCL was *line*.**

Explanation: An attempt to submit JCL directly to the internal reader failed. Return and reason codes are provided as well as the first line of the JCL that was submitted.

System programmer response: Ensure that the user has authority to submit JCL and that the internal reader is active. Also, ensure that the necessary system resources for submitting JCL are available. If the error persists, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG800W **Request was missing the required parameter *parm*.**

Explanation: The input to the request for a z/OSMF resource or service was incomplete or missing.

System programmer response: No action is required.

User response: Provide all required input for the request.

IZUG801W **Request included an incorrect value *value* for parameter *parm*.**

Explanation: An unsupported value was provided as a parameter to the request for a z/OSMF resource.

System programmer response: No action is required.

User response: Correct the input to the request.

IZUG802E **An error occurred. Error: *error***

Explanation: An error occurred processing the request. Context of the error is provided.

System programmer response: Examine the logs for more information about this failure. Verify the setup of z/OSMF.

User response: Contact your z/OSMF administrator or system programmer.

IZUG803E **The request failed because information is either missing or is not valid. Review the field level messages and make changes as needed.**

Explanation: When you click **OK** , any changes you made are saved and the panel or dialog box is closed. You cannot save any data that you entered on a panel or dialog box if required values are missing or if some of the specified values are not valid. The fields that contain errors have a red background and an image of a red circle with an X in the middle.

System programmer response: No action is required.

User response: Review the field-level messages, by clicking in the field or hovering over the image. Make changes as needed, then click **OK** . If you click **Cancel** , any changes that you entered will not be saved.

IZUG804E **Your Web browser is not enabled for JavaScript. To continue with z/OSMF, enable JavaScript in your browser settings and try again.**

Explanation: To work with z/OSMF, your browser must have JavaScript enabled.

System programmer response: No action is required.

User response: Change your browser settings to enable JavaScript. For the recommended browser settings for z/OSMF, see the topic on the environment checker tool in *IBM z/OS Management Facility Configuration Guide* , SA38-0652.

IZUG805E **Your Web browser is not enabled for cookies. To continue with z/OSMF, enable cookies in your browser settings and try again.**

Explanation: To work with z/OSMF, your browser must have cookies enabled for the z/OSMF site at your installation.

System programmer response: No action is required.

User response: Change your browser settings to enable cookies. For the recommended browser settings for z/OSMF, see the topic on the environment checker tool in *IBM z/OS Management Facility Configuration Guide* , SA38-0652.

IZUG806E **Your Web browser is not enabled for frames. To continue with z/OSMF, enable frames in your browser settings and try again.**

Explanation: To work with z/OSMF, your browser must have the frames option enabled.

System programmer response: No action is required.

User response: Change your browser settings to enable frames. For the recommended browser settings for z/OSMF, see the topic on the environment checker tool in *IBM z/OS Management Facility Configuration Guide* , SA38-0652.

IZUG807E **An error occurred while attempting to load a required program library. Error:** *error***.**

Explanation: A Dojo class failed to load. The context of the error is provided.

System programmer response: No action is required.

User response: Try loading the page again. If the problem persists, contact your z/OSMF administrator.

IZUG808W **Unsupported Web browser found:** *browser***. Some z/OSMF functions might not be available if you continue.**

Explanation: Your browser is not supported for use with z/OSMF. To access z/OSMF, your workstation requires a supported browser.

System programmer response: No action is required.

User response: Install a supported browser on your workstation and use it access z/OSMF. For the supported browsers, see the topic on the environment checker tool in *IBM z/OS Management Facility Configuration Guide* , SA38-0652.

IZUG809W **Unsupported Web browser version or level found:** *browser***. Some z/OSMF functions might not be available if you continue.**

Explanation: The version or level of your browser is not supported for use with z/OSMF. As a result, some z/OSMF functions might not be available if you continue.

System programmer response: No action is required.

User response: Install a supported level of this browser on your workstation and use it to access z/OSMF. For the supported browsers, see the topic on the environment checker tool in *IBM z/OS Management Facility Configuration Guide* , SA38-0652.

IZUG810W **To avoid a potential performance degradation, disable the Firebug add-on in your Web browser settings.**

Explanation: The Firebug add-on might cause a performance degradation. It is recommended that you disable this add-on when accessing z/OSMF.

System programmer response: No action is required.

User response: For optimal performance with z/OSMF, disable the Firebug add-on in your browser settings. For the recommended browser settings for

z/OSMF, see the topic on the environment checker tool in *IBM z/OS Management Facility Configuration Guide* , SA38-0652.

IZUG811W Unsupported operating system version found: *browser*. Some z/OSMF functions might not be available if you continue.

Explanation: The version of your workstation operating system is not supported for use with z/OSMF. As a result, some z/OSMF functions might not be available if you continue.

System programmer response: No action is required.

User response: Upgrade your workstation operating system to a supported version. For the supported versions, see the topic on the environment checker tool in *IBM z/OS Management Facility Configuration Guide* , SA38-0652.

IZUG850W The changes you made since you last clicked OK or Apply will be discarded. Do you want to continue?

Explanation: When you click Cancel, z/OSMF completes three actions:

- Discards your changes.
- Ends or cancels the action.
- Closes the panel or dialog box.

This dialog box allows you to confirm whether you want to cancel your request.

System programmer response: No action is required.

User response: To close the panel or dialog box and discard your changes, click OK. You cannot undo this action. To return to the panel or dialog box and keep your changes, click Cancel.

IZUG851E The user ID is not valid. Enter a valid user ID of one to eight alphanumeric characters.

Explanation: The user ID is not valid because it is missing, too long or contains incorrect characters. A valid user ID consists of one to eight characters (A-Z, a-z, 0-9, #, $, and @).

System programmer response: No action is required.

User response: Enter a valid user ID.

IZUG852I Archive manifest file at URL *url* was loaded with contents *data*.

Explanation: The archive manifest file has been loaded. An archive manifest file contains information about the product version and is present within a Java™ archive (.jar) file. For service purposes, the contents of the archive manifest file at the named location are logged in order to verify the level of the parts used in z/OSMF.

System programmer response: No action is required.

User response: No action is required.

IZUG853E Archive manifest file at URL *url-1* indicates a z/OSMF release of *release-1*, but archive manifest file at URL *url-2* indicates a z/OSMF release of *release-2*.

Explanation: z/OSMF releases are documented in the archive manifest file of each archive. An archive manifest file contains information about the product version and release and is present within a Java archive (.jar) file. The values are checked at startup to ensure that all the critical components are at the same level. This message indicates a mismatch with the locations and version or release IDs of the archive manifest files.

System programmer response: If you have recently upgraded or applied service, check the logs that were recorded by that operation for errors during the deployment. If this is a new installation, or the deployment logs do not offer further clues to the problem, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG854E An error occurred. The data could not be retrieved.

Explanation: An error occurred that prevented z/OSMF from retrieving the data; therefore, it cannot be displayed. This error could have occurred because either the system could not be reached or the Common Information Model (CIM) server is not running.

System programmer response: Check the z/OSMF logs to determine the status of the system and the CIM server. If the problem persists, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG855E An error occurred. Any settings that you have saved, such as column configurations, sorts, or filters, cannot be retrieved and new settings cannot be saved.

Explanation: z/OSMF cannot load your personal settings (such as column configurations, sorts, and filters). The panel is displayed using the default settings. You can modify the default settings; however, you cannot save your changes.

System programmer response: Check the z/OSMF logs for errors. Verify that the system is running and is configured properly. For more information, see the topic on configuring z/OSMF in *IBM z/OS Management*

Facility Configuration Guide , SA38-0652. If the problem persists, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUG856E Your Web browser session timed out. Because the server did not respond in the time allotted, z/OSMF cannot confirm that the request completed.

Explanation: z/OSMF is unable to confirm that the request completed because the server took too long to respond. Typically, this error occurs when the server is busy, when the server is not running, or when there is a network error.

System programmer response: Check the z/OSMF logs to determine the status of the server. Ensure that the server is running and check for system operations that are consuming a large amount of resources.

User response: Refresh the panel. If the request completed, typically, a message displays or the information displays on the panel. Try the request again. If the problem persists, contact your z/OSMF administrator or system programmer.

IZUG857E The requested URL could not be loaded. Status: *HTTP-status***.**

Explanation: The requested Uniform Resource Locator (URL) could not be loaded because of one of the following reasons:

- **403.** The server understood the request but is refusing to respond to it.
- **404.** The requested URL does not exist on the server.
- **500.** The server could not respond to the request because an error occurred.

System programmer response: Check the z/OSMF logs to determine the status of the server. Ensure that the server is running and that the user is authorized to access the URL.

User response: Complete the action that corresponds to the specified status. Do one of the following actions:

- **403.** Do not retry the request. Contact your z/OSMF administrator or system programmer.
- **404.** Verify that the URL is correct and then resubmit your request. If the error persists, contact your z/OSMF administrator or system programmer.
- **500.** Try your request again later. If the error persists, contact your z/OSMF administrator or system programmer.

IZUG858E Illegal Cross-Site-Request-Forgery (CSRF) HTTP request has been made; referrer is missing. Ensure that the request was issued from z/OSMF and not from direct access (that is, the address bar or bookmark).

Explanation: The Cross-Site-Request-Forgery (CSRF) checking failed because of one of the following reasons:

- The request was launched directly from a Web browser address bar or bookmark.
- The browser incorrectly formatted the request, omitting the **referer** attribute.

System programmer response: No action is required.

User response: Ensure that the request was issued from z/OSMF and from a supported Web browser. For a list of supported browsers, see the topic on the environment checker tool in *IBM z/OS Management Facility Configuration Guide* , SA38-0652.

IZUG859E Illegal Cross-Site-Request-Forgery (CSRF) HTTP request; host is missing.

Explanation: The Cross-Site-Request-Forgery (CSRF) checking failed because the host attribute was missing in the HTTP request.

System programmer response: No action is required.

User response: Ensure that the request was made from a supported Web browser. For a list of supported browsers, see the topic on the environment checker tool in *IBM z/OS Management Facility Configuration Guide* , SA38-0652.

IZUG860E Forgery (CSRF) HTTP request has been made: invalid referrer, referrer *ref_host***, request** *req_host***.**

Explanation: The Cross-Site-Request-Forgery (CSRF) checking failed because of because of a mismatch between the referrer host and request host.

System programmer response: No action is required.

User response: Ensure that the request was issued from z/OSMF.

IZUG861W *value* **Cross-Site-Request-Forgery (CSRF) attempts were detected since last reported.**

Explanation: The message provides the number of illegal Cross-Site-Request Forgery (CSRF) HTTP requests since last reported.

System programmer response: If a high number of illegal Cross-Site-Request Forgery (CSRF) HTTP requests has occurred, you might need to investigate the problem further to determine if the requests are simple user errors (that is, a user is attempting to directly access parts of z/OSMF) or if something more malicious is occurring.

User response: No action is required.

IZUG862W The changes you made will be discarded. Do you want to continue?

Explanation: You have made changes to the panel that have not been saved. This dialog box allows you to confirm whether you want to cancel your request.

System programmer response: No action is required.

User response: To close the panel or dialog box and discard your changes, click OK. You cannot undo this action. To return to the panel or dialog box and keep your changes, click Cancel.

IZUG863E All of the columns have been removed from the table. Reconfigure the columns and ensure that at least one column is displayed in the table.

Explanation: In the *Configure Columns* dialog box, all of the columns were removed from the Selected field; therefore, no columns are displayed in the table. Each table in z/OSMF must contain at least one column.

System programmer response: No action is required.

User response: In the *Configure Columns* dialog box, select at least one column to be displayed in the table.

IZUG910I An error occurred while attempting to access host *host-info* **as user** *user-id***. Request object was** *object-id***, and protocol was** *protocol***.**

Explanation: An error was encountered that could not be more specifically classified. Host and user information is provided including scheme and port as well as information about the request and the protocol. If user ID is "null," it indicates a guest user. Check for additional information in the z/OSMF or Websphere Application Server logs.

System programmer response: Check for the error-specific data that the message provides in the logs.

User response: Contact your z/OSMF administrator or system programmer.

IZUG911I Connection to *host-info* **cannot be established, or was lost and cannot be re-established using protocol** *protocol***.**

Explanation: The error occurs when a connection cannot be created to a system, host, or service, or a connection was dropped and could not be automatically recovered. Host and user information is provided including scheme and port as well as information about the request and the protocol. If user ID is "null," it indicates a guest user.

System programmer response: Ensure that the system or host destination is functioning properly.

User response: Contact your z/OSMF administrator or system programmer.

IZUG912I Access was denied for user *user-id* **for host** *host-info* **and object** *object-id***; protocol was** *protocol***.**

Explanation: A failure occurred either authenticating to the system, host, or service or trying to gain authorization to a specific system. Host and user information is provided including scheme and port as well as information about the request and the protocol. If user ID is "null," it indicates a guest user.

System programmer response: Ensure that the user has the appropriate authorization. If z/OS PassTickets are in use, ensure that they are properly configured.

User response: Request the appropriate authorization from your z/OSMF administrator or system programmer.

IZUG913I Object *object-id* **was requested by user** *user-id***. The request cannot be processed for host** *host-info***. The protocol was** *protocol***.**

Explanation: The system, host, or service could not process the request at this time. Host and user information is provided including scheme and port as well as information about the request and the protocol. If user ID is "null," it indicates a guest user.

System programmer response: Check the logs for additional information. Determine if the resource is in an incorrect state and correct the situation.

User response: Contact your z/OSMF administrator or system programmer.

IZUG914I Object *object-id* **was requested by user** *user-id***. The request is not valid for host** *host-info***. The protocol was** *protocol***.**

Explanation: The system, host, or service could not process the request because of an unsupported operation or parameter. Host and user information is provided including scheme and port as well as information about the request and the protocol. If user ID is "null," it indicates a guest user.

System programmer response: Ensure that the system, host, or service supports the request. Examine the logs for additional information.

User response: Contact your z/OSMF administrator or system programmer.

IZUG915I Object *object-id* **was requested by user** *user-id***. The object does not exist for host** *host-info***. The protocol was** *protocol***.**

Explanation: A request for properties or to invoke an

operation against a specific resource failed because the resource was not found. Host and user information is provided including scheme and port as well as information about the request and the protocol. If user ID is ″null,″ it indicates a guest user.

System programmer response: Check the logs for information about the resource, and correct the situation if appropriate.

User response: Contact your z/OSMF administrator or system programmer.

IZUG916I **Object** *object-id* **was requested by user** *user-id* **using protocol** *protocol* **for host** *host-info***, but the request has timed out.**

Explanation: A system or host destination did not respond in an appropriate amount of time. Host and user information is provided including scheme and port as well as information about the request and the protocol. If user ID is ″null,″ it indicates a guest user.

System programmer response: Check the z/OSMF logs to determine the status of the system or host destination and correct any problems.

User response: Contact your z/OSMF administrator or system programmer.

IZUG921I **The specified destination** *dest* **is not configured for protocol** *protocol***.**

Explanation: The system or host destination is not configured for the requested protocol.

System programmer response: Add or correct the protocol information for the destination.

User response: Contact your z/OSMF administrator or system programmer and have the protocol information added or corrected.

IZUG949W **An unknown exception was encountered during processing.**

Explanation: An exception was detected but could not be diagnosed appropriately.

System programmer response: Check the logs for information about the host or system concerning the failure. Otherwise, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUP162E **The problem number is not valid. Enter a valid problem number.**

Explanation: The problem number is not valid because it is either missing, too long, or contains incorrect characters. A valid problem number can be either an IBM problem management record (PMR) number, also known as an electronic technical response (ETR) number, or an independent software vendor (ISV) problem number. IBM PMR and ETR numbers contain 11 alphanumeric characters (A-Z, a-z, and 0–9) and two commas and have the format *nnnnn,bbb,ccc* where:

- *nnnnn* is the PMR or ETR number
- *bbb* is your branch office
- *ccc* is your country code

You can omit the branch and country code. When you refresh the *Incident Log* panel, z/OSMF displays the number with your installation's branch and country code appended.

ISV problem numbers can be any value that contains up to 20 characters including alphanumeric characters (A-Z, a-z, and 0–9), blanks, mathematical symbols (+ - = | ~ ( ) { } \), punctuation marks (? , . ! ; : ′ ″ / [ ]), and the following special characters: %, $, #, @, ^, *, and _.

The Problem number field cannot be blank in the *Send Diagnostic Data* wizard.

System programmer response: No action is required.

User response: Enter a valid problem number.

IZUP167E **The tracking ID is not valid. Enter a valid tracking ID.**

Explanation: The tracking ID is not valid because it is either too long or contains incorrect characters. A valid tracking ID can be any value that contains up to 20 characters including alphanumeric characters (A-Z, a-z, and 0–9), blanks, mathematical symbols (+ - = | ~ ( ) { } \), punctuation marks (? , . ! ; : ′ ″ / [ ]), and the following special characters: %, $, #, @, ^, *, and _.

System programmer response: No action is required.

User response: Enter a valid tracking ID.

IZUP198E **The SCHENV value is not valid. Enter a valid scheduling environment name.**

Explanation: The scheduling environment name is not valid because it is either too long or contains incorrect characters. A valid scheduling environment name contains up to 16 alphanumeric characters (A-Z, a-z, and 0–9) and the following special characters: @, $, #, and _. If you include an underscore (_) character in the name, you must imbed the underscore and enclose the name in single quotes. For example, 'PLEX_D01' is valid, but 'PLEX_' and PLEX_D01 are not valid. If you do not specify a scheduling environment, the job will not be associated with any Workload Manager (WLM) scheduling environment.

System programmer response: No action is required.

User response: Enter a valid scheduling environment name. You can obtain a list of the scheduling

environments defined for your installation by typing the SE command in System Display and Search Facility (SDSF) or by viewing the scheduling environments defined in the active WLM service policy.

IZUP199E **The CLASS value is not valid. Enter a class that contains one alphanumeric character (A-Z, a-z, and 0-9).**

Explanation: The class is not valid because it is either too long or contains incorrect characters. A valid class contains one alphanumeric character (A-Z, a-z, and 0–9). The class must be a valid class specified at JES initialization. If you do not specify a class, the default class specified at JES initialization is used.

System programmer response: No action is required.

User response: Enter a valid class.

IZUP200E **The MSGCLASS value is not valid. Enter an output class that contains one alphanumeric character (A-Z, a-z, and 0-9).**

Explanation: The output class is not valid because it is either too long or contains incorrect characters. A valid output class is identified by one alphanumeric character (A-Z, a-z, and 0–9). The class must be a valid output class specified at JES initialization. If you do not specify an output class, the default output class specified at JES initialization is used.

System programmer response: No action is required.

User response: Enter a valid output class.

IZUP601W **The number of incidents that match the date and time filter criteria exceeds the maximum number of displayable results. The log is incomplete because only** *maximum-number* **incidents are displayed.**

Explanation: The number of incidents that match the filter on the Date and Time column in the Incident Log table exceeds the maximum number of incidents that can be displayed in the log. The log is incomplete because only the specified maximum number of incidents are displayed. In this case, some of the incidents in which you are interested might not be shown in the log. For example, incidents that occurred at the beginning, middle, or end of the date and time range might not be displayed.

System action: z/OSMF closes the warning message when no more than the maximum number of incidents match the date and time filter.

System programmer response: No action is required.

User response: To ensure that you are working with a complete set of incidents, you can narrow the date and time filter criteria so that fewer incidents are retrieved or you can use the **Delete Incident** action to remove unneeded incidents from the log.

IZUP603E **An error occurred. Incidents cannot be retrieved from the sysplex dump directory.**

Explanation: Incidents cannot be retrieved from the sysplex dump directory because an error occurred.

System programmer response: Check the z/OS hardcopy log (for example, the syslog) for additional information.

User response: Try the request again. If the problem persists, contact your z/OSMF administrator or system programmer.

IZUP606E **The IBM PMR or ETR number** *PMR-ETR-number* **is missing the branch or country code. Enter a valid PMR or ETR number.**

Explanation: The specified IBM PMR or ETR number is not valid because the branch or country code is not included. You must enter the branch or country code because it is not defined in the CEAPRMxx parmlib member on the host system. IBM PMR and ETR numbers contain 11 alphanumeric characters (A-Z, a-z, and 0–9) and two commas and have the format *nnnnn*,*bbb*,*ccc* where:

- *nnnnn* is the PMR or ETR number
- *bbb* is your branch office
- *ccc* is your country code

System programmer response: To allow users to omit the branch and country code when entering the IBM PMR or ETR number, specify your installation's branch and country code in the CEAPRMxx parmlib member. For more information about setting up the CEAPRMxx parmlib member, see *z/OS MVS Initialization and Tuning Reference*, which is available online in the IBM z/OS Internet Library.

User response: Enter the 13 character PMR or ETR number.

IZUP608I **Incident** *incident-type* **created** *date-time* **was deleted.**

Explanation: The specified incident and all associated FTP status information and diagnostic data have been deleted.

System programmer response: No action is required.

User response: No action is required.

IZUP609I **Problem number set to** *problem-number* **for incident** *incident-type* **created** *date-time***.**

Explanation: The problem number indicated was set

for the specified incident. If the problem number is an IBM PMR or ETR number and you omitted the branch and country code, when you refresh the *Incident Log* panel, z/OSMF displays the number with your installation's branch and country code appended.

System programmer response: No action is required.

User response: If the number is an IBM PMR or ETR number and you omitted the branch and country code, refresh the *Incident Log* panel so that z/OSMF can display the number with your installation's branch and country code appended.

IZUP610I **Tracking identifier set to** *tracking-id* **for incident** *incident-type* **created** *date-time***.**

Explanation: The tracking ID indicated was set for the specified incident.

System programmer response: No action is required.

User response: No action is required.

IZUP615E **The request could not be completed. The diagnostic data** *data-type* **is currently being sent to the selected FTP destination.**

Explanation: The request failed because the specified diagnostic data is currently being sent to the selected FTP destination. While the send is in progress, you cannot re-send the diagnostic data to the FTP destination.

System programmer response: No action is required.

User response: On the *FTP Job Status* panel, view the status of the jobs for the selected diagnostic data. If you want to re-send diagnostic data that is associated with a job that is in progress, either wait for the job to complete or cancel the job before re-sending. You can also reselect the diagnostic data to send and omit the data that is currently being sent.

IZUP617I **z/OS will collect diagnostic data for the next occurrence of incident** *incident-type* **created** *date-time***.**

Explanation: The next time an SVC dump is requested for a problem with the same symptoms, the dump will be taken by the system and a new incident will be created.

System programmer response: No action is required.

User response: No action is required.

IZUP631E **The request could not be completed. The common event adapter (CEA) failed with reason code** *reason-code***. Reason:** *reason*

Explanation: The request could not be completed because CEA failed. The reason code and the reason might provide additional information about the failure. If the value for the reason code is *none* or if the value for the reason is blank (" "), CEA did not return the reason code or reason for the failure.

System programmer response: To obtain more details about the error, enable the Common Information Model (CIM) server tracing. For information about enabling CIM server tracing, see z/OS Common Information Model User's Guide.

To obtain additional information about the failure, you can also look up the reason code (if provided) in Table 21 on page 183. Contact the IBM Support Center and provide the CIM trace and this error information.

User response: Contact your z/OSMF administrator or system programmer.

IZUP633E **The request could not be completed. The incident does not exist.**

Explanation: The request failed because the incident associated with the selected diagnostic data could not be found. The incident might have been deleted by another user.

System programmer response: No action is required.

User response: Click **Refresh** to update the *Incident Log* panel.

IZUP634E **The request could not be completed. The common event adapter (CEA) address space is not running.**

Explanation: The request failed because the CEA address space is not running.

System programmer response: Start the CEA address space. To do so, issue the `S CEA` command from the operator console. To verify that CEA is active, issue the `D A,CEA` command from the operator console.

User response: Contact your z/OSMF administrator or system programmer.

IZUP635E **The request could not be completed. User** *user-id* **is not authorized to issue requests to the common event adapter (CEA).**

Explanation: The request failed because the specified user is not authorized to issue requests to CEA.

System programmer response: Grant the user permission to issue requests to CEA. z/OSMF includes scripts for authorizing user IDs to the required resources on your z/OS system. For information about the scripts, see Chapter 3, "Configuring z/OSMF," on page 25.

User response: Contact your z/OSMF administrator or system programmer.

IZUP636E **The request could not be completed. Incident** *incident-type* **created** *date-time* **does not exist.**

Explanation: The request failed because the selected incident could not be found by the system. The incident might have been deleted by another user.

System programmer response: No action is required.

User response: Click **Refresh** to update the *Incident Log* panel.

IZUP637E **The request could not be completed. User** *user-id* **is unable to access the active dump analysis and elimination (DAE) data set.**

Explanation: The request failed because either DAE has not been configured or the user does not have write access to the active DAE data set.

System programmer response: Ensure that DAE is configured; see "Configuring dump analysis and elimination" on page 162. Also, ensure that the specified user has write access to the active DAE data set.

User response: Contact your z/OSMF administrator or system programmer.

IZUP638E **The request could not be completed. No incident information is available.**

Explanation: The request could not be completed because no incident information is available. Typically, this error occurs when the sysplex dump directory is empty. The directory might be empty because:

- No incidents have occurred.
- Incidents were deleted from the sysplex dump directory.
- Incidents have occurred; however, because z/OSMF is not configured properly, the incidents are not stored in the sysplex dump directory.

System programmer response: Check the system to verify that no incidents have occurred. Ensure that z/OSMF is configured properly. For additional information about the error, see the Troubleshooting chapter in *IBM z/OS Management Facility User's Guide*, SA38-0652, in the IBM z/OS Internet Library.

User response: Verify that incidents are no longer available in the incident log. To do so, you might need to modify your date and time filter. If incidents are no longer available, contact your z/OSMF administrator or system programmer.

IZUP639E **The request could not be completed. An error occurred:** *error*

Explanation: The request failed because of one of the following errors:

1. The SYS1.MIGLIB data set might not be APF-authorized. Typically, this error occurs when the data set name is not listed in the PROGxx parmlib member.
2. Dump Analysis and Elimination (DAE) might not be configured or running. DAE might be restarting because a user ran the **Allow Next Dump** action.
3. If you attempted to delete an incident, another user may be browsing one or more of data sets associated with the incident, such as the dump data set. The incident cannot be deleted while the associated data sets are in use.
4. An unexpected error.

System programmer response: Perform one of the following steps:

1. To add the SYS1.MIGLIB data set name to PROGxx parmlib member, issue the following command: `SETPROG APF,ADD,DSN=SYS1.MIGLIB,VOL=nnnnnn`.
2. Ensure that DAE is configured. For information, see "Configuring dump analysis and elimination" on page 162. Also ensure that the user has write access to the active DAE data set.
3. Wait for the other user to release the data set and then retry your request to delete the incident.
4. To obtain more details about the error, enable the Common Information Model (CIM) server tracing. For information about enabling CIM server tracing, see z/OS Common Information Model User's Guide. Contact the IBM Support Center and provide the CIM trace and this error information.

User response: Try the request again. If the problem persists, contact your z/OSMF administrator or system programmer.

IZUP640E **The request could not be completed. The System REXX (SYSREXX) address space is not running.**

Explanation: The request failed because the SYSREXX address space is not running.

System programmer response: To start the SYSREXX address space issue the `START AXRPSTRT` command from the operator console. Verify SYSREXX is active by issuing the `D A,AXR` command.

User response: Contact your z/OSMF administrator or system programmer.

IZUP641E The request could not be completed. There is contention on the sysplex dump directory.

Explanation: The request could not be completed because there is contention on the sysplex dump directory. If another user is using Interactive Problem Control System (IPCS) to access the sysplex dump directory, that user has it exclusively locked; therefore, other users are not allowed to access the directory. Contention might also occur if several users are trying to access the sysplex dump directory at the same time.

System programmer response: No action is required.

User response: Try your request again later. If another user is using IPCS to access the sysplex dump directory, wait for the directory to be released and then retry your request.

IZUP642E The request could not be completed. z/OSMF could not open the sysplex dump directory.

Explanation: The request could not be completed because z/OSMF could not open the sysplex dump directory. The directory might not be set up correctly.

System programmer response: Verify that the sysplex dump directory has been constructed correctly. The default name is SYS1.SDDIR. For more information about setting up the sysplex dump directory, see *IBM z/OS Management Facility User's Guide*, SA38-0652, in the IBM z/OS Internet Library.

User response: Contact your z/OSMF administrator or system programmer.

IZUP643E The request could not be completed. The System REXX (SYSREXX) environment is not available.

Explanation: The request could not be completed because the SYSREXX environment is not available. Typically, this error occurs when the runtime support for compiled REXX has not been set up.

System programmer response: Install the REXX library and the REXX alternate library. For more information, see *IBM Compiler and Library for REXX on zSeries: User's Guide and Reference* in the IBM z/OS Internet Library.

User response: Contact your z/OSMF administrator or system programmer.

IZUP644E The system is busy and is unable to process the request. Try the request again later.

Explanation: The request failed because the system was not able to process the request before it timed out.

System programmer response: Check for system operations that are consuming a large amount of resources.

User response: Try the request again later. If the condition persists, contact your z/OSMF administrator or system programmer.

IZUP645E The system is busy and is unable to schedule the request. Try the request again later.

Explanation: The request failed because the System REXX (SYSREXX) could not schedule the request before it timed out.

System programmer response: Check for SYSREXX operations that are consuming a large amount of resources.

User response: Try the request again later. If the condition persists, contact your z/OSMF administrator or system programmer.

IZUP646W The request could not be completed. The symptom string for the SVC dump associated with incident *incident-type* **created** *date-time* **is not being suppressed by dump analysis and elimination (DAE).**

Explanation: The request failed because the symptom string for the SVC dump associated with the specified incident is not being suppressed by DAE. The next time an SVC dump is requested for a problem with the same symptoms, the dump will be taken by the system because it is not being suppressed. In this case, z/OSMF made no changes to DAE when the **Allow Next Dump** action was invoked.

DAE might not be suppressing dumps with this symptom string because DAE might have been disabled when the abend occurred.

System programmer response: No action is required.

User response: No action is required.

IZUP650I Job *job-name* **(***job-id***) has been submitted. The diagnostic data** *data-type* **is being sent in file** *file-name***.**

Explanation: The job with the name and ID specified has been submitted to z/OS. When it starts, the job will send the specified diagnostic data to the selected FTP destination. The diagnostic data is being sent in a file with the specified name.

System programmer response: No action is required.

User response: No action is required.

IZUP651E **The diagnostic data *data-type* was not sent to the FTP destination. An error occurred while submitting the FTP job.**

Explanation: The diagnostic data was not sent to the FTP destination because z/OSMF could not submit the FTP job. The previous error messages provide more details about the source of the problem.

System programmer response: Verify that the Incident Log task is configured correctly. For information about configuring the Incident Log task, see Chapter 3, "Configuring z/OSMF," on page 25. For additional help, contact the IBM Support Center.

User response: For more information about the problem, review the previous error messages. Contact your z/OSMF administrator or system programmer.

IZUP701I **Submitted job *job-id* to send diagnostic data for user *user-id*.**

Explanation: The specified job has been submitted for the specified user ID.

System programmer response: No action is required.

User response: No action is required.

IZUP702E **The incident could not be deleted. FTP jobs are currently in progress for incident *incident-type* created *date-time*.**

Explanation: The **Delete Incident** action failed for the specified incident because it has FTP jobs that are currently in progress. You cannot delete incidents that have FTP jobs in progress.

System programmer response: No action is required.

User response: On the *FTP Job Status* panel, view the status of the jobs for the selected incident. To delete the incident, either wait for the FTP jobs that are in progress to complete or can cancel the FTP jobs.

IZUP703I **The status was deleted for the FTP job submitted *date-time*. This job was used to send diagnostic data *data-type* to FTP destination *destination*.**

Explanation: The specified FTP job status has been removed from the FTP Job Status table.

System programmer response: No action is required.

User response: No action is required.

IZUP704I **The request to cancel FTP job *job-id* submitted *date-time* was received. This job was used to send diagnostic data *data-type* to FTP destination *destination*. To monitor the progress of the request, view the status of the job on the FTP Job Status panel.**

Explanation: The request to cancel the specified FTP job has been received. The job might not be cancelled immediately. To monitor the progress of the request, view the status of the job on the *FTP Job Status* panel. When the job has been cancelled, the Status column will contain the word *Cancelled*. If the status is a value other than *Cancelled* or *Cancel in progress*, the request might have failed.

System programmer response: No action is required.

User response: To view the current status of the job, refresh the *FTP Job Status* panel. To determine if the request failed, check the z/OS hard copy logs.

IZUP705E **The status for the FTP job submitted *date-time* does not exist. This job was used to send diagnostic data *data-type* to FTP destination *destination*. The request could not be completed.**

Explanation: The request failed because the requested job status could not be found. It might have been deleted by another user.

System programmer response: No action is required.

User response: Click **Refresh** to update the *FTP Job Status* panel.

IZUP706E **FTP job *job-id* was not cancelled. See previous error messages.**

Explanation: The FTP job could not be cancelled. The previous errors provide more details about the source of the problem.

System programmer response: Contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUP707E **The current status of FTP job *job-id* could not be retrieved. Reason: *reason***

Explanation: The current status of the FTP job could not be retrieved because of the specified reason.

System programmer response: Contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUP733E **The request could not be completed. z/OS failed to submit the job control language (JCL): *JCL***

Explanation: The request failed because z/OS could not submit the specified JCL. Typically, this error occurs when the JCL is not valid or when z/OS fails to run the JCL.

System programmer response: Ensure that the

specified JCL is valid. If it is not valid, re-invoke the *Send Diagnostic Data* wizard, enter valid information, and then re-send the diagnostic data. Otherwise, check the z/OSMF logs and operator messages for additional information. Contact the IBM Support Center and provide the log information.

User response: Contact your z/OSMF administrator or system programmer.

IZUP775I **FTP profile** *profile-name* **was modified.**

Explanation: The request to modify the properties for the named FTP profile has completed.

System programmer response: No action is required.

User response: No action is required.

IZUP776E **The request failed because FTP profile** *profile-name* **does not exist.**

Explanation: The request failed because the specified FTP profile could not be found. It might have been deleted by another user.

System programmer response: No action is required.

User response: Click **Refresh** to update the *FTP Profiles* panel.

IZUP777I **FTP profile** *profile-name* **was created.**

Explanation: The request to create a new FTP profile has completed.

System programmer response: No action is required.

User response: No action is required.

IZUP778I **FTP profile** *profile-name* **was deleted.**

Explanation: The request to delete the specified FTP profile has completed.

System programmer response: No action is required.

User response: No action is required.

IZUP779E **FTP profile** *profile-name* **was not created because an FTP profile with the same name already exists.**

Explanation: The request to create a new FTP profile failed because an FTP profile with the same name already exists. The FTP profile name must be unique. FTP profile names are case sensitive; for example, *FIRE1* and *Fire1* are two different FTP profiles.

System programmer response: No action is required.

User response: Enter a unique FTP profile name.

IZUP780E **The request failed because FTP profile** *profile-name* **contains errors. Review the field-level messages and make changes as needed.**

Explanation: When you click **OK**, any changes you made are saved and the panel or dialog box is closed. You cannot save any data that you entered on a panel or dialog box if required values are missing or if some of the specified values are not valid. The fields that contain errors have a red background and an image of a red circle with an X in the middle.

System programmer response: No action is required.

User response: Review the field-level messages, by clicking in the field or hovering over the image. Make changes as needed, then click **OK**. If you click **Cancel**, any changes that you entered will not be saved.

IZUP781E **FTP profile** *profile-name* **was not deleted because it is associated with an FTP destination.**

Explanation: You cannot delete an FTP profile when it is associated with an FTP destination.

System programmer response: No action is required.

User response: To delete the FTP profile, first, use the *FTP Destinations* panel to remove the association between the FTP destinations and the selected FTP profile. Then, delete the FTP profile.

IZUP782E **IBM-supplied FTP destinations cannot be modified.**

Explanation: You cannot modify IBM-supplied FTP destinations.

System programmer response: No action is required.

User response: If you want to create a similar destination, copy the IBM-supplied FTP destination and make changes as needed.

IZUP783E **The request failed because FTP destination** *destination* **does not exist.**

Explanation: The request failed because the specified FTP destination could not be found. It might have been deleted by another user.

System programmer response: No action is required.

User response: Click **Refresh** to update the *FTP Destinations* panel.

IZUP784E **The request failed because FTP destination** *destination* **contains errors. Review the field-level messages and make changes as needed.**

Explanation: When you click **OK**, any changes you

made are saved and the panel or dialog box is closed. You cannot save any data that you entered on a panel or dialog box if required values are missing or if some of the specified values are not valid. The fields that contain errors have a red background and an image of a red circle with an X in the middle.

System programmer response: No action is required.

User response: Review the field-level messages, by clicking in the field or hovering over the image. Make changes as needed, then click **OK**. If you click **Cancel**, any changes that you entered will not be saved.

IZUP785I **FTP destination** *destination* **was created.**

Explanation: The request to create a new FTP destination has completed.

System programmer response: No action is required.

User response: No action is required.

IZUP786I **FTP destination** *destination* **was deleted.**

Explanation: The request to delete the specified FTP destination has completed.

System programmer response: No action is required.

User response: No action is required.

IZUP787E **The FTP destination was not created because an FTP destination with the same system** *system* **and path name** *path-name* **already exists.**

Explanation: The request to create a new FTP destination failed because an FTP destination with the same system and path name combination already exists. The system and path name combination for each FTP destination must be unique. The FTP destination is not case sensitive; for example, *FOO.IBM.com/TOIBM/MVS* and *foo.ibm.com/toibm/mvs* are the same FTP destination.

System programmer response: No action is required.

User response: Enter a unique FTP destination.

IZUP788I **FTP destination** *destination* **was modified.**

Explanation: The request to modify the FTP destination has completed.

System programmer response: No action is required.

User response: No action is required.

IZUP802W **You are about to close the Send Diagnostic Data wizard. The send will be cancelled and all of the information you entered will be discarded. Do you want to continue?**

Explanation: When you click **Cancel**, z/OSMF completes three actions:

- Discards your changes.
- Ends or cancels the action.
- Closes the panel or dialog box.

This dialog box allows you to confirm whether you want to cancel your request.

System programmer response: No action is required.

User response: To close the *Send Diagnostic Data* wizard and discard your changes, click **OK**. You cannot undo this action. To return to the *Send Diagnostic Data* wizard and keep your changes, click **Cancel**.

IZUP804W **More than** *number* **incidents have been selected. This might increase the amount of time required to complete the action. Do you want to continue?**

Explanation: Selecting more than the number of incidents specified can increase the amount of time it takes for z/OSMF to complete the selected action.

System programmer response: No action is required.

User response: Click **OK** to continue. If you want to select fewer incidents, click **Cancel**.

IZUP805E **User ID is a required field. Enter a valid user ID.**

Explanation: When *Specify user ID and password* is selected, you must enter the user ID and password needed to access the FTP destination. The User ID and Password fields cannot be blank.

System programmer response: No action is required.

User response: Enter a valid user ID.

IZUP806E **Password is a required field. Enter a valid password.**

Explanation: When *Specify user ID and password* is selected, you must enter the user ID and password needed to access the FTP destination. The User ID and Password fields cannot be blank.

System programmer response: No action is required.

User response: Enter a valid password.

IZUP807E The firewall port is not valid. Enter a valid port number.

Explanation: The port number must be an integer between 1 and 65535. If you leave the Firewall port field blank, the installation's default firewall port is used.

System programmer response: No action is required.

User response: Enter a valid port number.

IZUP808E The FTP.DATA file name is not valid. Enter a valid file name.

Explanation: The FTP.DATA file name can be one of the following types:

- **Sequential data set.** The name consists of a set of names separated by periods. For example, *NAME1.NAME2.NAME3*. Each name can contain up to eight of the following characters: alphanumeric characters (A-Z, a-z, and 0-9), special characters ($ # @), and hyphens. The first character of each name must be an alphanumeric or special character. The data set name cannot contain leading or trailing periods. It has a maximum length of 44 characters (including periods).
- **Partitioned data set member.** The name has the same rules as the sequential data set name except that it contains up to 54 characters and the member name is included in parentheses. For example, *NAME1.NAME2.NAME3(MEMBER)*. The extra 10 characters are for the parentheses and eight character member name. The member name must conform to the same rules as the individual names in the sequential data set name.
- **Generation data group.** The name has the same rules as the sequential data set name except that it can contain up to 41 characters and an integer is included in parentheses. For example, *NAME1.NAME2.NAME3(-01)*. The individual names have a combined maximum length of 35 characters. The integer can be any number from -255 through +255. If the integer is not zero (0), the sign (+ or -) must be included. Leading zeros are allowed. For example, *-09*, *000*, or *+025*.
- **Hierarchical or zSeries® file system.** The name can contain up to 1023 characters including alphanumeric characters (A-Z, a-z, and 0–9), blanks, mathematical symbols (+ - = | ~ ( ) { } \), punctuation marks (? , . ! ; : ' " / [ ]), and the following special characters: %, $, #, @, ^, *, and _. For example, */etc/ftp.data*.

When sending diagnostic data to an FTP destination, if z/OSMF cannot find the specified FTP.DATA file, a job control language (JCL) error might occur and the send might fail.

System programmer response: No action is required.

User response: Enter a valid FTP.DATA file name.

IZUP809E Firewall user ID is a required field. Enter a valid firewall user ID.

Explanation: When the substitution variables `&PROXY_USER;`, `&PROXY_PW;`, or both are included in the Firewall Commands field for the selected FTP profile, you must enter the user ID and password needed to access your installation's firewall or proxy. The Firewall user ID and Firewall password fields cannot be blank.

System programmer response: No action is required.

User response: Enter a valid firewall user ID.

IZUP810E Firewall password is a required field. Enter a valid firewall password.

Explanation: When the substitution variables `&PROXY_USER;`, `&PROXY_PW;`, or both are included in the Firewall Commands field for the selected FTP profile, you must enter the user ID and password needed to access your installation's firewall or proxy. The Firewall user ID and Firewall password fields cannot be blank.

System programmer response: No action is required.

User response: Enter a valid firewall password.

IZUP818W You are about to delete the selected FTP profiles. Do you want to continue?

Explanation: When you select the **Delete** action, the selected FTP profiles are removed from the FTP Profiles table. This dialog box allows you to confirm whether you want to delete the selected FTP profiles.

System programmer response: No action is required.

User response: Click **OK** to delete the selected FTP profiles. You cannot undo this action. If you do not want to delete the selected FTP profiles, click **Cancel**.

IZUP819W You are about to delete the selected FTP destinations. Do you want to continue?

Explanation: When you select the **Delete** action, the selected FTP destinations are removed from the FTP Destinations table. This dialog box allows you to confirm whether you want to delete the selected FTP destinations.

System programmer response: No action is required.

User response: Click **OK** to delete the selected FTP destinations. You cannot undo this action. If you do not want to delete the selected FTP destinations, click **Cancel**.

IZUP820E The host name or IP address is not valid.

Explanation: The host name or IP address is not valid because it is either missing, too long, or contains incorrect characters. A valid host name can contain up

to 63 of the following characters: alphanumeric characters (A-Z, a-z, and 0–9), periods (.), and minus signs (-). Periods are allowed only as a delimiter within the host name. The first character must be an alphanumeric character. The last character cannot be a period or minus sign. The host name is not case sensitive; for example, *FOO.ibm.com* and *foo.ibm.com* are the same system.

A valid IP address can be either an IPv4 or IPv6 address. IPv4 addresses have a dot-decimal notation format where you can have a total of eight decimal digits separated by three periods. IPv6 addresses have a colon-hexadecimal notation format where you can have 32 hexadecimal digits separated by colons. Typically, IPv6 addresses are written as eight groups of four hexadecimal digits.

The System field cannot be blank.

System programmer response: No action is required.

User response: Enter a valid host name or IP address.

IZUP821E The path name is not valid. Enter a valid path name.

Explanation: The path name is not valid because it is either missing or too long. A valid path name can contain up to 730 characters. The path name is not case sensitive; for example, */toibm/mvs* and */TOIBM/MVS* are the same path name. The Path name field cannot be blank.

System programmer response: No action is required.

User response: Enter a valid path name.

IZUP822E The profile name is not valid. Enter a valid profile name.

Explanation: The profile name is not valid because it is either missing, too long, or contains incorrect characters. A valid profile name consists of up to 40 of the following characters: alphanumeric characters (A-Z, a-z, and 0–9), blanks, underscores (_), and hyphens (-). The Profile name field cannot be blank.

System programmer response: No action is required.

User response: Enter a valid profile name.

IZUP823E The firewall host name or IP address is not valid.

Explanation: The firewall host name or IP address is not valid because it is either missing, too long, or contains incorrect characters. A valid host name can contain up to 63 of the following characters: alphanumeric characters (A-Z, a-z, and 0–9), periods (.), and minus signs (-). Periods are allowed only as a delimiter within the host name. The first character must be an alphanumeric character. The last character cannot be a period or minus sign. The host name is not case sensitive; for example, *FOO.ibm.com* and *foo.ibm.com* are the same system.

A valid IP address can be either an IPv4 or IPv6 address. IPv4 addresses have a dot-decimal notation format where you can have a total of eight decimal digits separated by three periods. IPv6 addresses have a colon-hexadecimal notation format where you can have 32 hexadecimal digits separated by colons. Typically, IPv6 addresses are written as eight groups of four hexadecimal digits.

The Firewall host field cannot be blank.

System programmer response: No action is required.

User response: Enter a valid firewall host name or IP address.

IZUP824E The user ID is too long. Enter a user ID that contains no more than *maximum-number* characters.

Explanation: The user ID can contain up to the specified maximum number of characters.

System programmer response: No action is required.

User response: Enter a user ID that contains no more than the maximum number of characters.

IZUP825E The profile name is too long. Enter a profile name that contains no more than *maximum-number* characters.

Explanation: The profile name can contain up to the specified maximum number of characters.

System programmer response: No action is required.

User response: Enter a profile name that contains no more than the maximum number of characters.

IZUP826E The firewall commands are not valid. Enter firewall commands that contain no more than *maximum-number-1* rows and no more than *maximum-number-2* characters on each row.

Explanation: The firewall commands are not valid because the field either is blank, contains too many rows, or contains too many characters on a row. The Firewall Commands field is a required field. It cannot be blank. The Firewall Commands field can contain up to the specified maximum number of rows. Each row can contain up to the specified maximum number of characters.

System programmer response: No action is required.

User response: Enter firewall commands that do not exceed the maximum number of rows and do not exceed the maximum number of characters allowed for each row.

IZUP827E The port number is not valid. Enter a valid port number.

Explanation: The port number must be an integer between 1 and 65535. If you leave the Port number field blank, the installation's default port is used.

System programmer response: No action is required.

User response: Enter a valid port number.

IZUP828I You are about to allow dump analysis and elimination (DAE) to take a new memory dump for the same symptom when it recurs. Doing so will start DAE on each system in the sysplex. Do you want to continue?

Explanation: If DAE is active and an SVC dump is requested that has the same symptom string as the SVC dump associated with the selected incident, that dump is suppressed by DAE. You can update DAE so that it will not suppress the next dump request that has the same symptoms. To do so, click **OK**.

Each time you request to allow the next dump, DAE is recycled for each system in the sysplex. If DAE was not enabled on a system in the sysplex, invoking this action starts DAE.

System programmer response: No action is required.

User response: Click **OK** to allow the system to take the next dump that has the same symptoms as the dump associated with the selected incident. If you do not want to allow the next dump, click **Cancel**.

IZUP830E The firewall user name is too long. Enter a firewall user name that contains no more than *maximum-number* **characters.**

Explanation: The user name can contain up to the maximum number of characters specified in the message.

System programmer response: No action is required.

User response: Enter a user name that contains no more than the maximum number of characters.

IZUP831E The firewall password is too long. Enter a firewall password that contains no more than *maximum-number* **characters.**

Explanation: The password can contain up to the specified maximum number of characters.

System programmer response: No action is required.

User response: Enter a password that contains no more than the maximum number of characters.

IZUP832E The password is too long. Enter a password that contains no more than *maximum-number* **characters.**

Explanation: The password can contain up to the specified maximum number of characters.

System programmer response: No action is required.

User response: Enter a password that contains no more than the maximum number of characters.

IZUP834E The path name is too long. Enter a path name that contains no more than *maximum-number* **characters.**

Explanation: The path name can contain up to the specified maximum number of characters.

System programmer response: No action is required.

User response: Enter a path name that contains no more than the maximum number of characters.

IZUP835W You are about to delete the selected incidents and all associated information. Do you want to continue?

Explanation: When you select the **Delete Incident** action, the selected incidents are removed from the Incident Log table. Also, all associated FTP job status information and diagnostic data are removed from z/OSMF. This dialog box allows you to confirm whether you want to delete the selected incidents.

If system-initiated (abend-related) incidents have been selected, this dialog box also warns that z/OSMF might not have a record of future instances of the same symptoms if the dumps are being suppressed by dump analysis and elimination (DAE). To capture the next instance of the dumps, complete one of the following steps for each incident:

- Select **Allow next dump**.
- If the **Allow next dump** option is not provided, complete the following steps:
  - Click **Cancel** to exit the dialog box.
  - Use the **Allow Next Dump** action provided on the *Incident Log* panel.
  - Proceed with the **Delete Incident** action.

Each time you request to allow the next dump, DAE is recycled for each system in the sysplex. If DAE was not enabled on a system in the sysplex, invoking the **Allow Next Dump** action starts DAE.

System programmer response: No action is required.

User response: Click **OK** to delete the selected incidents. You cannot undo this action. If you do not want to delete the selected incidents, click **Cancel**.

IZUP836W You are about to delete the selected FTP job status. Do you want to continue?

Explanation: When you select the **Delete FTP Status** action, the selected FTP job status are removed from the FTP Job Status table. This dialog box allows you to confirm whether you want to delete the selected job status.

System programmer response: No action is required.

User response: Click **OK** to delete the selected FTP job status. You cannot undo this action. If you do not want to delete the selected FTP job status, click **Cancel**.

IZUP837W You are about to cancel the selected FTP jobs. Do you want to continue?

Explanation: When you select the **Cancel Job** action, the send is terminated. Information that has already been transmitted to the FTP destination is not removed; therefore, the FTP destination might have received incomplete diagnostic data files. This dialog box allows you to confirm whether you want to cancel the selected FTP jobs.

System programmer response: No action is required.

User response: Click **OK** to cancel the selected FTP jobs. You cannot undo this action. If you do not want to cancel the selected FTP jobs, click **Cancel**.

IZUP840E An error occurred. z/OSMF cannot retrieve your user ID. Enter a valid user ID and password.

Explanation: z/OSMF cannot retrieve your user ID; therefore, you must specify a user ID and password.

System programmer response: Verify that z/OSMF is configured properly; see Chapter 3, "Configuring z/OSMF," on page 25. If the problem persists, contact the IBM Support Center.

User response: Enter the user ID and password required to access the FTP destination. If the FTP destination allows anonymous FTP, enter `anonymous` in the ID field and enter your z/OSMF user ID followed by an at (@) sign in the Password field. For example, if your user ID is *ibmuser*, you would enter `ibmuser@`. If the problem persists, contact your z/OSMF administrator or system programmer.

IZUP841W A five character IBM PMR or ETR number is being used. The branch and country code will be added when the job is submitted.

Explanation: The IBM PMR or ETR number does not contain the installation's branch and country code. When you view the job control language (JCL), the name of the file being sent contains the specified number followed by placeholders for the branch (*bbb*) and country code (*ccc*). When the job is submitted, z/OSMF replaces the placeholders with the installation's branch and country code.

System programmer response: No action is required.

User response: No action is required.

IZUP842E The job settings are not valid. Enter valid job settings.

Explanation: The Job settings field contains errors. Typically, this error occurs when:

- There are more than 72 characters on a row. Each row in the Job settings field can contain up to 72 characters. For information about continuing job control language (JCL) statements, see *MVS JCL Reference* in the IBM z/OS Internet Library.
- The job name is formatted incorrectly. The job name is required and must:
  - Begin in column 3 of the JOB statement.
  - Be 1-8 characters in length.
  - Start with an alphabetic character (A-Z) or a special character (# @ $).
  - Contain only alphanumeric characters (A-Z and 0-9) or special characters (# @ $). Blanks cannot be included in the name.
- The JOB statement is missing. The JOB statement is required and must:
  - Contain the characters // in columns 1 and 2.
  - Have a name that starts in column 3.
  - Have an operation field that contains the characters JOB and is preceded and followed by at least one blank.

System programmer response: No action is required.

User response: Enter valid job settings.

IZUP910E The request could not be completed. The request to the Common Information Model (CIM) server failed.

Explanation: The request could not be completed because the request to the CIM server failed. The error might have occurred because the user is not authorized to access the CIM resource needed to complete the request.

System programmer response: For additional information about the error, view the logs for z/OSMF, IBM WebSphere® Application Server OEM Edition for z/OS, and z/OS hard copy logs. If the z/OS hard copy logs contain authority errors, grant the user the appropriate authority. For more information on authorizing users to CIM, see the topic on configuring the Incident Log task in *IBM z/OS Management Facility User's Guide*, SA38-0652, in the IBM z/OS Internet Library. If the problem persists, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUP911E The request could not be completed. The Common Information Model (CIM) server is not responding.

Explanation: The request could not be completed because z/OSMF could not connect to the CIM server or the connection was lost and could not be re-established.

System programmer response: Ensure that the Common Information Model (CIM) server is functioning properly. For more information about setting up CIM, see z/OS Common Information Model User's Guide.

User response: Try the request again later. If the problem persists, contact your z/OSMF administrator or system programmer.

IZUP912E The request could not be completed. The user *user-id* is not authorized to access the Common Information Model (CIM) server.

Explanation: A failure occurred either authenticating to the system, host, or service or trying to gain authorization to a specific system. If user ID is "null," it indicates a guest user.

System programmer response: Ensure that the user has the appropriate authorization.

User response: Request the appropriate authorization from your z/OSMF administrator or system programmer.

IZUP915E The request could not be completed. The requested resource does not exist.

Explanation: The request failed because the resource could not be found.

System programmer response: For more information about the error, check the z/OSMF logs. If the problem persists, contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUP916E The request could not be completed. The Common Information Model (CIM) server timed out.

Explanation: The request failed because the time to process the request exceeded the time allowed. The problem might be that the dump data set was migrated when you completed one of the following actions:

- Requested that an incident be deleted.
- Requested that the diagnostic data associated with an incident be sent to an FTP destination.
- Opened the *View Diagnostic Details* panel.

This error might also occur if the system is too busy to process the request.

System programmer response: Check the logs to determine the status of the system and correct any problems. If the error occurred when you completed one of the actions listed in the explanation, determine whether the dump data set is migrated. If the data set is migrated and automatic recall is not enabled for the hierarchical storage manager (HSM), recall it. Otherwise, wait for the auto recall to complete.

User response: Try the request again later. If the problem persists, contact your z/OSMF administrator or system programmer.

IZUP991E Unable to register the Incident Log task.

Explanation: An internal error occurred when initializing the Incident Log task. The Incident Log task will not be available to any user in z/OSMF.

System programmer response: Contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUP992E The request could not be completed. z/OSMF is unable to verify that the user is authorized to access the Incident Log task.

Explanation: The request failed because an error occurred while z/OSMF was verifying that the user is authorized to access the Incident Log task.

System programmer response: Check the z/OSMF logs for more information. Contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

IZUP999E The request could not be completed. An error occurred: *error*

Explanation: The request failed because the specified error occurred.

System programmer response: Check the error text to determine the problem or contact the IBM Support Center.

User response: Contact your z/OSMF administrator or system programmer.

Appendix A. z/OS system setup for z/OSMF

Enabling your z/OS system for z/OSMF requires some initial setup work on the z/OS host system. How much work depends largely on whether your installation plans to enable the Incident Log task in addition to the base functions of z/OSMF (referred to as *core functions* in this document).

To enable the Incident Log task, the z/OSMF configuration process performs a number of these updates to your z/OS system. For your reference, this section provides the manual steps for performing these updates.

Other steps, such as creating the sysplex dump directory, you must perform manually.

Summary of system changes for z/OSMF

Table 17 summarizes the z/OS system changes that are required or recommended for enabling the z/OSMF tasks and core functions. Much of this work might already be done on your system, for example, enabling the operations log (OPERLOG) log stream. If so, you can skip the particular setup action. Other setup actions might require modifications to an existing setting. For example, if your installation has already defined a couple data set for the system logger component, you might need to increase the space allocation for system logger log stream records. The setup actions are described in more detail in the sections that follow.

Table 17. z/OS setup actions by z/OSMF task

z/OS setup action	Used by	Where described
Define security authorizations on your z/OS system.	All tasks and core functions of z/OSMF.	The z/OSMF configuration process creates REXX execs with sample RACF commands for your installation's security administrator. See Chapter 3, "Configuring z/OSMF," on page 25.
Migrate the configuration backing stores from the Windows environment to the z/OS host system.	Configuration Assistant task	See "Updating z/OS for Configuration Assistant" on page 47.
If your system environment has not been set up with LOGR couple data sets for IBM WebSphere Application Server OEM Edition for z/OS, define these data sets in the sysplex in which z/OSMF is installed.	Incident Log task	See "Defining a couple data set for system logger" on page 156.
Define and enable the operations log (OPERLOG) in a system logger log stream.	Incident Log task	See "Enabling the operations log (OPERLOG)" on page 158

Table 17. z/OS setup actions by z/OSMF task (continued)

z/OS setup action	Used by	Where described
Define and enable the LOGREC log stream.	Incident Log task	See "Defining and activating the logrec log stream" on page 160.
Define OPERLOG and LOGREC model log streams for diagnostic log snapshots to be obtained by the common event adapter (CEA) component of z/OS.	Incident Log task	See "Defining diagnostic snapshot log streams" on page 161
Set up and configure automatic dump data set allocation (auto-dump).	Incident Log task	See "Configuring automatic dump data set allocation" on page 161.
Configure dump analysis and elimination (DAE): • Specify SUPPRESSALL in the ADYSET00 parmlib member to ensure that duplicate SVC dumps are suppressed. • Update ADYSET00 and ADYSET01 to have sysplex-wide scope.	Incident Log task	See "Configuring dump analysis and elimination" on page 162.
Create a sysplex dump directory.	Incident Log task	See "Creating the sysplex dump directory" on page 163.
Ensure that CEA is active.	Incident Log task	See "Ensuring that CEA is active" on page 165
Ensure that System REXX (SYSREXX) is active.	Incident Log task	See "Ensuring that System REXX is active" on page 166.
If your installation has chosen to rename a dump data set, ensure that the data set name in the sysplex dump directory is correct.	Incident Log task	"Ensuring that dump data set names are correct" on page 166.
Ensure that SYS1.MIGLIB is APF-authorized.	Incident Log task	See "Authorizing the SYS1.MIGLIB data set" on page 167

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.

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 Setting up a Sysplex*, SA22-7625.

System logger supports shared sysplex-scope (coupling facility resident) log streams and single-system DASD-only log streams, as follows:

- Coupling facility (CF) log streams are sysplex-wide in scope; any system in the sysplex can write to these log streams.
- DASD-only log streams can be written to by the local system only. When a DASD-only log stream is closed, it can be read from other systems in the sysplex if it resides on DASD that is shared by the other systems in the sysplex.

The system creates DASD-only log streams for the operations log (OPERLOG) and the sysplex LOGREC diagnostic snapshots. You do not need to predefine the DASD-only log streams. For the model used, see sample job CEASNPLG, which is supplied by IBM in SYS1.SAMPLIB(CEASNPLG).

Use shared DASD as the target for OPERLOG and LOGREC snapshots, so that the Incident Log task can access the log snapshots from any system in the sysplex.

In planning the space requirements for your system logger couple data set, plan for two DASD-only log streams per incident. To allow up to 100 incidents, for example, you must allow enough space for 200 log streams.

IBM recommends that you allow space for up to 1000 DASD-only log streams (or 500 incidents). To do so, use the IXCL1DSU format utility, for example:

```
//FMTLGCDS JOB  MSGLEVEL=(1,1)
//         EXEC PGM=IXCL1DSU
//* S SUBMIT,JOB=LOGGER.ZOS17.JCL(FORMAT17)
//* SETXCF COUPLE,ACOUPLE=(LOGGER.OSR12.LARGE.INVNTRY,LOGR3),TYPE=LOGR
//* SETXCF COUPLE,PSWITCH,TYPE=LOGR
//SYSPRINT DD   SYSOUT=*
//SYSIN    DD   *
 DEFINEDS SYSPLEX(PLEX1) DSN(LOGGER.OSR12.LARGE.INVNTRY) VOLSER(LOGR3)
   DATA TYPE(LOGR)
     ITEM NAME(LSR)      NUMBER(2000)
     ITEM NAME(LSTRR)    NUMBER(25)
     ITEM NAME(DSEXTENT) NUMBER(15)
     ITEM NAME(SMDUPLEX) NUMBER(1)
//
```

If the system logger couple data set lacks sufficient space to contain the diagnostic snapshots, the system issues message CEA0600I to indicate that the log streams could not be created.

To allow the Incident Log task to access diagnostic log snapshots on other systems in the sysplex, the log streams must reside on shared DASD. DASD-only log streams are expected to be written to SMS-managed DASD.

For more information about the following concepts, see *z/OS Setting Up a Sysplex*, which is available online in the IBM z/OS Internet Library:

- DASD-only log streams
- Setting up an SMS environment for DASD data sets
- Adding the data sets to the GRSRNL inclusion list
- Managing system logger log stream data sets
- Defining authorization.

Enabling the operations log (OPERLOG)

The operations log (OPERLOG) is a sysplex-scope 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.

To allow the system to obtain diagnostic snapshots of your installation's OPERLOG, the Incident Log task requires that OPERLOG be active in a system logger log stream. If you have not already enabled OPERLOG, it is recommended that you do so. For the steps to follow, see "Steps for setting up OPERLOG." If you choose to defer this step, the Incident Log runs without the ability to create OPERLOG snapshots.

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 Setting Up a Sysplex*, which is available online in the IBM z/OS Internet Library.

Before you begin

You must define the logger subsystem.

Procedure

1. Define the hardcopy device as OPERLOG in the HARDCOPY statement of the CONSOLxx parmlib member. You can change this setting using the command `V OPERLOG,HARDCPY`. To deactivate OPERLOG, you can use the command `V OPERLOG,HARDCOPY,OFF`.
2. Define the corresponding coupling facility structure in the CFRM policy. For example:

```
//OPERLOG JOB CLASS=A,MSGCLASS=A
//POLICY EXEC PGM=IXCMIAPU
//SYSPRINT DD SYSOUT=A
//SYSIN DD *
DATA TYPE(CFRM)
STRUCTURE NAME(OPERLOG)
SIZE(40448)
INITSIZE(40448)
PREFLIST(FACIL01,FACIL02)
```

3. Activate the CFRM policy through the command `START,POLICY,TYPE=CFRM,POLNAME=`*`polname`*, or through the COUPLExx parmlib member.
4. Define the log stream to the LOGR policy. The following example is for illustrative purposes only; follow the recommendations in *z/OS MVS Setting Up a Sysplex* and *z/OS MVS Programming: Assembler Services Guide*.

```
//OPERLOG JOB CLASS=A,MSGCLASS=A
//POLICY EXEC PGM=IXCMIAPU
//SYSPRINT DD SYSOUT=A
//SYSIN DD *
DATA TYPE(LOGR)
DEFINE STRUCTURE NAME(OPERLOG)
```

```
LOGSNUM(1)
MAXBUFSIZE(4092)
AVGBUFSIZE(512)
DEFINE LOGSTREAM NAME(SYSPLEX.OPERLOG)
STRUCTNAME(OPERLOG)
LS_DATACLAS(LOGR4K)
HLQ(IXGLOGR)
LS_SIZE(1024)
LOWOFFLOAD(0)
HIGHOFFLOAD(80)
STG_DUPLEX(NO)
RETPD(30)
AUTODELETE(No)
```

5. Create the security definitions for RACF (or an equivalent security product). In the following example, the SYSPLEX.OPERLOG of the LOGSTRM resource CLASS is given READ permission, which allows all users to browse the operations log and *userid1* has UPDATE access level, which allows *userid1* to delete records from the log stream. That is, the user ID associated with the job running the IEAMDBLG program. For example:

   ```
   RDEFINE LOGSTRM SYSPLEX.OPERLOG UACC(READ)
   PERMIT SYSPLEX.OPERLOG CLASS(LOGSTRM) ID(userid1)
   ACCESS(UPDATE) SETROPTS CLASSACT(LOGSTRM)
   ```

   This example is for illustrative purposes only. Follow the guidelines for your installation.

6. After you activate OPERLOG, you must manage the way in which records are handled.

   SYS1.SAMPLIB contains a sample program, IEAMDBLG, to read log blocks from the OPERLOG log stream and convert them to SYSLOG format. The program is an example of how to use the services of the system logger component to retrieve and delete records from the OPERLOG 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 stream all the records created prior to 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*, which is available online in the IBM z/OS Internet Library.

Results

To verify the completion of this work, enter the command `DISPLAY CONSOLES,HARDCOPY` to display OPERLOG status.

Defining and activating the logrec log stream

Logrec is the z/OS error log. It contains binary data describing error records that are written on behalf of system abends and other system recording requests. Logrec data is formatted through the batch utility EREP. The single-system version usually resides in a data set named SYS1.LOGREC,or *&SYSNAME*.LOGREC. The sysplex version resides in a system logger log stream.

To allow z/OSMF to obtain diagnostic snapshots of your installation logrec, the logrec data set must be active on your system. If you have not already defined the logrec data set, it is recommended that you do so. For the steps to follow, see "Steps for setting up the logrec log stream." If you choose to defer this step, the Incident Log task runs without the ability to create logrec snapshots.

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 Setting Up a Sysplex*, which is available online in the IBM z/OS Internet Library.

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 command `DISPLAY LOGREC` to display the current logrec error recording medium.

Defining diagnostic snapshot log streams

For optimal performance of the Incident Log task, it is recommended that your installation define operations log (OPERLOG) and logrec log streams for the CEA component of z/OS. Doing so allows the system logger component to determine the storage characteristics for storing diagnostic snapshots.

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*, which is available online in the IBM z/OS Internet Library.

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 accessable.

3. Start the function through the following command:

```
DUMPDS ALLOC=ACTIVE
```

For more details, see the following information:

- Topic on the DUMPDS command in *z/OS MVS System Commands*, SA22-7627
- Topic on SVC dump in *z/OS Tools and Service Aids*, GA22-7589.

If your installation does not use automatic dump data set allocation, it is likely that you have defined pre-allocated dump data sets (SYS1.DUMPxx) for the system to use. Typically, an installation archives an SVC dump to another data set as soon as the dump is complete, to avoid having the system overlay the data set with a subsequent dump. The archive data set name is defined by the installation and is not known to the system. If so, the following limitations result:

- Incident Log records identify the pre-allocated dumps. Thus, the same property information is shown for each incident.
- Send Data action does not locate the dump data set because the name is unknown to the Incident Log task. The system, however, continues to process the log snapshots.

To continue using pre-allocated dump data sets, your installation can use an IBM-supplied JCL step to rename the dump data set in the sysplex dump directory, to allow z/OSMF to locate the correct data set. For information, see "Ensuring that dump data set names are correct" on page 166.

Some installations use automatic dump data set allocation, but then, subsequently, copy the dump data sets to another volume (to preserve space in the SMS DASD set). If the copied data set has the same name as the original dump data set, and the data set is cataloged, the Incident Log "Send data" action will locate the copied dump data sets. However, if the copied dump data set has a different name, use the IBM-supplied JCL step to rename the dump data set in the sysplex dump directory so that the Incident Log task will locate it.

Configuring dump analysis and elimination

The Incident Log task requires that dump analysis and elimination (DAE) be active on the z/OS host system to avoid capturing duplicate problems in the Incident Log task display. If your installation has not already configured DAE, this topic summarizes the steps for doing so.

IBM recommends that you enable DAE to suppress SVC dumps with duplicate symptoms. This action ensures that the Incident Log task displays only the initial instance of a dump-related incident. If necessary, you can use the *allow next dump* option of the Incident Log task to allow the system to take and report the next dump that occurs for the same symptoms. You might use this option, for example, after you apply a fix for the problem. The Allow Next Dump option allows you to collect diagnostic data for the next new occurrence of the same problem.

IBM also recommends that you enable DAE to manage symptoms for a sysplex-wide collection of symptoms, rather than for a single system only.

For information about how to set up DAE, see *z/OS MVS Diagnosis: Tools and Service Aids*, which is available online in the IBM z/OS Internet Library.

To configure DAE processing, you use the following IBM-supplied members, which are provided in SYS1.PARMLIB:

- ADYSET00 to turn on DAE with single system scope
- ADYSET01 to turn off DAE with single system scope
- ADYSET02 is a copy of ADYSET00.

For more information about the IBM-supplied ADYSETxx parmlib members, see *z/OS MVS Initialization and Tuning Reference*, which is available online in the IBM z/OS Internet Library.

The steps for configuring DAE for Incident Log processing are summarized, as follows:

1. To ensure that duplicate SVC dumps are suppressed, verify that SUPPRESSALL is specified on the SVCDUMP parameter in the ADYSET00 member.
2. To have DAE use a sysplex-wide scope, edit the ADYSET00 and ADTSET01 members, as follows.
   - Edit the ADYSET00 member to include the settings SHARE, DSN and GLOBAL. For example:

```
DAE=START,RECORDS(400),
SVCDUMP(MATCH,SUPPRESSALL,UPDATE,NOTIFY(3,30)),
SYSMDUMP(MATCH,UPDATE),
SHARE(DSN,OPTIONS),DSN(SYS1.DAESH2) GLOBAL(DSN,OPTIONS)
```

   - Edit the ADYSET01 member to include the setting GLOBALSTOP. For example:

```
DAE=STOP,GLOBALSTOP
```

3. To turn on DAE, enter the command `SET DAE=00`. As supplied by IBM, the IEACMD00 member issues this command automatically at IPL-time.
4. Ensure that your 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*, which is available online in the IBM z/OS Internet Library.

Creating the sysplex dump directory

The sysplex dump directory is a shared VSAM data set that contains information about SVC dumps that have been taken on each of the systems in the sysplex. As each SVC dump is written to a data set, an entry is added by the dumping services address space (DUMPSRV) to the sysplex dump directory to store information like dump data set name, dump title, and symptom string.

The Incident Log task uses the sysplex dump directory as the repository for information about incidents that have occurred in the sysplex. If your installation has not already created a sysplex dump directory, this topic describes the steps for doing so.

Steps for creating the sysplex dump directory

To enable the Incident Log, your installation requires a sysplex dump directory data set (SYS1.DDIR or an installation-supplied name) with 15,000 records, which is about 60 cylinders. Approximately 50 directory entries are used for each incident and more are used for multi-system dumps.

To allow the Incident Log task (running on one system in the sysplex) to deliver a sysplex view of SVC dumps that are taken, select a DASD volume with shared access to all of the systems in the sysplex (or all systems that you want the Incident Log task to represent).

To create the sysplex dump directory, follow these steps:

1. Run the BLSCDDIR CLIST, which resides in system data set SYS1.SBLSCLI0(BLSCDDIR). For example:

   ```
   EXEC 'SYS1.SBLSCLI0(BLSCDDIR)'
   'DSNAME(SYS1.DDIR) VOLUME(VOLSER) RECORDS(15000)'
   ```

   This CLIST creates SYS1.DDIR as a VSAM data set with SHAREOPTIONS(1,3).
2. Update BLSCUSER with the dump directory name.
3. Recycle DUMPSRV so that the dump directory name is registered to this address space. To do so, enter the command CANCEL DUMPSRV. The DUMPSRV address space restarts automatically.
4. Start BLSJPRMI through the command START BLSJPRMI. This action registers the dump directory name to IPCS.

The name of the sysplex dump directory needs to be established before you perform any requests for incident information, and needs to be cataloged on the current system and any other (backup) system running the CIM server, to allow access by the Incident Log task.

For more information about using the BLSCDDIR CLIST, see *z/OS MVS IPCS User's Guide*, which is available online in the IBM z/OS Internet Library.

Considerations for using a sysplex dump directory

When using a sysplex dump directory, observe the following considerations:

- The sysplex dump directory (SYS1.DDIR, by default) is a shared VSAM data set serialized with an exclusive ENQ on the data set. This ENQ is used only by
  - DUMPSRV address space, when writing an entry to the directory for a new SVC dump
  - CEA address space, when reading or updating the dump directory for Incident Log requests.
- The sysplex dump directory is different from the IPCS user local dump directory. A local directory is created for each IPCS user to store detailed data related to the IPCS session. The sysplex dump directory is used only to save name and symptom data for all SVC dumps taken, and must not be used as an IPCS user local dump directory.
- **Do not access the sysplex dump directory from an IPCS user.** Instead, use a batch job to access the directory.
- If new entries are not being added to the Incident Log task, or if z/OSMF requests are not being satisfied, check for contention on the sysplex dump directory through the D GRS command. Verify that no IPCS user is accessing the sysplex dump directory.

Establishing a larger sysplex dump directory

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

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

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

   ```
   EXEC 'SYS1.SBLSCLI0(BLSCDDIR)'
   'DSNAME(SYS1.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. Update BLSCUSER with the new dump directory name (but make note of the old dump directory name).
3. Recycle the DUMPSRV address space (CANCEL DUMPSRV; it restarts automatically). This action registers the new dump directory name to DUMPSRV.
4. Run BLSJPRMI (START BLSJPRMI). This action updates the in-storage copy of the dump directory name.
5. 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)
   ```

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

Ensuring that CEA is active

The Incident Log task requires that the common event adapter (CEA) component be active on your z/OS system. The CEA address space is started automatically during IPL. If your installation has stopped CEA, it is recommended that you restart it. Otherwise, the Incident Log task will not be operational.

To verify that CEA is active, enter the following command:

```
D A,CEA
```

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
```

Ensuring that System REXX is active

For full functionality, the Incident Log task requires that the System REXX (SYSREXX) component be active on your z/OS system. 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.

Verify that System REXX is active by entering the following command:

```
D A,AXR
```

If the AXR address space is active on the z/OS host system, the System REXX component is active.

To start the SYSREXX component, enter the following command from the operator console:

```
START AXRPSTRT
```

The z/OSMF configuration process, described in Chapter 3, "Configuring z/OSMF," on page 25, does not require SYSREXX to be active. If you defer this step, however, the installation verification program (IVP) described in "Step 5: Complete the setup" on page 35 fails any tests that require an active SYSREXX component.

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 19 on page 167 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 19. 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.

Authorizing the SYS1.MIGLIB data set

SYS1.MIGLIB must be APF-authorized to allow AMATERSE to be called by System REXX execs, which are authorized.

To determine whether SYS1.MIGLIB is authorized, enter the following command:

```
D PROG,APF,DSNAME=SYS1.MIGLIB
```

To APF-authorize SYS1.MIGLIB, enter the following command:

```
SETPROG APF,ADD,DSNAME=SYS1.MIGLIB,VOLUME=xxxxx
```

where *xxxxx* is the volume serial (VOLSER).

Appendix B. Viewing 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 20 shows portions of an example of z/OSMF server side log data.

```
2009-04-29T18:38:51.285Z|00000012|com.ibm.zoszmf.util.eis.cim.ccp.CimClientPool|getWBEMClient(Endpoint, String,
Set<Locale>) INFO:IZUG911I: Connection to "http://null:5988" cannot be established, or was lost and cannot be
re-established using protocol "CIM" .
com.ibm.zoszmf.util.eis.EisConnectionException: IZUG911I: Connection to "http://null:5988" cannot be established,
or was lost and cannot be re-established using protocol "CIM" .
   com.ibm.zoszmf.util.eis.EisException.getEisException(EisException.java:145)
   com.ibm.zoszmf.util.eis.EisException.diagnoseAndThrow(EisException.java:221)
   com.ibm.zoszmf.util.eis.cim.ccp.CimClientPool.getWBEMClient(CimClientPool.java:279)

          o
          o
          o

+-> javax.wbem.WBEMException: JNI Exception type CannotConnectException:
   Cannot connect to local CIM server. Connection failed.
   org.sblim.cimclient.internal.jni.pegasus.CimReturnBuffer.getWBEMException(CimReturnBuffer.java:1244)
   org.sblim.cimclient.internal.jni.pegasus.NativeCimClient.verifyResult(NativeCimClient.java:1834)

          o
          o
          o

[tx0000000000000017:pegadm@IBM-FF0E8EC4FCB.pok.ibm.com (GET) /zosmf/pdw/PdwServiceServlet/
Incidents?filters=IncidentTime(FROM1240704000000)&dojo.preventCache=1241030163470]
```

Figure 20. Portion of a z/OSMF server side log data

As shown in Figure 20, each log record begins with a line divided by 'pipe' (|) characters into the following components:

- Timestamp in ISO8601 format, set to UTC timezone. Example: `2009-03-10T18:04:08.051Z`
- Thread ID as an 8 digit hex number. Example: `00000010`
- Class name. Example: `com.ibm.zoszmf.util.eis.cim.ccp.CimClientPool`
- Method name. Example: `getClient(Endpoint, String)`.

The next line of a log record contains the logging level, followed by a colon, followed by the message text. Messages logged at level INFO, WARNING, or SEVERE begin with an eight character message ID at the start of the message text. Message IDs that begin with "IZU" are part of the z/OSMF product. For descriptions of these messages, see Chapter 7, "Messages for z/OSMF," on page 107.

If the log record includes an exception, the exception is logged next. The exception class is logged, followed by a colon, followed by the message text of the exception. The lines following this make up the traceback information embedded in the exception, which is useful first-failure data capture. If the exception has attached causes, each cause is also logged with "+->" indicating the start of an attached cause.

The last line in every log record is contained in square brackets. If the log record is written during a specific user's context, information about that context is logged as follows:

- ″Transaction ID″. An internal counter value that applies to all actions between a specific set and clear of a context. This identifier begins with "tx", followed by a sixteen digit hex ID, and ends with a colon ':'.
- Remote user name (null for a guest user). This value is followed by an 'at' symbol (@).
- Remote host name. This value is followed by a space.
- Servlet ″verb″ is next, contained in parenthesis. Examples include GET and POST.
- URL of the request and query string, ending with the closing square bracket ']'.

If the log record is created during an initialization sequence, the transaction ID is printed and the user name is listed as "*bootstrap*". No other data are provided.

If the log record is created with no known context, only ″[tx:]″ appears on the last line.

Viewing client side log data

Included with the server statistics in the z/OSMF logs are client side data, which are used to monitor the JavaScript activity of each user login session. Client side log data differs in format from server side log data, as shown in Figure 21.

```
[tx0000000000000ED5:debug2@9.10.83.13 (POST) /zosmf/IzuUICommon/UILoggerServlet?preventCache=1243956783360]
2009-06-02T15:37:51.933Z|0000001A|com.ibm.zoszmf.util.log.servlet.UILoggerServlet|UILoggerServlet::doPost()
SEVERE: [2009-06-02T15:36:47.047Z] IZUG802E: An error occurred. Error: "makeTree error: Error: timeout exceeded"
[tx0000000000000ED8:debug2@9.10.83.13 (POST) /zosmf/IzuUICommon/UILoggerServlet?preventCache=1243956783360]
2009-06-02T15:37:52.020Z|0000001A|com.ibm.zoszmf.util.log.servlet.UILoggerServlet|UILoggerServlet::doPost()
SEVERE: [2009-06-02T15:36:47.203Z] IZUG802E: An error occurred. Error: "makeTree error: Error: timeout exceeded"
[tx0000000000000ED9:debug2@9.10.83.13 (POST) /zosmf/IzuUICommon/UILoggerServlet?preventCache=1243956783360]
```

Figure 21. 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 square brackets [ ]
- Browser name and level
- ENTRY or RETURN, to indicate the beginning or the end of a routine
- Package name, such as AuthorizationServices
- Module name, such as util.ui.messages.Message.js
- Method name, such as _getMessageType()
- Detailed message.

Appendix C. izusetup.sh script

z/OSMF provides a front end interactive script, called **izusetup.sh**, that you use to configure the product on your z/OS system. This script, when used with a number of different options, sets up and deploys a working instance of the product in your z/OS system. You can run this script from an OMVS or telnet/rlogin session. You cannot run the script from ISHELL.

Format

```
izusetup.sh -file <pathname/filename.cfg> -config [-system <SystemName>]
[-overridefile <overridefilename>] [-fastpath]

izusetup.sh -file <pathname/filename.cfg> -verify racf|core|log|all

izusetup.sh -file <pathname/filename.cfg> -prime

izusetup.sh -file <pathname/filename.cfg> -finish
```

Figure 22. izusetup.sh syntax

Required parameters

Include the `-file` parameter, which specifies the fully-qualified name of the file that the **izusetup.sh** script is to use the configuration file. The fully-qualified name includes the directory path to the file, and the file name. If this file exists, the script will use it. Otherwise, the script creates this file (by default, in the directory `/etc/zosmf`).

You must also specify one of the following parameters, which identify the particular operation that the **izusetup.sh** script is to perform. You cannot specify more than one of these operations on the same invocation.

-config
This parameter indicates that you want the script to collect configuration input and produce a REXX exec with sample RACF commands for setting up security. The script also creates and mounts the z/OSMF data file system if it does not already exist.

-verify
This parameter indicates that you want to verify the configuration of z/OSMF. To indicate the scope of this verification, specify -verify with one of the following options:

racf Verify the RACF security setup for all configured tasks and functions.

core Verify the RACF security setup for the core functions only.

log Verify the RACF security setup and the z/OS system customization for the Incident Log task only. See Table 1 on page 10.

all Verify the RACF security setup and the z/OS system customization for all configured tasks and functions.

-prime
This parameter indicates that you want to initialize the z/OSMF data file system.

-finish
This parameter indicates that you want to complete the configuration of the z/OSMF.

Optional parameters

The following optional parameters can only be specified with the `-config` parameter.

-system *SYSNAME*
This optional parameter indicates the system on which z/OSMF is to be configured. If you omit this value, the script will prompt you for it.

-overridefile *overridefilename*
This optional parameter indicates that you want to use the variable values that are specified in the override file, or in the configuration file. 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.

-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`.

Example

In the following example, the **izusetup.sh** script creates the configuration file `izuconfig1.cfg` in the directory `/etc/zosmf`.

```
izusetup.sh -file /etc/zosmf/izuconfig1.cfg -config
```

Appendix D. Default configuration file, and default override file variables

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.

Some values require that you provide a unique UID or GID. Instead of specifying these identifiers, you can specify the AUTOUID or AUTOGID operand (as appropriate) to have RACF automatically generate a unique ID for you. For more information about AUTOUID and AUTOGID, see *z/OS Security Server RACF Security Administrator's Guide*.

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 `/usr/lpp/zosmf/V1R11/defaults` directory.

Table 18. Default configuration file

Variable name	Default value	Description
IZU_ADMIN_NAME	ZOSMFAD	User ID for the z/OSMF administrator.
IZU_ADMIN_REGION	2096128	Region size for z/OSMF administrator identity.
IZU_ADMIN_UID	9001	UID for the z/OSMF administrator.
IZU_ADMIN_GROUP	ZOSMFGRP	Primary group for z/OSMF administrator identity.
IZU_ADMIN_GROUP_GID	9003	Group ID (GID) for the z/OSMF administrator group.
IZU_ADMIN_HOME	/u/zosmfad	Home directory for the z/OSMF administrator. Do not specify a home directory to be created under the mount point of the z/OSMF data file system, which by default is `/var/zosmf/data`. The mount point owner and group permissions do not allow the z/OSMF administrator ID access.
IZU_ADMIN_PROGRAM	/bin/sh	Program path for the z/OSMF administrator identity for z/OS UNIX system services.
IZU_WAS_CONFIG_FILE_KNOWN	Y	The WebSphere Application Server response file, which was created when you configured IBM WebSphere Application Server OEM Edition for z/OS on this system, exists and is available to be used as input to the IBM z/OS Management Facility process. This file is described in *IBM WebSphere Application Server OEM Edition for z/OSIBM WebSphere Application Server OEM Edition for z/OS Configuration Guide, Version 7.0*, GA32-0631.

Table 18. Default configuration file (continued)

Variable name	Default value	Description
IZU_WAS_CONFIG_FILE_LOCATION	/etc/zWebSphereOEM/V7R0/conf/CONFIG1/CONFIG1.responseFile	Full pathname of the WebSphere Application Server response file. Your installation created this file when customizing IBM WebSphere Application Server OEM Edition for z/OS for this system.
IZU_WAS_PROFILE_PREFIX	BBNBASE	WebSphere SAF profile prefix.
IZU_CLUSTER_TRANSITION_NAME	BBNC001	WebSphere cluster transition name.
IZU_APPSERVER_GROUP	WSCFG1	WebSphere application server group.
IZU_APPSERVER_ROOT	/zWebSphereOEM/V7R0/config1	WebSphere root directory path of the application server.
IZU_CELL_SHORT_NAME	BBNBASE	WebSphere application server cell short name.
IZU_CONTROL_USERID	WSCRU1	WebSphere application server control region user ID.
IZU_SERVANT_USERID	WSSRU1	WebSphere application server servant region user ID.
IZU_WBEM_ROOT	/usr/lpp/wbem	Root directory path of the CIM server installation.
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_SIZE	100	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_DATA_FS_VOLUME	'*'	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_CODE_ROOT	/usr/lpp/zosmf/V1R11	z/OSMF product file system that was created earlier when you ran the jobs described in the z/OSMF Program Directory.
IZU_DATA_DIR	/var/zosmf/data	Mount point (the full pathname) for the z/OSMF data file system.
IZU_CONFIG_DIR	/etc/zosmf	Mount point (the full pathname) for the z/OSMF configuration file system.
IZU_CIM_GROUP_NAME	CIMGP	CIM group name.
IZU_CIM_GROUP_ID	5321	CIM group GID for the CIM group admin identity.
IZU_CEA_UID	9002	Common event adapter (CEA) UID.
IZU_CEA_GROUP_NAME	CEAGP	Group name to use for allowing the Incident Log task to access CEA functions.
IZU_CEA_GROUP_ID	6321	CEA group GID to use for the CEA group administrator identity.
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.

Table 18. Default configuration file (continued)

Variable name	Default value	Description
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_PARMLIB	SYS1.PARMLIB	Target parmlib data set that will contain the newly created members for Incident Log processing (IEADMC*nn* and CEAPRM*nn*).
IZU_PARMLIB_SOURCE	SYS1.PARMLIB	Source parmlib 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_INCIDENT_LOG	Y	Do you want to configure the Incident Log task?
IZU_CIM_SETUP	N	Is the Common Information Model (CIM) server been configured already?
IZU_CIM_ADMIN_NAME	ZOSMFAD	CIM administrator user ID for your installation.
IZU_SYSNAME_PREFIX	@SYSNAME	Name of your z/OS system (up to 8 characters).
IZU_ADMIN_PROC	NO.DEFAULT.VALUE	TSO/E logon procedure to be used by the z/OSMF administrator.
IZU_ADMIN_ACCOUNT	NO.DEFAULT.VALUE	User account number for z/OSMF administrator identity.
IZU_COUNTRY_CODE	NO.DEFAULT.VALUE	IBM-defined country code for your site (3-character numeric).
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. • V indicates that the script is to prompt for up to seven volumes • S indicates that the script is to prompt for a single storage class name.

Default override file

The default override response file, izudflt.ovr, is the last configuration file to be processed. Therefore, you can use this file to:

- Override values in the default configuration file (izudflt.cfg) without directly modifying the default configuration file.
- Make variable substitutions.

This file is located in the `/usr/lpp/zosmf/V1R11/defaults` directory.

Figure 23 on page 176 shows the content of the override file that is supplied with z/OSMF.

```
IZU_ADMIN_NAME=ZOSMFAD
IZU_ADMIN_REGION=2096128
IZU_ADMIN_UID=9001
IZU_ADMIN_GROUP=ZOSMFGRP
IZU_ADMIN_GROUP_GID=9003
IZU_ADMIN_HOME=/u/zosmfad
IZU_ADMIN_PROGRAM=/bin/sh
IZU_WAS_CONFIG_FILE_KNOWN=Y
IZU_WAS_CONFIG_FILE_LOCATION=/etc/zWebSphereOEM/V7R0/conf/CONFIG1/CONFIG1.responseFile
IZU_DATA_FS_NAME=IZU.SIZUDATA
IZU_DATA_FS_TYPE=ZFS
IZU_DATA_FS_SIZE=100
IZU_DATA_FS_VOLUME='*'
IZU_DATA_DIR=/var/zosmf/data
IZU_CONFIG_DIR=/etc/zosmf
IZU_CIM_GROUP_NAME=CIMGP
IZU_CIM_GROUP_ID=5321
IZU_CEA_UID=9002
IZU_CEA_GROUP_NAME=CEAGP
IZU_CEA_GROUP_ID=6321
IZU_CEA_PARM_NAME=01
IZU_IEA_PARM_NAME=ZM
IZU_PARMLIB=SYS1.PARMLIB
IZU_PARMLIB_SOURCE=SYS1.PARMLIB
IZU_INCIDENT_LOG=Y
IZU_CIM_SETUP=N
IZU_CIM_ADMIN_NAME=ZOSMFAD
IZU_SYSNAME_PREFIX=@SYSNAME
IZU_ADMIN_PROC=NO.DEFAULT.VALUE
IZU_ADMIN_ACCOUNT=NO.DEFAULT.VALUE
IZU_COUNTRY_CODE=NO.DEFAULT.VALUE
IZU_BRANCH_CODE=NO.DEFAULT.VALUE
IZU_STORAGE_VALUE=NO.DEFAULT.VALUE
#IZU_STORAGE_VALUE="STORCLAS(STRCLS)"
#IZU_STORAGE_VALUE="VOLSER(VOL1,VOL2,VOL3,VOL4,VOL5,VOL6,VOL7)"
```

Figure 23. Default override file

As shown in Figure 23, the STORCLAS and VOLSER values must be enclosed in double quotes.

Appendix E. Modifying values for the WebSphere configuration

Experienced installers of WebSphere Application Server for z/OS: You can update several WebSphere settings in file **izuadmin.env** if the default values are not acceptable for your environment. In most cases, you should not need to change these values.

You can modify values for the following settings:

ltpatimeout
LTPA timeout value for forwarded credentials between servers; the z/OSMF default is 490 minutes. A z/OSMF user's session will expire after this period of time has elapsed (see "Re-authenticating in z/OSMF" on page 51).

ltpacachetimeout
Authentication cache settings cache timeout; the z/OSMF default is 29400 seconds.

sessiontimeout
Session management session timeout; the z/OSMF default is 495 minutes.

The z/OSMF configuration process obtains the values for these settings from the file **izuadmin.env**. If this file exists in the z/OSMF configuration file directory `/etc/zosmf`, the script uses that file. Otherwise, z/OSMF obtains the values from the **izuadmin.env** file in the z/OSMF product defaults directory:

```
/usr/lpp/zosmf/V1R11/defaults
```

To override any of these setting values, use this procedure:

1. Copy the file **izuadmin.env** from the directory `/usr/lpp/zosmf/V1R11/default` to the directory `/etc/zosmf`
2. Edit the `/etc/zosmf/izuadmin.env` file and update the setting values to be changed. Only the following settings are located in izuadmin.env: **ltpatimeout**, **ltpacachetimeout**, and **sessiontimeout**.

To have your changes to the WebSphere settings take effect, make the changes before running the script described in "Step 5: Complete the setup" on page 35. If you modify the WebSphere settings after running the script, there is no effect on your WebSphere Application Server configuration. You must re-run the configuration script to have an effect.

Attention: If you modify any of the core setup updates (see Table 19) directly in the WebSphere Application Server configuration, for example, through the WebSphere Administrative console, z/OSMF might not function properly.

Table 19. WebSphere Application Server updates done by the core configuration script

IBM WebSphere Application Server OEM Edition for z/OS configuration update	Notes
The enterprise application 'IzuManagementFacility' is deployed to the application server.	Not applicable.

Table 19. WebSphere Application Server updates done by the core configuration script (continued)

IBM WebSphere Application Server OEM Edition for z/OS configuration update	Notes
A shared library named 'IzuAppLibs' is defined and a reference to it is created from the 'IzuManagementFacility' enterprise application.	Not applicable.
A shared library named 'IzuSrvLibs' is defined and a reference to it is created from the application server.	Not applicable.
An environment entry named 'IZU_DATA_DIR' is created in the servant process that defines the z/OSMF data file system.	Not applicable.
An environment entry named 'IZU_WBEM_ROOT' is created in the Servant process that defines the CIM server root directory.	Not applicable.
A JVM environment entry named 'LIBPATH' is created in the Servant process to include the required libraries for z/OSMF.	Not applicable.
Application server is set to run in 64 bit mode	IBM WebSphere Application Server OEM Edition for z/OS default. Update details: • Substitution Variable 'JAVA_HOME' is set to '${WAS_HOME}/java64'. • Control process environment entry 'was.com.ibm.websphere.zos.jvmmode' is set to '64bit'. • Control process attribute 'startCommandArgs' is set to include 'AMODE=64'. • Servant process attribute 'startCommandArgs' is set to include 'AMODE=64'. • Adjunct process attribute 'startCommandArgs' is set to include 'AMODE=64'.
'Enable administrative security' is checked in the global security configuration.	IBM WebSphere Application Server OEM Edition for z/OS default. Update details: Security setting 'enabled' is set to 'true'.
'Use Java 2 security to restrict applications to local resources' is not checked.	IBM WebSphere Application Server OEM Edition for z/OS default. Update details: Security setting 'enforceJava2Security' is set to 'false'.

Table 19. WebSphere Application Server updates done by the core configuration script (continued)

IBM WebSphere Application Server OEM Edition for z/OS configuration update	**Notes**
'Authenticate only when the URI is protected' is checked in the Web security general settings	IBM WebSphere Application Server OEM Edition for z/OS default. Update details: Setting 'com.ibm.wsspi.security.web.webAuthReq' is set to 'persisting'.
'Enable application security' is checked in the global security configuration.	Update details: Security setting 'appEnabled' is set to 'true'.
'Use available authentication data when an unprotected URI is accessed' is checked in the Web security general settings.	Update details: Setting 'com.ibm.wsspi.security.web.webAuthReq' is set to 'persisting'.
'Enable application server and z/OS thread identity synchronization' is checked in the z/OS security options.	Update details: Security setting 'was.security.EnableSyncToOSThread' is set to 'true'.
Allow multiple language encoding support.	Update details: Servant JVM Property 'client.encoding.override' is set to 'UTF-8'.
'LTPA timeout value for forwarded credentials between servers' is set to the value specified in izuadmin.env.	Default in izuadmin.env is 490 minutes. Update details: LTPA setting 'timeout' is set.
'Authentication cache settings cache timeout' is set to the value specified in izuadmin.env.	Default in izuadmin.env is 29400 seconds. Update details: Security setting 'cacheTimeout' is set.
'Session management sSession timeout' is set to the value specified in izuadmin.env.	Default in izuadmin.env is 495 minutes. Update details: Tuning parameter 'invalidationTimeout' is set.
The following log level details are added: com.ibm.zoszmf.environment.ui=finer: com.ibm.zoszmf.*=INFO	

Appendix F. Common event adaptor (CEA) security profiles

The common event adapter (CEA) component of z/OS has security profiles for protecting different portions of its processing.

The RACF command exec created by the z/OSMF configuration process (see "Step 2: Run the security commands" on page 31) provides CEA group access to CEA.CEAPDWB* in the SERVAUTH class.

Table 20 shows the profiles that are included in this group.

Table 20. CEA security profiles

Security Profile	Corresponding CEA function
CEA.CEAPDWB.CEAGETINCIDENTCOLLECTION	Obtain collection of incident data for all incidents matching a filter.
CEA.CEAPDWB.CEADELETEINCIDENT	Delete selected Incidents, including the dumps, all diagnostic snapshot files and the corresponding sysplex dump directory entry.
CEA.CEAPDWB.CEAGETINCIDENT	Obtain data associated with a specific incident.
CEA.CEAPDWB.CEAPREPAREINCIDENT	Prepare data for FTP (locate and compress/terse).
CEA.CEAPDWB.CEASETPROBLEMTRACKINGNUMBER	Set a problem ID (such as a PMR number) or problem management tracking ID.
CEA.CEAPDWB.CEAUNSUPPRESSDUMP	Allow dump related to and incident, marked for suppression by DAE to be taken.
CEA.CEAPDWB.CEACHECKSTATUS	Check status and return incident information.
CEA.CEAGETPS	Obtain job information. Used by Incident Log FTP processing.
CEA.CEADOCMD	Cancel job. Used by Incident Log FTP processing.
CEA.CEADOCONSOLECMD *	Allow the IVP to issue operator commands to accomplish its function.

Appendix G. 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.

Table 21 describes the configuration-related CEA reason codes and includes a cross-reference of reason codes to CIM messages and z/OSMF messages. Where an associated z/OSMF message is indicated, check the z/OSMF message for more information about resolving the error. By default, CEA reason codes without an associated z/OSMF message are accompanied by z/OSMF message IZUP631E.

Table 21. Common event adapter (CEA) reason codes

Reason code (hex)	Description	System programmer action	CIM message	Associated z/OSMF message	IBM service information
100	CEA address space is not running.	Follow the steps in "Ensuring that CEA is active" on page 165.	CEZ05002E	IZUP634E	CEAUNAVAIL
121	CIM indication processing is unavailable because the CEA address space is running in MIN mode. To support Incident Log processing, CEA must be run in FULL mode.	Use the MODIFY CEA,MODE command to adjust the CEA mode of operation to FULL mode. To do so, enter the following command from the operator console: `F CEA,MODE=FULL` z/OS UNIX System Services must be available for CEA to be transitioned into FULL mode.	CEZ05013E		CEAFORCEMINMODE
32D	User is not authorized for this request.	Define the appropriate authority for the user. See "Creating commands to authorize a user to all tasks" on page 40.	CEZ05003E	IZUP635E	CEANOINSTRAUTH
33E	Abend occurred in the CEA task that interacts with the IPCS environment.	Report the problem to IBM Support.	CEZ05001E	IZUP639E	CEAIPRQServerAbended
342	Sysplex dump directory is empty.	Ensure that the sysplex dump directory is not empty.			CEASDDIREMPTY
343	Dump incident was not found. Most likely, the incident was deleted by another user.	No action is required.	CEZ05004E	IZUP636E	CEAADDFAILED

Table 21. Common event adapter (CEA) reason codes (continued)

Reason code (hex)	Description	System programmer action	CIM message	Associated z/OSMF message	IBM service information
352	Dump analysis and elimination (DAE) data set name (typically SYS1.DAE) could not be determined. Most likely, DAE is not configured or is not running. Or, the user attempted to unsuppress a dump without having write access to the DAE data set.	Ensure that: • DAE is active. • DAE is configured, as described in *z/OS MVS Diagnosis: Tools and Service Aids*. • User has write access to the active DAE data set. For more information, see "Configuring dump analysis and elimination" on page 162.		IZUP637E	CEADAEDSNNOTAvailable
357	Could not generate a prepared DSN.	Verify that the compiled REXX exec CEACDMPP exists and can be run by System REXX.			CEAGENPREPAREDDSNFAIL
358	Error was encountered when invoking a REXX exec. Typically, this error occurs when the SYS1.MIGLIB data set is not APF-authorized (is not defined in the PROGxx parmlib member). If so, this reason code is accompanied by message CEZ05000E with the following codes (in decimal): • DIAG1=12 • DIAG2=25 • DIAG3=774.	Follow the steps in "Authorizing the SYS1.MIGLIB data set" on page 167.	CEZ05000E	IZUP639E	CEAREXENVERROR
359	Internal CEA error occurred when attempting to invoke a SYSREXX exec.	If this reason code is accompanied by the following codes (in decimal), check the SYSREXX concatenation for a missing exec: • DIAG=8 • DIAG2=851. Also, check message CEZ05000E in SYSLOG. CEAERRO_Msg contains the name of the SYSREXX exec.	CEZ05000E		CEAREXXERROR
365	System REXX address space or the functions it provides are not available.	Follow the steps in "Ensuring that System REXX is active" on page 166.	CEZ05005E	IZUP640E	CEASYSREXXNOTACTIVE

Table 21. Common event adapter (CEA) reason codes (continued)

Reason code (hex)	Description	System programmer action	CIM message	Associated z/OSMF message	IBM service information
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 active" on page 166.	CEZ05006E	IZUP643E	CEASYSREXXBAD ENVIRONMENT
367	System REXX cannot process the exec at this time.	Try the request again later.	CEZ05007W	IZUP644E	CEAEXECTIMEOUT
368	System REXX cannot schedule the exec to run at this time.	Try the request again later.	CEZ05008W	IZUP645E	CEASYSREXXOVERLOADED
36E	SYS1.MIGLIB is not APF-authorized, which is preventing REXX execs from being invoked.	Follow the steps in "Authorizing the SYS1.MIGLIB data set" on page 167.	CEZ05009E		CEAMIGLIBNOTAPFAUTH
36F	User is not authorized to view OPERLOG snapshot information.	Perform the corrective action described in "User is not SAF authorized" on page 90.	CEZ05010E		CEANOSAFOPERLOGSNAP
370	System logger 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 156. For information about the IXGCON macro, see *z/OS MVS Authorized Assembler Services Reference EDT-IXG*, which is available online in the IBM z/OS Internet Library.	CEZ05011E		CEALOGGERNOTAVAIL
371	When preparing incident materials to be sent through FTP, a function could not allocate a new data set for the tersed diagnostic snapshot.	Look for system messages indicating why the failure occurred in the CIM trace associated with the failed return code. For assistance, contact IBM Support.			CEATERSEBADALLOC1

Table 21. Common event adapter (CEA) reason codes (continued)

Reason code (hex)	Description	System programmer action	CIM message	Associated z/OSMF message	IBM service information
372	The function that prepares an incident to be sent through FTP was unable to 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.			CEATERSEBADALLOC1
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. Also, see "Incidents have only dumps associated with them, no other diagnostic logs" on page 100.			CEANOSNAPSHOT
378	No log data was accumulated in diagnostic snapshot.	If this problem occurs frequently, adjust the DUMPCAPTURETIME setting in the CEAPRMxx parmlib member.			CEAPDWBDIAGDATAEMPTY
379	Incorrect format or value was supplied for the IBM PMR number.	Correct the IBM PMR number and try again. The format of the IBM PMR number should be *nnnnn.ccc.bbb* where *nnnnn* is the PMR number, *bbb* is the branch code, and *ccc* is the country code.			CEAWRONGIBMPMR FORMAT
37D	Attempt to obtain the enqueue on the sysplex dump directory failed; another program already holds the enqueue.	• Ensure that only one user is attempting to access the dump information at one time. To check for enqueue contention, enter the following command at the operator console: `D GRS` • Wait for the enqueue to be released and try again.	CEZ05017E	IZUP641E	CEAIPCSENQERROR
37E	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 163.	CEZ05016E	IZUP642E	CEASDDIROPENERROR
382	Component table is corrupted.	Report the problem to IBM Support.			CEAXMLTAGSTOODEEP

Table 21. Common event adapter (CEA) reason codes (continued)

Reason code (hex)	Description	System programmer action	CIM message	Associated z/OSMF message	IBM service information
385	Diagnostic data being sent is currently in use.	Try the request again later.			CEAPREPAREOBJINUSE
386	Diagnostic data being sent is currently in use.	Try the request again later.			CEAPREPAREENQERR
38C	The sysplex dump directory (default name SYS1.DDIR) has no space available to record new SVC dumps.	See "Establishing a larger sysplex dump directory" on page 165.			CEACKSTINVALIDALLOC VALUE

Appendix H. Security exec examples

The contents of the **izuconfig1.cfg.rexx** exec depends on whether your installation has selected to configure the Incident Log task, and, if so, whether to configure the CIM server or use an existing CIM server configuration.

For your reference, this topic contains the sample REXX output that would be created for each of these possible scenarios.

Example 1: Core functions only

Figure 24 shows an example of the REXX file created for configuring the z/OSMF core functions only.

```
/* Create the z/OSMF Administrator default group */
Call RacfCmd "ADDGROUP ZOSMFGRP OMVS(GID(9003))"

/* Create the z/OSMF Administrator UserID */
/* The home directory is created in the -prime step.  If automount managed, pre-create it before */
/* the -prime step */

Call RacfCmd "ADDUSER ZOSMFAD DFLTGRP(ZOSMFGRP) OMVS(UID(9001) HOME(/u/zosmfad) PROGRAM(/bin/sh))"

Call RacfCmd "ALU ZOSMFAD TSO(PROC(OMVS1234) ACCTNUM(IZU123) SIZE(2096128))"

Call RacfCmd "ALU ZOSMFAD NOPASSWORD"

/* Connect the z/OSMF Administrator UserID to the Application Server Group */
Call RacfCmd "CONNECT ZOSMFAD GROUP(WSCFG1)"

/* Connect the z/OSMF Administrator UserID to Core */
/* Assumption APPL class has been defined, activated, and raclisted as part of WebSphere */
/* Application Server OEM setup. */
Call RacfCmd "PERMIT BBNBASE CLASS(APPL) ID(ZOSMFAD) ACCESS(READ)"
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"

/* Assumption EJBROLE is defined, activated, and raclisted. */
Call RacfCmd "RDEFINE EJBROLE BBNBASE.izuUsers UACC(NONE)"
Call RacfCmd "PERMIT BBNBASE.izuUsers CLASS(EJBROLE) ID(ZOSMFAD) ACCESS(READ)"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"

/* SyncToOSThread permits */
/* Assumption BBO.SYNC.XXXXXX.YYYYYY facility class has been defined, activated, and raclisted */
/* as part of WebSphere Application Server OEM setup. */
/* Call RacfCmd "RDEFINE FACILITY BBO.SYNC.BBNBASE.BBNC001 UACC(NONE) " */
Call RacfCmd "PERMIT BBO.SYNC.BBNBASE.BBNC001 CLASS(FACILITY) ID(WSCRU1) ACC(READ)"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"

/* Assume SURROGAT class was defined.  It is shipped with z/OS. */
Call RacfCmd "RDEFINE SURROGAT BBO.SYNC.ZOSMFAD UACC(NONE)"
Call RacfCmd "SETROPTS CLASSACT(SURROGAT)"
Call RacfCmd "PERMIT BBO.SYNC.ZOSMFAD CLASS(SURROGAT) ID(WSSRU1) ACCESS(READ)"
/* If SURROGAT was previously RACLISTed use the one below. If not comment the one below and */
/* uncomment the one after */
Call RacfCmd "SETROPTS RACLIST(SURROGAT) REFRESH"
/* Call RacfCmd "SETROPTS RACLIST(SURROGAT)" */

/*-------------------------------------------------------------------- */
/* Step 1 Setup for Multi-Layer Security (MLS)                    */
/* This step is only necessary if the installation is                 */
/* already using MLS. Otherwise, it can be skipped.                   */
/*--------------------------------------------------------------------*/
/*Call RacfCmd "ALTUSER ZOSMFAD  SECLABEL(SYSMULTI)"*/
/*Call RacfCmd "PERMIT SYSMULTI CLASS(SECLABEL) ID(ZOSMFAD) ACCESS(READ)"*/
```

Figure 24. Sample RACF commands for securing the z/OSMF core functions only

Example 2: All functions and tasks but without configuring CIM

If your installation has chosen to configure the Incident Log task, and is using an existing CIM server configuration, the **izuconfig1.cfg.rexx** exec creates the security definitions for CEA and the other system components used in Incident Log processing. An example of this REXX output is shown in Figure 25 and Figure 26 on page 191.

```
/* Create the z/OSMF Administrator default group */
Call RacfCmd "ADDGROUP ZOSMFGRP OMVS(GID(9003))"

/* Create the group that will be used to access CEA resources */
Call RacfCmd "ADDGROUP CEAGP OMVS(GID(6321))"

/* Create the z/OSMF Administrator UserID */
/* The home directory is created in the -prime step.  If automount managed, pre-create it before the -prime step */

Call RacfCmd "ADDUSER ZOSMFAD DFLTGRP(ZOSMFGRP) OMVS(UID(9001) HOME(/u/zosmfad) PROGRAM(/bin/sh))"

Call RacfCmd "ALU ZOSMFAD TSO(PROC(OMVS1234) ACCTNUM(IZU123) SIZE(2096128))"

Call RacfCmd "ALU ZOSMFAD NOPASSWORD"

/* Connect the z/OSMF Administrator UserID to the Application Server Group */
Call RacfCmd "CONNECT ZOSMFAD GROUP(WSCFG1)"

/* Connect the z/OSMF Administrator UserID to Core */
/* Assumption APPL class has been defined, activated, and raclisted as part of WebSphere Application Server OEM setup. */
Call RacfCmd "PERMIT BBNBASE CLASS(APPL) ID(ZOSMFAD) ACCESS(READ)"
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"

/* Assumption EJBROLE is defined, activated, and raclisted. */
Call RacfCmd "RDEFINE EJBROLE BBNBASE.izuUsers UACC(NONE)"
Call RacfCmd "PERMIT BBNBASE.izuUsers CLASS(EJBROLE) ID(ZOSMFAD) ACCESS(READ)"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"

/* SyncToOSThread permits */
/* Assumption BBO.SYNC.XXXXXX.YYYYYY facility class has been defined, activated, and raclisted as part of */
/* WebSphere Application Server OEM setup. */
/* Call RacfCmd "RDEFINE FACILITY BBO.SYNC.BBNBASE.BBNC001 UACC(NONE) " */
Call RacfCmd "PERMIT BBO.SYNC.BBNBASE.BBNC001 CLASS(FACILITY) ID(WSCRU1) ACC(READ)"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"

/* Assume SURROGAT class was defined.  It is shipped with z/OS. */
Call RacfCmd "RDEFINE SURROGAT BBO.SYNC.ZOSMFAD UACC(NONE)"
Call RacfCmd "SETROPTS CLASSACT(SURROGAT)"
Call RacfCmd "PERMIT BBO.SYNC.ZOSMFAD CLASS(SURROGAT) ID(WSSRU1) ACCESS(READ)"
/* If SURROGAT was previously RACLISTed use the one below. If not comment the one below and */
/* uncomment the one after */
Call RacfCmd "SETROPTS RACLIST(SURROGAT) REFRESH"
/* Call RacfCmd "SETROPTS RACLIST(SURROGAT)" */

/* Connect the z/OSMF Administrator UserID to the CEA group */
Call RacfCmd "CONNECT ZOSMFAD GROUP(CEAGP)"
Call RacfCmd "PERMIT CIMSERV CLASS(WBEM) ACCESS(CONTROL) ID(ZOSMFAD)"
/* Assumption WBEM class has already been raclisted. */
Call RacfCmd "SETROPTS RACLIST(WBEM) REFRESH"
Call RacfCmd "RDEFINE SURROGAT BPX.SRV.ZOSMFAD UACC(NONE)"
Call RacfCmd "PERMIT BPX.SRV.ZOSMFAD CL(SURROGAT) ID(ZOSMFAD) ACCESS(CONTROL)"
/* Assumption SURROGAT has been raclisted.  If not comment out line below and uncomment the */
/* one underneath it */
Call RacfCmd "SETROPTS RACLIST(SURROGAT) REFRESH"
/* Call RacfCmd "SETROPTS RACLIST(SURROGAT)" */

/* Setup the z/OSMF Administrator UserID to CEA and CIM */
/*-------------------------------------------------------------------- */
/* Step 1 Setup the Common Event Adapter (CEA) Support                */
/* Define the CEA UserID with UNIX System Services support.               */
/*--------------------------------------------------------------------*/
Call RacfCmd "ADDUSER CEA DFLTGRP(SYS1) OMVS( UID(9002)  FILEPROCMAX(1024))"
Call RacfCmd "RDEFINE STARTED CEA.** STDATA(USER(CEA) GROUP(SYS1) TRACE(YES))"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
```

Figure 25. Sample RACF commands for authorizing core functions and Incident Log task, without CIM server setup requested (Part 1 of 2)

```
/*-------------------------------------------------------------------- */
/* Step 2 Setup for Multi-Layer Security (MLS)                    */
/* This step is only necessary if the installation is                 */
/* already using MLS. Otherwise, it can be skipped.                   */
/*--------------------------------------------------------------------*/
/*ALTUSER CEA SECLABEL(SYSMULTI) */
/*PERMIT SYSMULTI CLASS(SECLABEL) ACCESS(ALTER) ID(CEA) */
/*PERMIT SYSHIGH CLASS(SECLABEL) ACCESS(ALTER) ID(CEA) */
/*PERMIT SYSLOW CLASS(SECLABEL) ACCESS(ALTER) ID(CEA) */
/*ADDSD 'CEA.*' SECLABEL(SYSNONE) */

/*SETROPTS GENERIC(STARTED) REFRESH */
/*SETROPTS RACLIST(STARTED) REFRESH */
/*SETR CLASSACT(SECLABEL) */
/*SETR RACLIST(SECLABEL) REFRESH */

/*Call RacfCmd "ALTUSER ZOSMFAD  SECLABEL(SYSMULTI)"*/
/*Call RacfCmd "PERMIT SYSMULTI CLASS(SECLABEL) ID(ZOSMFAD) ACCESS(READ)"*/

/*-------------------------------------------------------------------- */
/* Step 3 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 CEAGroup, authority to the following and to grant access */
/* to perform JES operations and obtain job properties.               */
Call RacfCmd "PERMIT CEA.CEAGETPS CLASS(SERVAUTH) ID(CEAGP) ACCESS(UPDATE)"
Call RacfCmd "PERMIT CEA.CEADOCMD CLASS(SERVAUTH) ID(CEAGP) ACCESS(UPDATE)"

/* Permit CEAGroup to Incident Log */
Call RacfCmd "RDEFINE SERVAUTH CEA.CEAPDWB* UACC(NONE)"
Call RacfCmd "PERMIT CEA.CEAPDWB* CLASS(SERVAUTH) ID(CEAGP) ACCESS(UPDATE)"
Call RacfCmd "RDEFINE SERVAUTH CEA.CEADOCONSOLECMD UACC(NONE)"
Call RacfCmd "PERMIT CEA.CEADOCONSOLECMD CLASS(SERVAUTH) ID(CEAGP) 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"

/* ------------------------------------------------------------------ */
/* Step 4 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(ZOSMFAD) ACCESS(UPDATE)" */
/* Call RacfCmd "SETROPTS GENERIC(DATASET) REFRESH"                                      */

/* If your installation protects MVS commands with RACF class opercmds */
/* you need to give the admin identity permission.  This is required   */
/* for the incident log verify step.                                   */
/* Call RacfCmd "PERMIT MVS.** CLASS(OPERCMDS) ID(ZOSMFAD) ACCESS(CONTROL)" */
/* Call RacfCmd "SETROPTS RACLIST(OPERCMDS) REFRESH"                          */

/* If your installation sets up PROTECT-ALL (RACF exit to protect all datasets) */
/* you will need to setup a CEA.* RACF profile and permit CEA and user admin    */
/* identity.                                                                    */
/* Call RacfCmd "ADDSD 'CEA.*' UACC(NONE)"                                      */
/* Call RacfCmd "PERMIT 'CEA.*' ID(CEA) ACCESS(ALTER)"                          */
/* Call RacfCmd "PERMIT 'CEA.*' ID(ZOSMFAD) ACCESS(ALTER)"              */
/* Call RacfCmd "SETROPTS GENERIC(DATASET) REFRESH"                             */

/* After running this exec (yourConfigFileName.cfg.rexx), you must start the CIM server. */
/* Or, if the CIM server is already running, you must restart it.                  */
```

Figure 26. Sample RACF commands for authorizing core functions and Incident Log task, without CIM server setup requested (Part 2 of 2)

Example 3: All functions and tasks with CIM setup performed

If your installation has selected to configure the Incident Log task, and has allowed the script to configure the CIM server as part of the z/OSMF configuration process, the **izuconfig1.cfg.rexx** exec creates the security definitions for the CIM server, CEA, and the other system components that are used in Incident Log task processing.

An example of the REXX output is shown in Figure 27, Figure 28 on page 193, Figure 29 on page 194, and Figure 30 on page 195.

```
/* Create the z/OSMF Administrator default group */
Call RacfCmd "ADDGROUP ZOSMFGRP OMVS(GID(9003))"

/* Create the CIM group */
Call RacfCmd "ADDGROUP CIMGP OMVS(GID(5321))"

/* Create the group that will be used to access CEA resources */
Call RacfCmd "ADDGROUP CEAGP OMVS(GID(6321))"

/* Create the z/OSMF Administrator UserID */
/* The home directory is created in the -prime step.  If automount managed, pre-create it before the -prime step */

Call RacfCmd "ADDUSER ZOSMFAD DFLTGRP(ZOSMFGRP) OMVS(UID(9001) HOME(/u/zosmfad) PROGRAM(/bin/sh))"

Call RacfCmd "ALU ZOSMFAD TSO(PROC(OMVS1234) ACCTNUM(IZU123) SIZE(2096128))"

Call RacfCmd "ALU ZOSMFAD NOPASSWORD"

/* Connect the z/OSMF Administrator UserID to the Application Server Group */
Call RacfCmd "CONNECT ZOSMFAD GROUP(WSCFG1)"

/* Connect the z/OSMF Administrator UserID to Core */
/* Assumption APPL class has been defined, activated, and raclisted as part of WebSphere Application Server OEM setup. */
Call RacfCmd "PERMIT BBNBASE CLASS(APPL) ID(ZOSMFAD) ACCESS(READ)"
Call RacfCmd "SETROPTS RACLIST(APPL) REFRESH"

/* Assumption EJBROLE is defined, activated, and raclisted. */
Call RacfCmd "RDEFINE EJBROLE BBNBASE.izuUsers UACC(NONE)"
Call RacfCmd "PERMIT BBNBASE.izuUsers CLASS(EJBROLE) ID(ZOSMFAD) ACCESS(READ)"
Call RacfCmd "SETROPTS RACLIST(EJBROLE) REFRESH"

/* SyncToOSThread permits */
/* Assumption BBO.SYNC.XXXXXX.YYYYYY facility class has been defined, activated, and raclisted as part of WebSphere */
/* Application Server OEM setup. */
/* Call RacfCmd "RDEFINE FACILITY BBO.SYNC.BBNBASE.BBNC001 UACC(NONE) " */
Call RacfCmd "PERMIT BBO.SYNC.BBNBASE.BBNC001 CLASS(FACILITY) ID(WSCRU1) ACC(READ)"
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"

/* Assume SURROGAT class was defined.  It is shipped with z/OS. */
Call RacfCmd "RDEFINE SURROGAT BBO.SYNC.ZOSMFAD UACC(NONE)"
Call RacfCmd "SETROPTS CLASSACT(SURROGAT)"
Call RacfCmd "PERMIT BBO.SYNC.ZOSMFAD CLASS(SURROGAT) ID(WSSRU1) ACCESS(READ)"
/* If SURROGAT was previously RACLISTed use the one below. If not comment the one below and */
/* uncomment the one after */
Call RacfCmd "SETROPTS RACLIST(SURROGAT) REFRESH"
/* Call RacfCmd "SETROPTS RACLIST(SURROGAT)" */

/* Connect the z/OSMF Administrator UserID to the CIM and CEA groups */
Call RacfCmd "CONNECT ZOSMFAD GROUP(CIMGP)"
Call RacfCmd "CONNECT ZOSMFAD GROUP(CEAGP)"
```

Figure 27. Sample RACF commands for authorizing z/OSMF core functions and Incident Log task, with CIM server setup requested (Part 1 of 4)

```
/* Setup CIM */
Call RacfCmd "RDEFINE FACILITY BPX.FILEATTR.PROGCTL UACC(NONE)"
Call RacfCmd "PERMIT BPX.FILEATTR.PROGCTL CLASS(FACILITY) ID(CIMGP) ACCESS(READ)"

/* Setup program control to authorize library */
/* Assumption that PROGRAM has been activated. If not uncomment the next two lines */
/* Call RacfCmd "RDEFINE PROGRAM * " */
/* Call RacfCmd "SETROPTS WHEN(PROGRAM)" */
Call RacfCmd "RALTER PROGRAM * ADDMEM('CEE.SCEERUN'//NOPADCHK) UACC(READ)"
Call RacfCmd "RALTER PROGRAM * ADDMEM('CEE.SCEERUN2'//NOPADCHK) UACC(READ)"
Call RacfCmd "SETROPTS WHEN(PROGRAM) REFRESH"

Call RacfCmd "RDEFINE FACILITY BPX.SERVER UACC(NONE)"
Call RacfCmd "PERMIT BPX.SERVER CLASS(FACILITY) ID(ZOSMFAD) ACCESS(READ)"
/* Assumption FACILITY has been raclisted.  If not comment out line below and uncomment the */
/* one underneath it */
Call RacfCmd "SETROPTS RACLIST(FACILITY) REFRESH"
/* Call RacfCmd "SETROPTS RACLIST(FACILITY)" */

/*********************************************************************/
/** Define WBEM specifics for CIM                                   **/
/*********************************************************************/
Call RacfCmd "RDEFINE CDT WBEM UACC(NONE) CDTINFO( CASE(UPPER) MAXLENGTH(246) " || ,
    "FIRST(ALPHA) OTHER(ALPHA,NUMERIC) MAXLENX(246) KEYQUALIFIERS(0) PROFILESALLOWED(YES) POSIT(200) " || ,
    "DEFAULTRC(8) DEFAULTUACC(NONE) RACLIST(REQUIRED)) "
Call RacfCmd "SETROPTS CLASSACT(CDT)"
Call RacfCmd "SETROPTS RACLIST(CDT)"
Call RacfCmd "SETROPTS RACLIST(CDT) REFRESH"

Call RacfCmd "SETROPTS CLASSACT(WBEM)"
Call RacfCmd "SETROPTS RACLIST(WBEM)"
Call RacfCmd "RDEFINE WBEM CIMSERV"
Call RacfCmd "SETROPTS RACLIST(WBEM) REFRESH"

Call RacfCmd "PERMIT CIMSERV CLASS(WBEM) ACCESS(CONTROL) ID(CIMGP)"
Call RacfCmd "SETROPTS RACLIST(WBEM) REFRESH"

Call RacfCmd "RDEFINE SURROGAT BPX.SRV.ZOSMFAD UACC(NONE)"
Call RacfCmd "PERMIT BPX.SRV.ZOSMFAD CL(SURROGAT) ID(ZOSMFAD) ACCESS(CONTROL)"
/* If SURROGAT was previously RACLISTed use the one below. If not comment the one below and */
/* uncomment the one after */
Call RacfCmd "SETROPTS RACLIST(SURROGAT) REFRESH"
/* Call RacfCmd "SETROPTS RACLIST(SURROGAT)" */

/* Setup the z/OSMF Administrator UserID to CEA and CIM */

/*-------------------------------------------------------------------- */
/* Step 1 Setup the Common Event Adapter (CEA) Support                 */
/* Define the CEA UserID with UNIX System Services support.              */
/*--------------------------------------------------------------------*/
Call RacfCmd "ADDUSER CEA DFLTGRP(SYS1) OMVS( UID(9002)  FILEPROCMAX(1024))"
Call RacfCmd "RDEFINE STARTED CEA.** STDATA(USER(CEA) GROUP(SYS1) TRACE(YES))"
Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"
```

Figure 28. Sample RACF commands for authorizing z/OSMF core functions and Incident Log task, with CIM server setup requested (Part 2 of 4)

```
/*-------------------------------------------------------------------- */
/* Step 2 Setup for Multi-Layer Security (MLS)                    */
/* This step is only necessary if the installation is                */
/* already using MLS. Otherwise, it can be skipped.                  */
/*-------------------------------------------------------------------*/
/*ALTUSER CEA SECLABEL(SYSMULTI) */
/*PERMIT SYSMULTI CLASS(SECLABEL) ACCESS(ALTER) ID(CEA) */
/*PERMIT SYSHIGH CLASS(SECLABEL) ACCESS(ALTER) ID(CEA) */
/*PERMIT SYSLOW CLASS(SECLABEL) ACCESS(ALTER) ID(CEA) */
/*ADDSD 'CEA.*' SECLABEL(SYSNONE) */

/*SETROPTS GENERIC(STARTED) REFRESH */
/*SETROPTS RACLIST(STARTED) REFRESH */
/*SETR CLASSACT(SECLABEL) */
/*SETR RACLIST(SECLABEL) REFRESH */

/*Call RacfCmd "ALTUSER ZOSMFAD  SECLABEL(SYSMULTI)"*/
/*Call RacfCmd "PERMIT SYSMULTI CLASS(SECLABEL) ID(ZOSMFAD) ACCESS(READ)"*/

/*-------------------------------------------------------------------- */
/* Step 3 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 CEAGroup, authority to the following and to grant access */
/* to perform JES operations and obtain job properties.               */
Call RacfCmd "PERMIT CEA.CEAGETPS CLASS(SERVAUTH) ID(CEAGP) ACCESS(UPDATE)"
Call RacfCmd "PERMIT CEA.CEADOCMD CLASS(SERVAUTH) ID(CEAGP) ACCESS(UPDATE)"

/* Permit CEAGroup to Incident Log */
Call RacfCmd "RDEFINE SERVAUTH CEA.CEAPDWB* UACC(NONE)"
Call RacfCmd "PERMIT CEA.CEAPDWB* CLASS(SERVAUTH) ID(CEAGP) ACCESS(UPDATE)"
Call RacfCmd "RDEFINE SERVAUTH CEA.CEADOCONSOLECMD UACC(NONE)"
Call RacfCmd "PERMIT CEA.CEADOCONSOLECMD CLASS(SERVAUTH) ID(CEAGP) ACCESS(UPDATE)"

/* Activate authority checking for the SERVAUTH class: */
Call RacfCmd "SETROPTS RACLIST(SERVAUTH) CLASSACT(SERVAUTH)"

/* If the SERVAUTH class is already active, issue: */
Call RacfCmd "SETROPTS RACLIST(SERVAUTH) REFRESH"
```

Figure 29. Sample RACF commands for authorizing z/OSMF core functions and Incident Log task, with CIM server setup requested (Part 3 of 4)

```
/* ---------------------------------------------------------------- */
/* Step 4 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(ZOSMFAD) ACCESS(UPDATE)" */
/* Call RacfCmd "SETROPTS GENERIC(DATASET) REFRESH"                                      */

/* If your installation protects MVS commands with RACF class opercmds */
/* you need to give the admin identity permission.  This is required   */
/* for the incident log verify step.                                   */
/* Call RacfCmd "PERMIT MVS.** CLASS(OPERCMDS) ID(ZOSMFAD) ACCESS(CONTROL)" */
/* Call RacfCmd "SETROPTS RACLIST(OPERCMDS) REFRESH"                          */

/* If your installation sets up PROTECT-ALL (RACF exit to protect all datasets) */
/* you will need to setup a CEA.* RACF profile and permit CEA and user admin    */
/* identity.                                                                    */
/* Call RacfCmd "ADDSD 'CEA.*' UACC(NONE)"                                      */
/* Call RacfCmd "PERMIT 'CEA.*' ID(CEA) ACCESS(ALTER)"                          */
/* Call RacfCmd "PERMIT 'CEA.*' ID(ZOSMFAD) ACCESS(ALTER)"                    */
/* Call RacfCmd "SETROPTS GENERIC(DATASET) REFRESH"                             */

/* The following two statements may be useful if you want the CIM server          */
/* to run as a started task                                                       */
/* Call RacfCmd "RDEFINE STARTED CFZCIM.* STDATA(USER(ZOSMFAD) GROUP(ZOSMFGRP))"*/
/* Call RacfCmd "SETROPTS RACLIST(STARTED) REFRESH"                               */
```

Figure 30. Sample RACF commands for authorizing z/OSMF core functions and Incident Log task, with CIM server setup requested (Part 4 of 4)

Glossary

Terms and abbreviations

This glossary defines technical terms and abbreviations used in IBM z/OS Management Facility (z/OSMF) information. If you do not find the term you are looking for, refer to IBM Glossary of Computing Terms, located at: http://www.ibm.com/software/globalization/terminology/index.jsp.

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.

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.

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.

authentication
Verification of the identity of a user or the user's eligibility to access an object.

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.

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.

client A system or process that is dependent on another system or process (usually called the server) to provide it with access to data, services, programs, or resources. Contrast with *server*.

code page
A particular assignment of code points to graphic characters. Within a given code page, a code point can have only one specific meaning. A code page also identifies how undefined code points are handled.

A specification of code points from a defined encoding structure for each graphic character in a set or in a collection of graphic character sets. Within a code page, a code point can have only one specific meaning.

common event adapter (CEA)
A z/OS component that enables the delivery of z/OS management data to clients, such as the CIM server.

Common Information Model (CIM)
An implementation-neutral, object-oriented schema for describing network management information. The Distributed Management Task Force (DMTF) develops and maintains CIM specifications.

An open standard for systems management that defines the exchange of information between managed elements such as systems, networks, applications, and services.

Common Information Model Object Manager (CIMOM)
The common conceptual framework for data management that receives, validates, and authenticates the Common Information Model (CIM) requests from the client application. It then directs the requests to the appropriate component or service provider. Synonymous with *Common Information Model server*.

Common Information Model server (CIM server)
Software, such as OpenPegasus, that allows use of the CIM standard on a system.

An object management engine that exists between the managed system and the management product. z/OSMF interacts with the CIM server (or similar technology) through a layer that converts the data from the CIM model to a format useable by the z/OSMF tasks. Synonymous with *Common Information Model Object Manager*.

component
A set of modules that performs a major function within a system.

component ID
Alphanumeric identifier that uniquely identifies the z/OS component.

content area
In a Web page that is based on a page template, the editable region of the page.

Area of the z/OSMF browser interface (the central pane) in which data for the active task is displayed.

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*.

coupling facility
A special logical partition that provides high-speed caching, list processing, and locking functions in a sysplex.

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.

description
See *incident description*.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent. See *FTP destination*.

diagnostic
Pertaining to the detection and isolation of an error.

diagnostic data
The collected information for an incident, such as dumps, OPERLOG, the logrec data set, and the logrec summary.

diagnostic details
Properties of an incident. The details include additional information about an incident and a list of the diagnostic data collected for the incident.

DNS See *Domain Name System*.

domain name server
In the Internet suite of protocols, a server program that supplies name-to-address translation by mapping domain names to IP addresses.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dump analysis and elimination (DAE)
A z/OS service that enables an installation to suppress SVC dumps and ABEND SYSUDUMP dumps that are not needed because they duplicate previously written dumps.

E

Electronic Technical Response (ETR)
See *problem management record*.

Environmental Record Editing and Printing (EREP)
The program that formats and prepares reports from the data contained in the error recording data set.

EREP See *Environmental Record Editing and Printing*.

error A discrepancy between a computed, observed, or measured value or condition

and the true, specified, or theoretically correct value or condition.

The smallest detectable anomaly or exception that can occur in an information system. Errors may be caused by hardware, software, internal code, media, or external causes, for example, people or environmental abnormalities.

error log
A data set or file that is used to record error information about a product or system. See *logrec*.

error message
An indication that an error has been detected.

error summary
A summary log of system errors. This log corresponds to a logrec summary report.

F

file permission bits
In z/OS UNIX, information about a file that is used, along with other information, to determine if a process has read, write, or execute/search permission to a file or directory. The bits are divided into three parts, which are owner, group, and other.

firewall
A network configuration, usually both hardware and software, that prevents unauthorized traffic into and out of a secure network.

An intermediate server that functions to isolate a secure network from an insecure network.

fixed-length record
A record having the same length as all other records with which it is logically or physically associated. Contrast with *variable-length record*.

FTP See *File Transfer Protocol*.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

FTP data file
See *FTP.DATA file*.

FTP destination
An FTP server typically managed by a third party technical support organization. The FTP destination stores information required to initiate a transfer of incident-related data to the third party to assist in problem determination.

FTP job
A job running on z/OS that sends incident-related information to an FTP destination.

FTP job status
The state of the FTP job. For details about the status of an FTP job, see the online help for the Incident Log task *FTP Job Status* panel.

FTP profile
Information needed by an FTP job to gain access to an FTP destination through an organization's firewall or proxy.

FTP.DATA file
In z/OSMF, an installation-defined data set that contains the information needed by an FTP job to send incident-related information to an FTP destination. The FTP.DATA file contains information about the installation's configuration (firewall and proxy) and the FTP destination (default server name or IP address). When saved, the FTP.DATA file is available for use by any of the installation's FTP jobs. The FTP.DATA file is a z/OS UNIX file system data set, for example, a zFS.

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 z/OSMF without an explicit role assignment. Depending on how a guest user enters z/OSMF, the user is considered either authenticated or non-authenticated, as follows:

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

A z/OSMF administrator can manage the access of guest users to z/OSMF tasks through the *z/OSMF Roles* task.

GUI See *graphical user interface*.

H

hardcopy log
In systems with multiple console support or a graphic console, a permanent record of system activity.

header
Area of the z/OSMF browser interface (the upper pane) in which the banner is displayed.

HFS See *hierarchical file system*.

hierarchical file system (HFS)
A system for organizing files in a hierarchy, as in a UNIX® system.

I

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 system through a Web browser interface. Structurally, z/OSMF comprises a Web browser interface that communicates with the z/OSMF application running on the z/OS host system. z/OSMF is offered by IBM as a separately licensed program product for z/OS.

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.

incident
An event that is not part of the standard operation of a service and causes or may cause a disruption to or a reduction in the quality of services and customer productivity.

incident description
In the Incident Log task, the dump title for an incident, as it was specified by the operator or the abending system function.

Incident Log task
In z/OSMF, the management task that allows you to display a log of system records with details about each potential system problem. The Incident Log task provides a list of incidents through a summary view (*Incident Log* panel) and a selectable detail view (*Diagnostic Details* panel). The Incident Log task can help you obtain, aggregate, and send data to IBM Support or an independent software vendor (ISV) and manage the data associated with a particular problem.

initial program load (IPL)
The process of loading the operating system and other basic software into main storage.

The process by which an operating system is initialized at the beginning of the day or session. At IPL, the system operator enters the installation-specific information the operating system must have in order to manage the installation's workloads. This information includes system parameters, system data set definitions, and other information needed for the operating system to begin operating.

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 The links listed under the Links category in z/OSMF are links to external resources that you might use when performing system management tasks.

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.

member
A partition of a partitioned data set (PDS) or partitioned data set extended (PDSE).

MSGCLASS
Parameter on the JCL JOB statement that specifies the output class for output listings (SYSOUT). Output classes are defined by the installation to designate unit record devices, such as printers.

N

navigation area
Area of the z/OSMF browser interface (the left pane) from which the user can select among various systems management tasks. For example: "To view potential problems, select the Incident Log task from the z/OSMF navigation area."

O

operations log (OPERLOG)
In a sysplex, the log of operational messages (WTOs and WTORs), which is stored in a z/OS system logger log stream.

OPERLOG
See *operations log*.

P

partitioned data set (PDS)
A data set in direct access storage that is divided into partitions, called members, each of which can contain a program, part of a program, or data. Synonymous with program library. Contrast with *sequential data set*.

partitioned data set extended (PDSE)
A system-managed data set that contains an indexed directory and members that are similar to the directory and members of partitioned data sets. A PDSE can be used instead of a partitioned data set.

pass phrase
A string consisting of mixed-case letters, numbers, and special characters, including blanks, that is used to control access to data and systems.

password
A string of characters known to a user who must specify it to gain full or limited access to a system and to the data stored within it. RACF uses a password to verify the identity of the user.

PDS See *partitioned data set*.

PDSE See *partitioned data set extended*.

PMR See *problem management record.*

port An access point for data entry or exit.

port number
The part of a socket address that identifies a port within a host.

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.

profile
A file containing customized settings for a system or user.

proxy An application gateway from one network to another for a specific network application such as FTP.

R

RACF See *Resource Access Control Facility*.

reason code
A return code that describes the reason for the failure or partial success of an attempted operation.

record A group of related data, words, or fields treated as a unit, such as one name, address, and telephone number.

A self-contained collection of information about a single object. A record is made up of a number of distinct items, called fields. See *fixed-length record*, *variable-length record*.

Remote Technical Assistance and Information Network (RETAIN®)
Database used by IBM Support Centers to record all known problems with IBM licensed programs.

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.

RETAIN
See *Remote Technical Assistance and Information Network*.

role In z/OSMF, a functional grouping of task authorizations. A role represents the authorizations associated with that role.

S

SCHENV parameter
Parameter on the JCL JOB statement that specifies the name of the WLM scheduling environment for a job.

send diagnostic data
In the Incident Log task, the option to collect the information necessary for sending diagnostic data to IBM or another destination and initiate the FTP action.

sequential data set
A data set whose records are organized on the basis of their successive physical positions, such as on magnetic tape.

A data set in which the contents are arranged in successive physical order and are stored as an entity. The data set can contain data, text, a program, or part of a program. Contrast with *partitioned data set (PDS)*.

server In a network, hardware or software that provides facilities to clients. Examples of a server are a file server, a printer server, or a mail server.

A computer that contains programs, data, or provides the facilities that other computers on the network can access.

The party that receives remote procedure calls. Contrast with *client*.

ServerPac
A software-delivery package consisting of products and service for which IBM has performed the System Modification Program/Extended (SMP/E) installation steps and some of the post-SMP/E installation steps.

session
The period of time during which a user of a terminal can communicate with an interactive system; usually, the elapsed time from when a terminal is logged into the system until it is logged out of the system.

A logical or virtual connection between two stations, software programs, or devices on a network that allows the two elements to communicate and exchange data.

The time during which an authenticated user is logged in.

solution
A combination of products that addresses a particular customer problem or project.

source In the Incident Log task, it is the name of the data set or log stream in which the dump or log is stored.

SPECIAL attribute
A user attribute that gives the user full control over all of the RACF profiles in the RACF database and allows the user to issue all RACF commands, except for commands and operands related to auditing.

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.

structure
A construct used to map and manage storage on a coupling facility.

superuser
In z/OS UNIX, a system user who operates with the special privileges needed to perform a specified administrative task.

superuser authority
In z/OS UNIX, the unrestricted authority to access and modify any part of the operating system, usually associated with the user who manages the system.

supervisor call (SVC)
An instruction that interrupts a program being executed and passes control to the

supervisor so that it can perform a specific service indicated by the instruction.

SVC See *supervisor call*.

SVC dump
A dump that is issued when a z/OS or a DB2® functional recovery routine detects an error.

A representation of the virtual storage for the system when an error occurs. Typically, a system component requests an SVC dump from a recovery routine when an unexpected error occurs. However, an authorized program or the operator can also request an SVC dump when diagnostic dump data is needed to solve a problem.

SYSLOG
See *system log*.

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*.

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.

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)
A single-system log of operational messages, stored in JES spool files The system log includes all entries made by the WTL (write-to-log) macro as well as the hardcopy log.

system logger
A central logging facility provided by z/OS. The system logger component provides an integrated logging facility that can be used by system and subsystem components. System logger 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
See *system REXX*.

T

task In z/OSMF, a systems management function that is selectable from the product's navigation area.

terse The process of compacting (packing) data before transmitting a copy to another site, typically employing FTP as the transmission mechanism. A complementary unpack service is provided to create a similar data set at the receiving site. On z/OS, the AMATERSE service aid program is used to compact data.

tracking ID
A local problem tracking number, available to correlate an incident with a problem management system.

U

user A person who requires the services of a computing system.

user-initiated abend
A request made by user code to the operating system to abnormally terminate a routine. Contrast with *system-initiated abend*.

V

variable-length record
A record having a length independent of the length of other records with which it is logically or physically associated. Contrast with *fixed-length record*.

W

WLM See *workload manager*.

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 host system
The system on which z/OSMF is running.

z/OSMF
See *IBM z/OS Management Facility*.

zFS See *zSeries file system*.

zSeries file system (zFS)
A type of file system that resides in a Virtual Storage Access Method (VSAM) linear data set (LDS).

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:

IBM Corporation
Mail Station P300
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.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates 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.

Programming Interfaces Information

This book documents information that is NOT intended to be used as Programming Interfaces of z/OS.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (&regtm; or &tm;), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml.

These terms are trademarks or registered trademarks of Ricoh Co., Ltd., in the United States, other countries, or both:

- AFP
- Infoprint

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo 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 may be trademarks or service marks of others.

Index

Special characters

A

B

C

D

E

F

T

U

V

W

Z

Readers' Comments — We'd Like to Hear from You

z/OS
IBM z/OS Management Facility User's Guide
Version 1 Release 11

Publication No. SA38-0652-02

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

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 state on this form.

Comments:

Thank you for your support.

Submit your comments using one of these channels:
- Send your comments to the address on the reverse side of this form.
- Send your comments via e-mail to: mhvrcfs@us.ibm.com

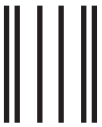
If you would like a response from IBM, please fill in the following information:

Name	Address
Company or Organization	
Phone No.	E-mail address

Readers' Comments — We'd Like to Hear from You
SA38-0652-02

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
MHVRCFS, Mail Station P181
2455 South Road
Poughkeepsie, NY
12601-5400

Fold and Tape | **Please do not staple** | Fold and Tape

SA38-0652-02

Cut or Fold
Along Line

Program Number: 5655-S28

Printed in USA

SA38-0652-02