z/OS
Version 2 Release 3

IBM z/OS Management Facility Configuration Guide

SC27-8419-30

Note

Before using this information and the product it supports, read the information in "Notices" on page 329.

This edition applies to Version 2 Release 3 of z/OS (5650-ZOS) and to all subsequent releases and modifications until otherwise indicated in new editions.

Last updated: 2019-06-27

Contents

Figures

Tables

About this document

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

Who should use this document

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

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

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

Where to find more information

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

z/OSMF home page

For more information about z/OSMF, visit the z/OSMF Marketplace at https://www.ibm.com/us-en/marketplace/zos-management-facility.

The z/OS Basic Skills Information Center

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

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

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

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

How to send your comments to IBM

We invite you to submit comments about the z/OS product documentation. Your valuable feedback helps to ensure accurate and high-quality information.

Important: If your comment regards a technical question or problem, see instead "If you have a technical problem" on page xxiii.

Submit your feedback by using the appropriate method for your type of comment or question:

Feedback on z/OS function
If your comment or question is about z/OS itself, submit a request through the IBM RFE Community (www.ibm.com/developerworks/rfe/).

Feedback on IBM Knowledge Center function
If your comment or question is about the IBM Knowledge Center functionality, for example search capabilities or how to arrange the browser view, send a detailed email to IBM Knowledge Center Support at ibmkc@us.ibm.com.

Feedback on the z/OS product documentation and content
If your comment is about the information that is provided in the z/OS product documentation library, send a detailed email to mhvrcfs@us.ibm.com. We welcome any feedback that you have, including comments on the clarity, accuracy, or completeness of the information.

To help us better process your submission, include the following information:

- Your name, company/university/institution name, and email address
- The following deliverable title and order number: IBM z/OSMF Configuration Guide, SC27-8419-30
- The section title of the specific information to which your comment relates
- The text of your comment.

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

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

If you have a technical problem

If you have a technical problem or question, do not use the feedback methods that are provided for sending documentation comments. Instead, take one or more of the following actions:

- Go to the IBM Support Portal (support.ibm.com).
- Contact your IBM service representative.
- Call IBM technical support.

Summary of changes

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

Summary of changes made in z/OS Version 2 Release 3, as updated December 2018

This document contains information that was previously presented in *IBM z/OS Management Facility Configuration Guide*, SC27-8419-30, which supports IBM z/OS Management Facility Version 2 Release 3.

New information

New function is available for z/OSMF V2R3 when you install the December 2018 functional updates.

With the installation of APAR PH03137, the IBM zERT Network Analyzer task is a new optional plug-in of z/OSMF. You can use this task to identify the cryptographic protection characteristics of TCP and Enterprise Extender (EE) connections with local endpoints on your z/OS system. For more information, see the following topics:

- For an overview, see "IBM zERT Network Analyzer task overview" on page 81.
- For customization information, see "Updating z/OS for the IBM zERT Network Analyzer Plug-in" on page 150.
- For troubleshooting information, see "Problems when using IBM zERT Network Analyzer" on page 219.

With the installation of APAR PI99307, the Sysplex Management task is enhanced with functions for modifying coupling facilities, CF structures, CF connectivity paths, and couple data sets in the enterprise scope. For more information, see "Sysplex Management task overview" on page 92.

The following information is new: Chapter 10, "Configuring z/OSMF for high availability," on page 169.

Changed Information

The Software Management task is enhanced to allow you to view, a create and perform workflows defined to a specified software instance and for software that is being deployed.

- Read access controls for performing workflows against a software instances have been added. For more information see "Authorizing users to software instances" on page 136.
- Resource authorizations for the software deployment plug-in have been updated. For more information see Table 45 on page 306.

Summary of changes made in z/OS Version 2 Release 3, as updated August 2018

This document contains information that was previously presented in *IBM z/OS Management Facility Configuration Guide*, SC27-8419-30, which supports IBM z/OS Management Facility Version 2 Release 3.

New information

With the installation of APAR PI93759, a new command is added for displaying the settings for a particular z/OSMF server. For information, see "Displaying the z/OSMF server settings" on page 33.

New customization information is available for the Sysplex Management plug-in. See "Updating z/OS for the Sysplex Management plug-in" on page 143.

Summary of changes made in z/OS Version 2 Release 3, as updated June 2018

This document contains information that was previously presented in *IBM z/OS Management Facility Configuration Guide*, SC27-8419-30, which supports IBM z/OS Management Facility Version 2 Release 3.

New information

New function is available for z/OSMF V2R3 when you install the June 2018 functional updates.

The CLOUD_SEC_ADMIN keyword is added to the z/OSMF parmlib member, IZUPRMxx. If your installation plans to allow automatic security updates for Cloud Provisioning, you must define a valid user ID for the CLOUD_SEC_ADMIN keyword in your active IZUPRMxx parmlib member. When specified, automatic security updates are performed under this user ID. Otherwise, if this value is omitted, user authorizations for Cloud Provisioning must be maintained manually by your security administrator. For more information, see "IZUPRMxx reference information" on page 36.

The IZUPRSEC job is added to SYS1.SAMPLIB. This job contains sample RACF commands for enabling the Cloud Provisioning functions. If your installation uses an external security manager other than RACF, your security administrator can refer to the IZUPRSEC job for examples when creating equivalent authorizations for your system. For more information, see "Help with security setup" on page 55.

The Cloud Provisioning installation verification procedure (IVP) is new. This program, which is supplied with z/OSMF, is intended to help you verify that security is set up correctly for the domain administrator. For more information, see "Verify that security is set up for the domain administrator" on page 61.

The Cloud Provisioning plug-in adds support for Swagger, which is an interface for displaying information about REST APIs. To enable users to access and use Swagger, you must create the authorization that is described in "Resource authorizations for application developers" on page 68.

Summary of changes made in z/OS Version 2 Release 3, as updated May 2018

This document contains information that was previously presented in *IBM z/OS Management Facility Configuration Guide*, SC27-8419-30, which supports IBM z/OS Management Facility Version 2 Release 3.

New information

With the installation of APAR PI92211, IBM is changing the recommended mount point for the z/OSMF data directory (sometimes called the *user directory*) to `/global/zosmf`, rather than `/var/zosmf`.

The use of the global directory is intended to:

- Make it easier for z/OSMF-based applications with sysplex scope to remain synchronized with sysplex-scoped data repositories, such as the RACF database, WLM policy, and TCP/IP profile
- Make it easier to move the z/OSMF server to a different z/OS system in the sysplex
- Help simplify automatic recovery from LPAR or z/OSMF server failures.

In this document, the defaults, instructions, and examples are updated, where appropriate, to show the use of the `/global/zosmf` mount point.

Summary of changes made in z/OS Version 2 Release 3, as updated March 2018

This document contains information that was previously presented in *IBM z/OS Management Facility Configuration Guide*, SC27-8419-30, which supports IBM z/OS Management Facility Version 2 Release 3.

Changed information

Chapter 3, “Setting up z/OSMF for the first time,” on page 15 has been reorganized to make it easier to use.

Summary of changes made in z/OS Version 2 Release 3, as updated December 2017

This document contains information that was previously presented in *IBM z/OS Management Facility Configuration Guide*, SC27-8419-30, which supports IBM z/OS Management Facility Version 2 Release 3.

This document contains new or changed information for maintenance.

Summary of changes made in z/OS Version 2 Release 3, as updated November 2017

This document contains information that was previously presented in *IBM z/OS Management Facility Configuration Guide*, SC27-8419-30, which supports IBM z/OS Management Facility Version 2 Release 3.

New information

With the installation of APAR PI88651, you can use an alternative name for the z/OSMF angel process by coding the name on the ANGEL_PROC parameter in the IZUPRMxx member. By default, the angel is named IZUANG1. For more information, see “IZUPRMxx reference information” on page 36 and “Considerations for using a named angel” on page 28.

Summary of changes made in z/OS Version 2 Release 3, as updated October 2017

This document contains information that was previously presented in *IBM z/OS Management Facility Configuration Guide*, SC27-8419-30, which supports IBM z/OS Management Facility Version 2 Release 3.

This document contains new or changed information for maintenance.

Changes made in z/OS Version 2 Release 3, SC27-8419-30

This document contains information that was previously presented in *IBM z/OS Management Facility Configuration Guide,* SC27-8419-06, which supported IBM z/OS Management Facility Version 2 Release 2.

New autostart capability

In z/OS V2R3, the base element z/OSMF is started by default at system IPL. This behavior, which is referred to as *z/OSMF autostart*, means that z/OSMF is available for use as soon as the system is up.

Related to this support are the following enhancements:

- Statements and keywords are added to the z/OSMF parmlib member, IZUPRMxx.
- Parameters are added to the z/OSMF started procedure, IZUSVR1.
- System parameter IZU= is added to the IEASYSxx parmlib member. Use the IZU= parameter to identify one or more IZUPRMxx parmlib members to be used for your z/OSMF configuration.

Authorized programs can use the event notification facility (ENF) to determine whether the z/OSMF server is up or down. For more information, see “Detecting whether the z/OSMF server is available” on page 161.

With z/OSMF autostart, it is no longer necessary for your installation to explicitly start the z/OSMF server after each system IPL, whether through automation or commands entered manually at the operations console. Therefore, you must review and, if necessary, modify or remove any methods that you currently use for starting the z/OSMF server. For example, check for **START** commands for the z/OSMF started procedures in the COMMNDxx parmlib member and your automation products.

If you prefer not to have z/OSMF started automatically, you can disable the autostart function. However, if you do so, the JES2 Email Delivery Services (EDS) function in z/OS V2R3 does not operate with full function until an autostarted z/OSMF server is active in your sysplex.

For more information, see Chapter 8, "Autostart concepts in z/OSMF," on page 157.

New system management tasks

The following tasks are new in this release:

- The Sysplex Management task is new in this release. You can use this task to view sysplex topology and the details of sysplex objects, such as coupling facilities, coupling facility structures, and couple data sets. See "Sysplex Management task overview" on page 92.
- The z/OS Operator Consoles task is new in this release. You can use this task to work with z/OS consoles, enter commands, and view system messages. See "z/OS Operator Consoles task overview" on page 98.

Your installation can customize the z/OSMF Welcome page by using the Settings task. You might do so, for example, to provide users with information they should read before they log in to z/OSMF, such as instructions specific to your company. In previous releases, it was necessary to edit the Welcome properties file to specify text for the header and footer areas. In this release, you can do so directly, through the z/OSMF user interface (UI). As a result, the information about editing the Welcome properties file is removed from this edition of the book.

For more information about the new tasks, see the online help that ships with z/OSMF. Begin with the topics *What's new* and *z/OSMF tasks at a glance*. The z/OSMF online help is also available in IBM Knowledge Center at: IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SSLTBW/welcome).

Changed information

The z/OSMF server requires a minimum of 4 GB of system memory to be configured.

z/OSMF requires the following level of Java™:

> IBM 64-bit SDK for z/OS, Java Technology Edition, V8 SR4 FP10 (5655-DGH).

The list of supported web browsers is changed. See "Software prerequisites for z/OSMF" on page 6.

Moved information

The migration actions for z/OSMF are now described in *z/OS Migration*.

Deleted information

The script **`izumigrate.sh`** is deprecated and is no longer used. In previous releases, this script was used for migrating to a new release of z/OSMF.

Information applicable to all releases

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

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

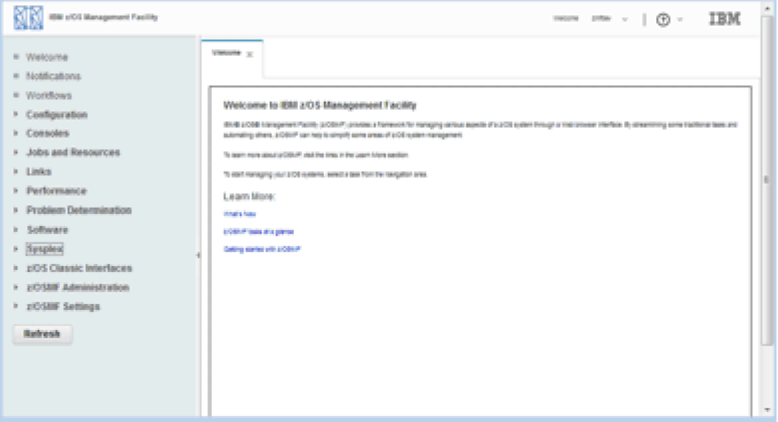
Part 1. Introduction

An introduction to z/OSMF includes the following topics:

- Chapter 1, “Overview of z/OSMF,” on page 3
- Chapter 2, “Project plans for configuring z/OSMF,” on page 9.

Chapter 1. Overview of z/OSMF

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



Welcome to IBM z/OS Management Facility

[illegible]

Learn More:

[illegible]

Figure 1. Introducing z/OSMF: The Welcome page

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

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

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

z/OSMF allows you to communicate with the z/OS system through a web browser, so you can access and manage your z/OS system from anywhere. Multiple users can log into z/OSMF using different computers, different browsers, or multiple instances of the same browser.

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

z/OSMF and related system components

z/OSMF is shipped as part of z/OS.

z/OSMF can run on a parallel sysplex, monoplex, or XCF local mode environment.

Structurally, z/OSMF is a set of web applications that are hosted on your z/OS system. Depending on the task to be performed, z/OSMF interfaces with other z/OS components to offer you a simplified interface for performing those tasks.

The z/OS components make up the environment necessary for using the z/OSMF functions. z/OSMF neither requires a client workstation component nor does it provide one. All that is needed is a compatible web browser for accessing z/OSMF from your workstation.

z/OSMF includes the following software:

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

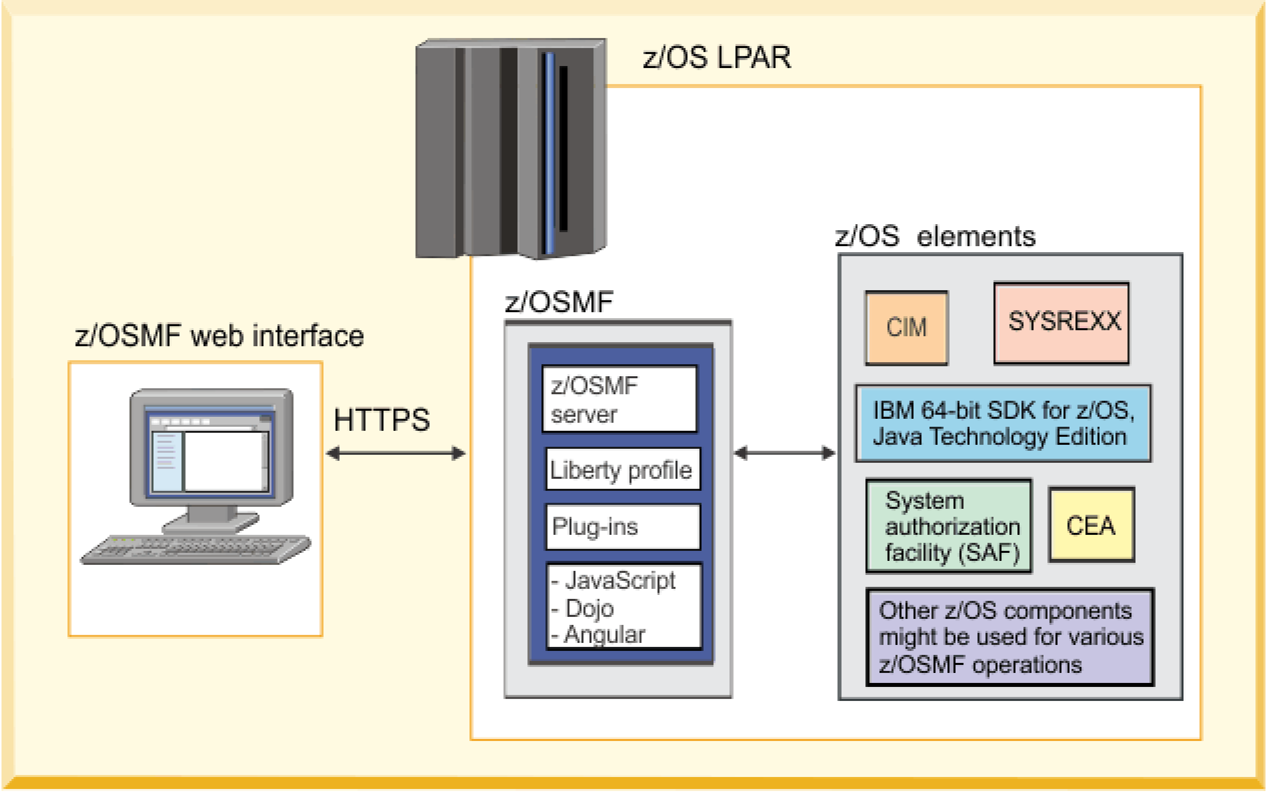

z/OS LPAR
z/OS elements
z/OSMF web interface
z/OSMF
HTTPS
z/OSMF server
Liberty profile
Plug-ins
- JavaScript
- Dojo
- Angular
CIM
SYSREXX
IBM 64-bit SDK for z/OS, Java Technology Edition
System authorization facility (SAF)
CEA
Other z/OS components might be used for various z/OSMF operations

Figure 2. z/OSMF and related system components

The goal of this architecture is to provide simplified systems management function through a common, easy-to-use, graphical user interface. Figure 2 on page 4 shows a typical architecture and flow, starting with the user's browser session and continuing through z/OSMF, with information passed to various z/OS system components as needed.

Depending on the particular task that is being performed, z/OSMF uses various enabling technologies on z/OS, such as the following:

- IBM 64-bit SDK for z/OS, Java Technology Edition. This IBM software development kit (SDK) contains the Java Runtime Environment (JRE) and other tools that support Java applications.
- Common Information Model (CIM) server 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 the selected z/OS events.
- System authorization facility (SAF). This component enables programs to use system authorization services to control access to resources, such as data sets and MVS™ commands. SAF either processes security authorization requests directly or works with RACF®, or other external security manager, to process them.
- System REXX (SYSREXX). This component provides an infrastructure through which programs that are written in the REXX language can be run outside the normal TSO/E or batch environments, using a programming interface.

Security concepts in z/OSMF

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

Besides the ability to authenticate, a would-be z/OSMF user requires authorization to one or more z/OSMF resources (tasks and links), which is necessary before the user can do useful work in z/OSMF (Figure 3 on page 5).

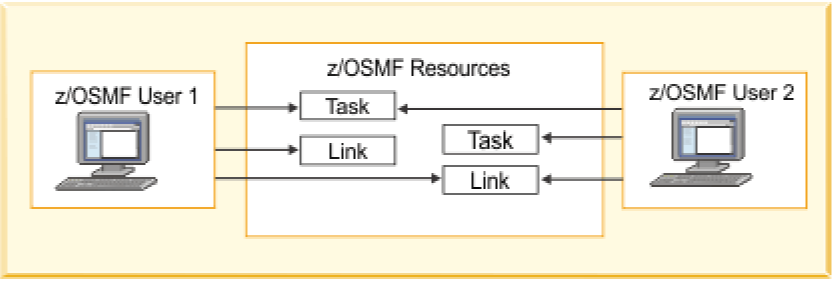


Figure 3. User authorizations in z/OSMF

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

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

Help with setting up security

IBM provides a set of jobs in SYS1.SAMPLIB with sample RACF commands to help with your z/OSMF configuration and its prerequisites. The IZUSEC job represents the authorizations that are needed for the z/OSMF core functions. Each of the other IZUxxSEC jobs is associated with a plug-in. Your security administrator can edit and run these jobs to secure various resources on the z/OS system. To create user authorizations for the plug-ins, your security administrator can use the IZUAUTH job in SYS1.SAMPLIB. It is assumed that your security administer has a user ID with the RACF SPECIAL attribute. For more information, see Chapter 6, “Setting up security for the z/OSMF plug-ins,” on page 101.

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

z/OSMF does not support multilevel security

If the z/OSMF server is running in a *multilevel secure (MLS)* z/OS system, some z/OSMF functions might fail to work properly. The failures can occur because z/OSMF does not assign a SECLABEL to its started task address space. As a result, the functions that use inter-address space communication might fail because of a SECLABEL mismatch. For example, a failure can occur in the ISPF task because it starts a TSO address space with the SECLABEL of the current z/OSMF user. Other z/OSMF functions that might fail include the z/OS data set and file REST interface and the TSO/E address space services.

Software delivery options for z/OSMF

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

These differences are explained as follows:

ServerPac users:

- If you select the full system replacement installation type, a default instance of z/OSMF is set up for you. Here, a base z/OSMF configuration is created through a ServerPac post-installation job, using IBM-supplied defaults. The default instance of z/OSMF does not include any of the optional plug-ins, such as Network Configuration Assistant, Incident Log, and so on. Enabling the optional plug-ins in z/OSMF requires some customization of the z/OS host system, as described in Chapter 7, “Customizing your z/OS system for the z/OSMF plug-ins,” on page 105.
- If you select the software upgrade installation type, you require the planning and configuration information in this document to create a z/OSMF configuration. Your system programmer can create a customized version of the IZUPRMxx member on your system, and define plug-ins to it.

ServerPac provides customization guidance for configuring z/OSMF. See the copy of *ServerPac: Installing Your Order* that is supplied with your order.

CBPDO users:

If you receive z/OSMF in a Custom-Built Product Delivery Option (CBPDO) software delivery package, you require the planning and configuration information in this document. Your installation's system programmer can create a customized IZUPRMxx member to define an instance of z/OSMF on your system.

Hardware prerequisites for z/OSMF

z/OSMF requires a certain amount of CPU resource and memory for satisfactory operation. On a z/OS V2R3 system that is running on the IBM z14 (z14) server, the minimum hardware memory requirement is 8 gigabyte (8G) of central storage. On a z/OS V2R3 system that is running on an earlier processor, it is recommended that the target system for z/OSMF have at least 4 gigabyte (4G) of central storage.

For a system that is running in an LPAR, ensure that the LPAR configuration has a Processor Capacity Index (PCI) of at least 50, though a smaller value might be sufficient on a system with an IBM z Integrated Information Processor (zIIP).

Software prerequisites for z/OSMF

The following Java level must be installed and operational on your system:

IBM 64-bit SDK for z/OS, Java Technology Edition, V8 SR4 FP10 (5655-DGH).

This set-up must be done before you configure z/OSMF. By default, the SDK resides in the directory `/usr/lpp/java/J8.0_64` on your system. If you installed it in another location, be sure to include the JAVA_HOME statement in your IZUPRMxx parmlib member, as shown in “IZUPRMxx reference information” on page 36.

It is recommended that you complete the planning for z/OSMF before you configure it. Also, be sure to obtain the latest PTFs; see “Receiving service updates for z/OSMF” on page 7.

For ServerPac users, use the jobs and documentation that is supplied with your ServerPac order to create an initial instance of z/OSMF. During the ServerPac process, you need sections of this document to complete certain actions. Thereafter, you can refer to this document for information about performing various post-configuration actions, such as configuring the optional plug-ins.

Note that the optional plug-ins in z/OSMF have different system set-up requirements. For more information, see Chapter 7, "Customizing your z/OS system for the z/OSMF plug-ins," on page 105.

The following web browsers are supported by z/OSMF, and are recommended for best results:

- Microsoft Internet Explorer Version 11
- Microsoft Edge (Windows 10)
- Mozilla Firefox ESR Version 52 or later.

What setup is needed for z/OSMF?

As a base element of the operating system, z/OSMF is installed when you install z/OS. By default, z/OSMF is installed into the z/OS root file system, in the directory `/usr/lpp/zosmf`.

Enabling z/OSMF on your system involves the following phases:

- Planning for z/OSMF. The z/OSMF server requires a minimum of 4 GB of system memory to be configured.
- Configuring an instance of z/OSMF in your sysplex, and adding optional plug-ins. This phase requires certain z/OS elements to be set up, commands to be run, and security setup to be performed for RACF or an equivalent external security manager. Information for these activities is provided in this document.

Using z/OSMF requires sufficient authority in z/OS. Specifically, on the z/OS system to be managed, the resources to be accessed on behalf of users (data sets, operator commands, and so on) are secured through the external security manager at your installation, such as RACF. Your installation's security administrator must create the authorizations in your external security manager. To assist your security administrator, IBM provides sample jobs for z/OSMF in SYS1.SAMPLIB. More information about security setup is provided in Chapter 6, "Setting up security for the z/OSMF plug-ins," on page 101 and Appendix A, "Security configuration requirements for z/OSMF," on page 287.

Unless you choose to manage the start-up and shutdown of the z/OSMF server through an automation product, z/OSMF is started automatically when you IPL your z/OS system. This behavior, which is referred to as *z/OSMF autostart*, means that z/OSMF is available for use as soon as the system is up. To make the best use of the z/OSMF autostart capability, you must plan how to deploy one or more z/OSMF servers in your environment. Generally, having one z/OSMF server active in a sysplex or monoplex is sufficient, but you might choose to have more, based on your workload requirements. The goal is to ensure that at least one z/OSMF server is always active in your environment.

For more information, see Chapter 8, "Autostart concepts in z/OSMF," on page 157.

Migrating to a new release

When you migrate to a new release of z/OSMF, you can reuse much of the customization from your current configuration.

The migration actions for z/OSMF are described in *z/OS Migration*.

Receiving service updates for z/OSMF

IBM ships service for z/OSMF in the form of program temporary fixes (PTFs). As a z/OS element, z/OSMF should be updated on the same schedule that you use to update the rest of z/OS.

Here are some useful links:

- IBMLink web site at IBM ServiceLink (www.ibm.com/ibmlink/servicelink)
- List of fix category (FIXCAT) values and descriptions on the SMP/E web site at http://www.ibm.com/systems/z/os/zos/smpe/fixcategory.html.
- Information about IBM Recommended Service Upgrade (RSU) and service testing at Consolidated Service Test and the RSU (www.ibm.com/support/docview.wss?uid=isg3T1027575).
- IBM Preventive Service recommendations at https://www.ibm.com/systems/resources/zOS_Preventive_Maintenance_Strategy.pdf.

Chapter 2. Project plans for configuring z/OSMF

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

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

- "First-time installation" on page 9
- "Migrating to a new release" on page 10
- "Adding plug-ins to your configuration" on page 10
- "Post-configuration" on page 11.

First-time installation

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

Table 1. Planning checklist for a first-time installation

√	Task summary:	IT role / skills:	Where to find instructions:
	Learn what z/OSMF is—a framework for web-based, system management tasks on z/OS.	System planners and installation managers	Chapter 1, "Overview of z/OSMF," on page 3
	Verify that your installation meets the prerequisites for using z/OSMF.	System programmer	"Software prerequisites for z/OSMF" on page 6
	Learn about the z/OSMF configuration process.	System programmer	"The configuration process" on page 15
	Verify that your workstation meets the prerequisites for using z/OSMF.	System programmer	"Preparing your workstation for z/OSMF" on page 16
	Set up the z/OSMF started procedures.	System programmer	"Updating your system for the z/OSMF started procedures" on page 24
	Optionally, gather information about your environment, to be used for creating a configuration parmlib member, IZUPRMxx.	System programmer	"IZUPRMxx reference information" on page 36
	Follow a procedure to create a base z/OSMF configuration (core functions only).	Security administrator and system programmer	"Creating a base z/OSMF configuration" on page 17
	Learn what authorities are needed to create a base configuration.	Security administrator and system programmer	"Selecting a user ID for configuration" on page 17
	Know that z/OSMF is started automatically when the z/OS system is IPLed.	System programmer	"Step 3: Prepare for z/OSMF server initialization" on page 21

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

√	Task summary:	IT role / skills:	Where to find instructions:
	Verify that the z/OSMF server is started by checking for messages on the operator console and entering **DISPLAY A** commands.	System programmer	"Step 4: Verify server initialization" on page 29
	Verify the results of your work by opening a web browser to the **Welcome** page of z/OSMF.	System programmer	"Step 5: Access the z/OSMF Welcome page" on page 30
	After you are satisfied with the base configuration, you can add function to it through the addition of one or more optional plug-ins.	System programmer	See the steps in Table 3 on page 11 for "Adding plug-ins to your configuration" on page 10.

Migrating to a new release

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

Table 2. Planning checklist for migrating to a new release

√	Task summary:	IT role / skills:	Where to find instructions:
	Perform the migration actions for z/OSMF.	System programmer	*z/OS Migration*
	Edit the IZUPRMxx parmlib member to specify the Java home directory and other settings for the new system.	System programmer	"IZUPRMxx reference information" on page 36
	Use the latest versions of the cataloged procedures for the z/OSMF started tasks. Transfer any customizations that you require to the new procedures.	System programmer	"Customizing the IZUSVR1 started procedure" on page 28
	Know that z/OSMF is started automatically when the z/OS system is IPLed.	System programmer	"Step 3: Prepare for z/OSMF server initialization" on page 21
	Verify that the z/OSMF server is started by checking for messages on the operator console and entering **DISPLAY A** commands.	System programmer	"Step 4: Verify server initialization" on page 29
	Verify the results of your work by opening a web browser to the **Welcome** page of z/OSMF.	System programmer	"Step 5: Access the z/OSMF Welcome page" on page 30

Adding plug-ins to your configuration

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

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

√	Task summary:	IT role / skills:	Where to find instructions:
	Learn about the optional z/OSMF plug-ins; determine which plug-ins to configure.	System programmer	Chapter 5, “Selecting which z/OSMF plug-ins to add,” on page 77
	Plan the security requirements for users of the z/OSMF tasks.	Security administrator and system programmer	Chapter 6, “Setting up security for the z/OSMF plug-ins,” on page 101
	Perform the z/OS system customization for each z/OSMF plug-in.	System programmer	Chapter 7, “Customizing your z/OS system for the z/OSMF plug-ins,” on page 105
	Define the plug-ins to the IZUPRMxx parmlib member.	System programmer	See the description of the PLUGINS statement in “IZUPRMxx reference information” on page 36.
	Authorize users and groups to access the z/OSMF tasks.	Security administrator and system programmer	Chapter 6, “Setting up security for the z/OSMF plug-ins,” on page 101

Post-configuration

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

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

- Chapter 11, “Linking z/OSMF tasks and external applications,” on page 173
- Chapter 12, “Configuring your system for asynchronous job notifications,” on page 175
- Chapter 13, “Adding links to z/OSMF,” on page 185
- Chapter 14, “Deleting incidents and diagnostic data,” on page 189
- Chapter 15, “Troubleshooting problems,” on page 193
- Chapter 16, “Configuration messages,” on page 225.

Part 2. Configuration

Configuring z/OSMF includes the following topics:

Chapter 3. Setting up z/OSMF for the first time

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

For ServerPac installers:

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

If you are upgrading from a previous release of z/OSMF, skip this chapter. Instead, perform the migration actions for z/OSMF, which are described in *z/OS Migration*.

The configuration process

In short, configuring an instance of z/OSMF is done by running the IBM-supplied jobs IZUSEC and IZUMKFS. z/OSMF is started automatically by default. when you IPL your z/OS system.

The z/OSMF configuration process occurs in three stages:

Stage 1 - Security setup
Stage 2 - Configuration
Stage 3 - Server initialization.

This document assumes that you will carry out the steps in the order in which they are presented.

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

Configuration stage
During this stage, you allocate and mount the z/OSMF file system and create the z/OSMF data directory. IBM supplies a sample job, SYS1.SAMPLIB(IZUMKFS) to help you with this task.

You might choose to substitute your own configuration values for the z/OSMF default settings. If so, you can create an IZUPRMxx parmlib member for your system or sysplex and specify settings in the server's started procedure, IZUSVR1. IBM supplies a sample parmlib member, SYS1.SAMPLIB(IZUPRM00), which you can use as a model, and supplies a copy of the started procedure in the PROCLIB data set.

Server initialization
During this stage, the necessary setup is done to enable z/OSMF to be started automatically when you IPL your z/OS system.

Overview of the configuration steps

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

1. Set up the security for z/OSMF (once per sysplex or security domain). Your security administrator can run the sample job IZUSEC to create a base set of security groups, user IDs, and resource profiles for your z/OSMF configuration. Before running the job, it must be reviewed and modified as necessary to ensure that the definitions will work in your security environment. See "Step 1: Create security definitions for the z/OSMF resources" on page 18.
2. Allocate the z/OSMF file system, which is used by the z/OSMF server. Here, you will edit and run the job IZUMKFS. Do this once for each z/OSMF autostart group in a sysplex. See "Step 2: Allocate and mount the z/OSMF file system" on page 20.
3. z/OSMF is intended to be started when you IPL your z/OS system. Processing is managed through the z/OSMF server, which runs as a pair of started tasks, with these default names: IZUANG1 and IZUSVR1. IBM supplies cataloged procedures for these tasks.

Additional tasks might include:

- Customizing the configuration settings for z/OSMF. See "IZUPRMxx reference information" on page 36 and "Customizing the IZUSVR1 started procedure" on page 28.
- Updating parmlib members for subsequent IPLs. For example, you should copy the mount commands from the sample mount job to your BPXPRMxx parmlib member.
- Adding the optional plug-ins. When you have established the base configuration, you can add function to z/OSMF by enabling plug-ins. Sample commands for creating resource authorizations for the plug-ins are provided in the IZUxxSEC jobs in SYS1.SAMPLIB. Sample commands for authorizing users to some plug-ins are provided in the IZUAUTH job in SYS1.SAMPLIB, while others are provided in the IZUxxSEC sample jobs.

  For more information, see Chapter 7, "Customizing your z/OS system for the z/OSMF plug-ins," on page 105.

Preparing your workstation for z/OSMF

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

- Your workstation requires a compatible operating system and web browser. For more information and other usage considerations, see the Browser Compatibility link on the http://www.ibm.com/systems/z/os/zos/zosmf/.
- z/OSMF requires a minimum screen resolution of 1024 by 768 pixels. If your workstation is set to a lower resolution, some content might not be displayed.
- Ensure that your browser is enabled for JavaScript. For instructions, see Table 30 on page 196 or Table 31 on page 198, as appropriate.
- z/OSMF uses session cookies to track which users are logged in from a specific browser. If you want to use multiple z/OSMF servers from the same workstation, you might need to either launch another browser instance (as with Internet Explorer), or, configure another browser profile (as with Firefox). For information about creating Firefox profiles, see the Mozilla web site: http://www.mozilla.com.
- If you use the Internet Explorer 8 browser, you might experience:
  - Browser memory issues, if you open multiple tabs. If so, close some unneeded tabs to use less memory.
  - Slow responsiveness for certain data-intensive operations. If so, consider using another supported browser.

After you have configured z/OSMF, you can use the included environment checker tool to verify your browser and workstation settings at any time. For more information, see "Verifying your workstation with the environment checker" on page 194.

Creating a base z/OSMF configuration

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

Before you begin

Before you continue with the z/OSMF configuration process:

1. Complete the planning checklist for a first-time installation in Chapter 2, “Project plans for configuring z/OSMF,” on page 9.
2. Review the z/OSMF configuration default values to ensure that they are acceptable for your environment. If not, you can specify alternative values by using an installation-supplied IZUPRMxx parmlib member, as described in “IZUPRMxx reference information” on page 36.
3. Verify that the TCP/IP resolver trace function is not enabled on your system. This step is necessary to ensure that z/OSMF uses the correct hostname for your system. If the trace is required, you can resume it after the z/OSMF server is initialized. For more information about this requirement, see “Initialization fails with messages IZUG401E and IZUG620E” on page 208.

Who is needed to configure z/OSMF?

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

Table 4 on page 17 shows the performer for each step of the z/OSMF configuration process.

Table 4. Actions and performers for configuring z/OSMF

Step to perform	Performed by
“Step 1: Create security definitions for the z/OSMF resources” on page 18.	Security administrator
“Step 2: Allocate and mount the z/OSMF file system” on page 20.	z/OSMF installer
“Step 3: Prepare for z/OSMF server initialization” on page 21	z/OSMF installer
“Step 4: Verify server initialization” on page 29.	z/OS operator
“Step 5: Access the z/OSMF Welcome page” on page 30.	Any authorized z/OSMF user or the z/OSMF installer
“Step 6: Log into z/OSMF” on page 31	Any authorized z/OSMF user or the z/OSMF installer

Selecting a user ID for configuration

Select a user ID to use for running the IZUMKFS job on your system. This user ID, which is referred to as the *installer user ID*, requires superuser authority.

The installer user ID requires superuser authority to perform the following system updates:

- Creating directories
- Allocating and mounting the z/OSMF file system
- Changing directory ownership and permissions.

Besides superuser authority, the installer user ID also requires update authority to the following data sets:

- Parmlib data set for any members that are to be modified during the configuration process
- Proclib data set in which the IZUSVR1 and IZUANG1 procedures are stored.

About superuser authority

There are three ways to grant a user superuser authority in z/OS:

- By granting access to UNIXPRIV class profiles, which is the recommended way. The user ID that is used to run the IZUMKFS job requires access to the following profiles in the UNIXPRIV class:
  - CONTROL access to SUPERUSER.FILESYS
  - UPDATE access to SUPERUSER.FILESYS.MOUNT
  - READ access to SUPERUSER.FILESYS.CHOWN
  - READ access to SUPERUSER.FILESYS.CHANGEPERMS
  - READ access to SUPERUSER.FILESYS.PFSCTL
- By granting access to the BPX.SUPERUSER resource in the FACILITY class.
- Assigning the user ID a UID of 0, which is the least desirable way.

For more information about how to define a user with superuser authority, see z/OS UNIX System Services User's Guide. For a list of the resource names available in the UNIXPRIV class, the z/OS UNIX privilege that is associated with each resource, and the level of access that is required to grant the privilege, see z/OS UNIX System Services Planning.

Step 1: Create security definitions for the z/OSMF resources

Both z/OSMF and its users need access to resources. Your security administrator must create security definitions to control access and maintain security for these resources. To assist the security administrator, IBM supplies a sample job IZUSEC, which can be used to create RACF security definitions for the z/OSMF core functions. It is strongly recommended that your security administrator review the contents of the job before running it, and make any changes that are needed to be consistent with your installation's security policies.

About this step

The sample job IZUSEC contains RACF commands for creating resource profiles for the z/OSMF core functions. The profiles are needed to protect the resources that are used by z/OSMF, and to grant users access to the z/OSMF core functions. The job also contains commented sections for additional authorizations that might be applicable for your installation.

During this step, you will:

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

If your installation uses an external security manager other than RACF, ask your security administrator to create equivalent commands for your environment. The RACF requirements are listed in Appendix A, “Security configuration requirements for z/OSMF,” on page 287.

The sample RACF setup jobs assign the user ID IZUSVR to all three z/OSMF started tasks, IZUANG1, IZUSVR1, and IZUINSTP. You can assign different user IDs by using profiles in the RACF STARTED class or by using the RACF Started Procedures Table. For more information about assigning user IDs to started tasks, see *z/OS Security Server RACF Security Administrator's Guide*. For other considerations, see “Define the z/OSMF started procedures to RACF” on page 24.

The IZUSEC job also contains sample RACF commands for defining the z/OSMF started procedures to the STARTED class. Figure 4 on page 19 shows the commands that are provided in the job.

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

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

Note: When you use the STARTED class, you can modify the security definitions for started procedures dynamically. For more information, see the topic on using started procedures in *z/OS Security Server RACF Security Administrator's Guide*.

Authorizing users to the z/OSMF REST interfaces

The IZUSEC job includes sample RACF commands for:

- Defining the TSO/E logon procedure and the associated account number to the TSOPROC and ACCTNUM classes, respectively.
- Authorizing z/OSMF users to the TSO/E logon procedure and account number.
- Authorizing z/OSMF users and the z/OSMF server to use CEA TSO/E address space services.
- Creating discrete security profiles for approved sites and a generic profile to disallow REST requests from all other sites.

Some z/OSMF tasks have REST interfaces, such as the Software Management task. Using these tasks can require additional authorizations.

Table 5 on page 19 describes the authorizations that are created by the IZUSEC job.

Table 5. Security authorizations for the z/OSMF REST interfaces

Resource class	Resource name	Who needs access?	Type of access required	Why
ACCTNUM	IZUACCT	IZUADMIN IZUUSER	READ	Allows callers to access the account number that is used for the procedure for the z/OSMF REST interfaces.
SERVAUTH	CEA.CEATSO.TSOREQUEST	IZUADMIN IZUUSER	READ	Allows callers to access the CEA TSO/E address space services. This setting allows HTTP client applications on your z/OS system to start and manage TSO/E address spaces.
SERVAUTH	CEA.CEATSO.TSOREQUEST	IZUSVR	READ	Allows the z/OSMF server to access the CEA TSO/E address space services. This setting allows the z/OSMF server to start and manage TSO/E address space services.
TSOPROC	IZUFPROC	IZUADMIN IZUUSER	READ	Allows callers to access the procedure for the z/OSMF REST interfaces.
ZMFAPLA	*<saf-prefix>*.REST.**	No users.	UACC (NONE)	Prevents access to the z/OSMF REST interfaces by users who are not permitted through discrete profiles.

Before running the job

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

Commands for activating the required classes are included in commented sections in the IZUSEC job. Or, your security administrator can enter the commands directly, as shown in "Class activations that z/OSMF requires" on page 287.

Running the job

Authority
This job is intended to be run by your security administrator. It is assumed that this user ID has the RACF SPECIAL attribute.

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

Invocation
Submit IZUSEC as a batch job.

Results

On completion, the job creates the security definitions that are needed to run z/OSMF.

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

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

In this step, you run the job IZUMKFS to define, format, and temporarily mount the z/OSMF file system. This step needs to be done only when you set up z/OSMF for the first time.

About this step

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

The job performs the following actions:

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

Storage consideration for IBM Cloud Provisioning and Management for z/OS

Cloud Provisioning templates, instances, and workflows on your z/OS system consume space in the z/OSMF file system. The allocated space is freed when instances and templates are removed. Likewise, Cloud Provisioning workflows consume space in the file system.

A rule of thumb is to allow an additional 600 kilobytes per template and 600 kilobytes per provisioned instance. This amount consumes approximately 13 tracks per template or instance on a 3390-formatted disk device. For example, 10 templates and 100 provisioned instances would require approximately 92 cylinders of disk space on a 3390 device.

A rule of thumb for workflow space is to allow 1 MB of space, approximately 22 tracks of 3390 space, per workflow. One hundred workflows would require approximately an additional 143 cylinders of disk space.

If your installation plans to use many templates and instances, consider specifying a larger initial allocation for the file system. By default, the primary allocation amount for the z/OSMF file system data set is 200 cylinders, and the secondary allocation amount is set to 20 cylinders. Consider increasing these allocation amounts if you plan to use Cloud Provisioning.

Storage consideration for the Workflows task

Workflow instances consume space in the z/OSMF file system. This space is freed by z/OSMF after workflow instances are deleted by users. A rule of thumb for workflow space is to allow 1 MB of space, approximately 22 tracks of 3390 space, per workflow. One hundred workflows would require approximately an additional 143 cylinders of disk space. In general, larger workflows consume more system resources than smaller workflows. The use of complex workflows with many steps and variables will require more space. If your installation plans to use large or complex workflows, consider allocating a larger file system. By default, the initial allocation is 200 cylinders.

Before running the job

1. Create a copy of the job SYS1.SAMPLIB(IZUMKFS), read its instructions, and make your changes to the copy.
2. The job mounts the z/OSMF file system at mount point `/global/zosmf`. This is a sysplex-scope mount point that is intended to allow access to the file system from any z/OS system.

Running the job

Authority
To run this job, you require a user ID with superuser authority.

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

Invocation
Submit IZUMKFS as a batch job.

Results

On completion, the z/OSMF file system has been allocated, formatted, and mounted and the necessary directories have been created.

If the job ends with errors, see the troubleshooting actions that are listed in “Problems during configuration” on page 207.

Step 3: Prepare for z/OSMF server initialization

This topic describes the actions that you must perform so that the z/OSMF server is initialized during system IPL.

The following information is provided:

- “Started procedures for the z/OSMF server” on page 22
- “Logon procedure for the z/OSMF REST interfaces” on page 22
- “Output messages file” on page 23
- “Updating your system for the z/OSMF started procedures” on page 24
- “Verify that the z/OSMF server has sufficient authorization” on page 24
- “Define the z/OSMF started procedures to RACF” on page 24
- “Updating your system for the z/OSMF REST interfaces” on page 24
- “Updating the BPXPRMxx member of parmlib” on page 25

- “Creating an IZUPRMxx parmlib member” on page 26
- “Specifying the IZU keyword in IEASYSxx” on page 26
- “Specify the IZUPRMxx members that you want to use” on page 27
- “How the IZUPRM settings in IZUSVR1 and IEASYSxx interact” on page 27
- “Customizing the IZUSVR1 started procedure” on page 28
- “Considerations for using a named angel” on page 28

Started procedures for the z/OSMF server

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

- **ServerPac and CustomPac orders:** IBM supplies the z/OSMF procedures in the SMP/E managed proclib data set. In ServerPac and SystemPac, the data set is named SYS1.IBM.PROCLIB, by default.
- **CBPDO orders:** For a CBPDO order, the SMP/E-managed proclib data set is named SYS1.PROCLIB. However, the z/OS installer might have renamed this data set.

The z/OSMF started procedures are IZUANG1, IZUSVR1, and IZUINSTP. Be sure to use the z/OS V2R3 level of the z/OSMF started procedures because the IZUANG1 and IZUSVR1 procedures are different from those used for prior releases.

The IZUINSTP procedure is new in z/OS V2R3; it is used by the z/OSMF server for communicating with z/OS components. Do not modify IZUINSTP.

Note: Another started procedure, IZUSVR2, is provided in SYS1.SAMPLIB. If you choose not to autostart the z/OSMF server, the IZUSVR2 procedure can be used for starting the z/OSMF server manually.

Place the started procedures in a data set that is in the IEFPDSI concatenation that is used by the system to find started procedures before the primary subsystem (JES) initializes. It is recommended that this data set is the same data set that is used by JES to find started procedures after JES initializes.

Existing z/OSMF installations using older levels of the IZUANG1 and IZUSVR1 procedures must replace or update them from the new ones that are part of z/OS V2R3. Otherwise, the z/OSMF server might not start on a z/OS V2R3 system.

Logon procedure for the z/OSMF REST interfaces

IBM supplies a default logon procedure, IZUFPROC, in the PROCLIB data set. The procedure is used internally by the z/OSMF REST interfaces. Review the procedure to ensure that it is suitable for use in your environment.

Ensure that the SMP/E-managed PROCLIB data set resides in the JES PROCLIB concatenation that is used for TSO/E logon procedures. Or, copy IZUFPROC to a data set that is in the JES PROCLIB concatenation. For more information. For more information, see *z/OS TSO/E Customization*.

Note: z/OSMF uses the ISPEXEC load module in the ISPF library SISPLOAD. If your installation does not include the SISPLOAD data set in the link list, you must add SISPLOAD to the ISPLLIB DD concatenation in the logon procedure.

If you prefer, you can use a different logon procedure, if it provides the same function as the shipped IZUFPROC procedure. Specifically, the logon procedure must contain, at a minimum:

- All of the DD statements from IZUFPROC; these must reference the system data sets that contain the z/OS UNIX REXX exec programs and ISPF libraries.
- The PROC statement must specify the z/OSMF root code directory path on the ROOT variable, for example: ROOT=`'/usr/lpp/zosmf'`

If your installation configured z/OSMF to use another path for the root code directory, specify that path instead. The path must be enclosed in quotation marks, begin with a forward slash ('/'), and be fully qualified (it cannot be relative). Mixed-case file system names are allowed.

- If your installation uses permanent (non-temporary) data set for ISPFPROF, the logon procedure must be configured to allow profile sharing.
- The PROC statement must specify the Language Environment message file (MSGFILE), which is used for storing runtime messages from the z/OS data set and file REST services. For details, see "Output messages file" on page 23.

The topic "IZUPRMxx reference information" on page 36 describes options for the TSO/E logon procedure that can be specified on the COMMON_TSO statement. You can specify a different TSO/E logon procedure name, account number, and address space region size, or use the default specifications.

The defaults should be adequate for most z/OS installations. If you specify alternative values, you must ensure that the z/OSMF user and z/OSMF administrator security groups are authorized to use the logon procedure name and account number that you specify. Also, ensure that the address space region size is at least 50 MB, and that your SMFLIMxx parmlib member and IEFUSI exit allow TSO/E users to use this amount of memory.

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

Output messages file

The z/OS data set and file REST services write runtime messages to a common output messages file. The messages describe error conditions and suggest possible solutions to the errors. By default, these messages are written to SYSOUT.

Your installation can select another destination for message output by using the Language Environment MSGFILE runtime option. In the logon procedure that is used by the z/OS data set and file REST services, ensure that the message file ddname is specified, as follows:

- If your installation does not specify a message file ddname, you must ensure that the SYSOUT DD statement is specified in the logon procedure. For example:

  ```
  //SYSOUT   DD SYSOUT=H
  ```

- If your installation uses the Language Environment MSGFILE runtime option, you must ensure that the logon procedure is changed accordingly.

  To view the current MSGFILE definition on your system, you can use the following command:

  ```
  D CEE,ALL
  ```

  Which displays output, such as the following:

  ```
  PARMLIB(CEEPRM60)              MSGFILE(LEMSG,FBA,121,0,NOENQ)
  ```

  In this example, the message file ddname is LEMSG (not SYSOUT). Thus, you would modify the logon procedure, as follows:

  ```
  //LEMSG   DD SYSOUT=H
  ```

  Or, to write the data to a specific data set, you can modify the logon procedure, as follows:

  ```
  //LEMSG DD DSN=YOUR.CREATED.DATASET,DISP=OLD
  ```

  In this example, the diagnostic logs are written to the data set that you specify. Ensure that the data set is created with the format `FBA,121,0,NOENQ`.

Updating your system for the z/OSMF started procedures

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

The following setup actions are required:

- "Verify that the z/OSMF server has sufficient authorization" on page 24
- "Define the z/OSMF started procedures to RACF" on page 24.

Verify that the z/OSMF server has sufficient authorization

To ensure that the z/OSMF server can perform as required, verify that the z/OSMF started task user ID has sufficient permissions for your environment. By default, this user ID is IZUSVR, but you might have specified another user ID during the configuration process; see "Step 1: Create security definitions for the z/OSMF resources" on page 18.

The sample RACF setup jobs assign the user ID IZUSVR to both z/OSMF started tasks, IZUANG1 and IZUSVR1. You can assign different user IDs by using profiles in the RACF STARTED class or by using the RACF Started Procedures Table. For more information about assigning user IDs to started tasks, see *z/OS Security Server RACF Security Administrator's Guide*. For other considerations, see "Define the z/OSMF started procedures to RACF" on page 24.

Define the z/OSMF started procedures to RACF

The IZUSEC job contains sample RACF commands for defining the z/OSMF started procedures to the STARTED class. Figure 5 on page 24 shows the commands that are provided in the job.

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

Figure 5. RACF commands for defining the started procedures to the STARTED class

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

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

Updating your system for the z/OSMF REST interfaces

IBM supplies a default TSO/E logon procedure that is named IZUFPROC, which is used internally by the z/OSMF REST interfaces. You must include the logon procedure in your configuration and grant z/OSMF users authorization to use it. This topic describes the configuration settings and security setup that are required for the logon procedure during the configuration process.

The topic "IZUPRMxx reference information" on page 36 describes the options for the TSO logon procedure that is used by the z/OSMF REST interfaces. Your installation can customize the options for the logon procedure by using the COMMON_TSO statement in the IZUPRMxx parmlib member. You can specify the TSO logon procedure name, along with a corresponding TSO account number and address space region size. The configuration process supplies default values; you can accept the defaults or supply installation-supplied alternative values in the IZUPRMxx parmlib member.

It is recommended that you accept the defaults, which should be adequate for most z/OS installations. If you specify alternative values, you must ensure that the z/OSMF users and z/OSMF administrators security groups are authorized to the logon procedure name and account number that you specify. Also, ensure that the address space region size is at least 50 MB and that this setting is acceptable in your environment to avoid a possible system memory exception error.

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

Updating the BPXPRMxx member of parmlib

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

This topic contains the following information:

- "Ensuring that the user file system is mounted at IPL time" on page 25
- "Reviewing the IPCMSGQBYTES option of BPXPRMxx" on page 25

Ensuring that the user file system is mounted at IPL time

The file system that is used to store persistent data for z/OSMF must be automatically mounted at IPL time. This requires updates to your BPXPRMxx parmlib member.

By default, the z/OSMF file system uses the name IZU.SIZUUSRD, and is mounted in read/write mode at the location `/global/zosmf`.

This file system should be mounted automatically at IPL time. Add a MOUNT command for the file system to your currently active BPXPRMxx parmlib member. For your reference, Table 6 on page 25 provides a sample MOUNT command.

Table 6. Sample MOUNT command for the z/OSMF file system

z/OSMF file system to be mounted	MOUNT command example

Data file system	`MOUNT FILESYSTEM('IZU.SIZUUSRD') TYPE(ZFS) MODE(RDWR)`
	`MOUNTPOINT('/global/zosmf') PARM('AGGRGROW') UNMOUNT`

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

```
BPXM048I BPXOINIT FILESYSTEM SHUTDOWN INCOMPLETE.
1 FILESYSTEM IS STILL OWNED BY THIS SYSTEM.
```

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

Reviewing the IPCMSGQBYTES option of BPXPRMxx

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

It is required that you specify an IPCMSGQBYTES value of at least 20971520 (20 M) in BPXPRMxx. To set this value dynamically, you can enter the following operator command:

```
SETOMVS IPCMSGQBYTES=20971520
```

Creating an IZUPRMxx parmlib member

You do not have to create an IZUPRMxx parmlib member to get z/OSMF up and running. Instead, you might find that the z/OSMF configuration defaults are sufficient for your environment. If your z/OSMF setup requires customization, you can provide a customized IZUPRMxx member that uses installation-specific values for your configuration.

Before you create an IZUPRMxx member, review the z/OSMF defaults to determine whether the values are sufficient for your installation. For information about the IZUPRMxx member, see "IZUPRMxx reference information" on page 36.

To create an IZUPRMxx parmlib member, follow these steps:

1. Copy the sample parmlib member into the desired parmlib data set with the desired suffix.
2. Update the parmlib member as needed.
3. Specify the IZUPRMxx parmlib member or members that you want the system to use on the IZU parameter of IEASYSxx, as described in "Specify the IZUPRMxx members that you want to use" on page 27. Or, code a value for IZUPRM= in the IZUSVR1 started procedure, as described in "Customizing the IZUSVR1 started procedure" on page 28. If you specify both IZU= in IEASYSxx and IZUPARM= in IZUSVR1, the system uses the IZUPRM= value you specify in the started procedure.

Most likely, you need to specify or modify at least these parameters in IZUPRMxx:

- HOSTNAME
- HTTP_SSL_PORT
- INCIDENT_LOG UNIT
- JAVA_HOME
- RESTAPI_FILE ACCT
- COMMON_TSO ACCT
- WLM_CLASSES DEFAULT
- PLUGINS

Specifying the IZU keyword in IEASYSxx

If you use one or more IZUPRMxx parmlib members, you can specify their suffixes in an active IEASYSxx member of parmlib. Do this when you are not using the IZUPRM= parameter of the server started procedure (IZUSVR1).

You can specify the suffixes for up to 38 IZUPRMxx members on the IZU= parameter, as follows:

```
IZU={xx|(xx,...,zz)}
```

If an IZUPRMxx statement is found more than once, either in the same member or in multiple members, the value from the last one found is used. For example, suppose that your installation uses members IZUPRM01 and IZUPRM02, and you specify IZU=(01,02) in IEASYSxx. If the HOSTNAME parameter is specified in both IZUPRM01 and IZUPRM02, the system uses the HOSTNAME value from IZUPRM02. For the syntax of the IEASYSxx parmlib member, see *z/OS MVS Initialization and Tuning Reference*.

IBM-supplied default for the IZU= keyword

The IZU= keyword has no default value. If you do not specify a value for IZU=, the system uses the default values for z/OSMF or those specified in the started procedure for the server.

Regardless of whether you specify a value for IZU= in IEASYSxx, if you specify a suffix for IZUPRMxx by coding a value for IZUPRM= in the IZUSVR1 started procedure, the system uses that suffix to find IZUPRMxx.

For a description of the IZUPRMxx member and its default values, see "IZUPRMxx reference information" on page 36.

Specify the IZUPRMxx members that you want to use

If you create one or more IZUPRMxx members, IBM recommends that you define them for use by the z/OSMF server when it starts automatically at IPL time.

Do the following:

1. Specify the desired IZUPRMxx suffixes on the IZU system parameter in the IEASYSxx parmlib member, as follows:

```
IZU={xx|(xx,...,zz)}
```

2. In the IZUSVR1 started procedure, default to or define IZUPRM=PREV to specify that the z/OSMF server uses the same IZUPRMxx parmlib members as it did for the previous server start-up that was done during the life of the same z/OS IPL. Note that, while the same IZUPRMxx suffixes will be used to select the parmlib members to be used, any changes made to the members themselves will take effect when the server is restarted. See Figure 6 on page 27.

```
//IZUPRM='PREV'
⋮
//ZPARM   EXEC  PGM=IZUPARMS,REGION=0M,
// PARM='/
IZUPRM=&IZUPRM,TRACE=&TRACE,USERDIR=&USERDIR,SERVER=&SERVER'
//*
//DFLTCFG  DD  PATH='&ROOT./defaults/configuration.defaults'
//*
//STDOUT   DD  SYSOUT=&OUTCLS
//STDERR   DD  SYSOUT=&OUTCLS
//CEEDUMP  DD  SYSOUT=&OUTCLS
//*
```

Figure 6. In the IZUSVR1 started procedure, the IZUPRM parameter specifies the IZUPRMxx parmlib members to be used.

IBM recommends specifying `'IZUPRM=PREV'` to make occasional manual restarts easy and consistent.

How the IZUPRM settings in IZUSVR1 and IEASYSxx interact

Table 7 on page 27 shows how the IZUPRMxx suffixes specified on the IZU system parameter of IEASYSxx and the IZUSVR1 started procedure interact when the z/OSMF server starts automatically or is manually started:

Table 7. Interaction of IZUPRMxx settings specified in IZUSVR1 started procedure and IEASYSxx

IEASYSxx setting	IZUSVR1 procedure setting	IZUPRMxx parmlib members used
IZU - no suffixes specified	IZUPRM=PREV	No IZUPRMxx parmlib members used
	IZUPRM=SYSPARM	No IZUPRMxx parmlib members used
	IZUPRM=NONE	No IZUPRMxx parmlib members used
	IZUPRM={*xx*|(*xx*,...,*zz*)}	IZUPRMxx parmlib members that are specified in IZUSVR1 used

Table 7. Interaction of IZUPRMxx settings specified in IZUSVR1 started procedure and IEASYSxx (continued)

IEASYSxx setting	IZUSVR1 procedure setting	IZUPRMxx parmlib members used
IZU={*xx*|(*xx*,...,*zz*)}	IZUPRM=PREV	At IPL time, or if autostart is disabled, the member or members that are specified by the IZU parameter in IEASYSxx are used. If the server is restarted after it runs during the same IPL, the IZUPRMxx parmlib members last used are used for the server when it is restarted.
	IZUPRM=SYSPARM	IZUPRMxx parmlib members that are specified in IEASYSxx used
	IZUPRM=NONE	No IZUPRMxx parmlib members used
	IZUPRM={*xx*|(*xx*,...,*zz*)}	IZUPRMxx parmlib members that are specified in IZUSVR1 used

Customizing the IZUSVR1 started procedure

During IPL, the z/OS system invokes the IZUSVR1 started procedure to start the z/OSMF server. If you rename the IZUSVR1 procedure, you must specify the name of your procedure in the SERVER_PROC statement of the IZUPRMxx parmlib member.

If you need to change the defaults, see "IZUSVR reference information" on page 44.

Considerations for using a named angel

During initialization, the z/OSMF server attempts to connect to an angel process, which provides authorized services to the z/OSMF server. By default, the z/OSMF angel process is IZUANG1, which is recommended for most z/OS installations. However, you might choose to use a specific *named angel* with the z/OSMF server. If so, read this section for considerations.

If your installation uses an autostarted z/OSMF server, the angel is started internally during system initialization. If you plan to use a different angel name (not IZUANG1), you must ensure that name of the angel matches the name of its started procedure. To do so, specify the angel name on the ANGEL_PROC parameter in the IZUPRMxx member. This parameter indicates both the name of the angel and its started procedure.

If your installation starts the z/OSMF server through another means, such by operator command or through automation, you must ensure that the name specified on the ANGEL_PROC parameter in IZUPRMxx matches the angel name that is specified for the angel process. You can give an angel a name by coding the NAME parameter on the START command: **`START IZUANG1,NAME=`***proc-name*. Or, you can specify the angel name on the NAME parameter of the PROC statement of the angel started procedure before you enter the command **`START IZUANG1`**.

For a named angel, ensure that the following authorizations are done:

- z/OSMF user and z/OSMF administrator security groups are authorized to the started procedure name.
- z/OSMF server started task user ID is authorized to the angel name.

Note: The angel name must be unique on the LPAR. Two angels with the same name cannot be running concurrently on the same LPAR.

Step 4: Verify server initialization

z/OSMF is intended to be started automatically when you IPL the z/OS system.

When the z/OSMF server is initialized, a number of messages are written to the operator console, as follows.

```
SY1 $HASP100 IZUANG1 ON STCINRDR
- SY1 $HASP373 IZUANG1 STARTED
SY1 CWWKB0069I: INITIALIZATION IS COMPLETE FOR THE IZUANG1 ANGEL PROCESS.
...
SY1 $HASP100 IZUSVR1 ON STCINRDR
- SY1 $HASP373 IZUSVR1 STARTED
...
- SY1 IZUG400I: The z/OSMF Web application services are initialized.
SY1 +CWWKF0011I: The server zosmfServer is ready to run a smarter planet.
```

After the z/OSMF server is started, any optional plug-ins that your installation has selected are started. To indicate that all of the optional plug-ins are started, z/OSMF writes message IZUG024I to the server job log.

```
IZUG024I: All applications specified have started.
```

IBM recommends that you use an application-specific dynamic VIPA (DVIPA) when running one or more instances of z/OSMF in a sysplex, so that the URL does not change when the z/OSMF server is moved from one z/OS system to a different z/OS system. If you plan to run multiple AUTOSTART groups in a sysplex, the IZUPRMxx member for each one must connect to a unique combination of HOSTNAME and HTTP_SSL_PORT, and each should use a different application-specific DVIPA. For information about setting up application-specific DVIPAs, see *z/OS Communications Server: IP Configuration Reference*.

If you do not use a DVIPA, check the z/OSMF initialization message IZUG349I to confirm the link (a URL) for accessing z/OSMF. In the message, the URL is based on the configured host name. In either case, you must provide users with the new URL to use for accessing z/OSMF, as described in "Step 5: Access the z/OSMF Welcome page" on page 30.

If the server cannot be started:

- Recheck the setup steps and read the messages in the two STDERR data sets for the started task to help guide problem diagnosis. For instructions about configuring the started tasks, see "Updating your system for the z/OSMF started procedures" on page 24.
- Ensure that the TCP/IP resolver trace function is not enabled on your system. If so, disable it. If the trace is required, you can resume it after the z/OSMF server is initialized. For more information about this requirement, see "Initialization fails with messages IZUG401E and IZUG620E" on page 208.

You can prevent an automatic start of z/OSMF at IPL time. To do so, specify CONNECT on the AUTOSTART statement in the IZUPRMxx parmlib member: `AUTOSTART(CONNECT)`. You might choose to use this technique to control when the z/OSMF address spaces start, or if you prefer to use an automation product to start the z/OSMF server.

How to verify that the z/OSMF server is running

To verify that the z/OSMF angel and server are running, you can enter the **DISPLAY A** operator command for the started tasks, IZUANG1 and IZUSVR1, and route it to all systems to verify that the angel and server are running, and see what system or systems they are running on.

For example, to verify that started task IZUSVR1 is running, enter the following **DISPLAY** command:

```
ROUTE *ALL,D A,IZUSVR1
```

Figure 7 on page 30 shows an example of the expected result. In this example, IZUSVR1 is running only on the C09 system, and not on the C0A or C0B systems.

```
C0A      RESPONSES ---------------------------------------------------
CNZ4106I 15.36.13 DISPLAY ACTIVITY 707
 JOBS     M/S    TS USERS    SYSAS    INITS   ACTIVE/MAX VTAM     OAS
00405    00089    00221      00070    00835    00221/03500       00738
IZUSVR1 NOT FOUND
C0B      RESPONSES ---------------------------------------------------
CNZ4106I 15.36.13 DISPLAY ACTIVITY 513
 JOBS     M/S    TS USERS    SYSAS    INITS   ACTIVE/MAX VTAM     OAS
00297    00084    00197      00077    00557    00197/03500       00439
IZUSVR1 NOT FOUND
C09      RESPONSES ---------------------------------------------------
CNZ4106I 15.36.13 DISPLAY ACTIVITY 273
 JOBS     M/S    TS USERS    SYSAS    INITS   ACTIVE/MAX VTAM     OAS
00385    00090    00210      00068    00652    00209/03500       00522
 IZUSVR1  IZUSVR1  ZOSMF    IN   *O  A=0151   PER=NO   SMC=000
                                     PGN=N/A  DMN=N/A  AFF=NONE
                                     CT=728.445S  ET=49.08.35
                                     WUID=S0884167 USERID=IZUSVR
                                     WKL=STC_WLD  SCL=STCHI    P=1
                                     RGP=N/A      SRVR=NO  QSC=NO
                                     ADDR SPACE ASTE=1EA67440
```

Figure 7. Example result from a ***ROUTE *ALL,D A,IZUSVR1*** *command*

Step 5: Access the z/OSMF Welcome page

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

The URL for the Welcome page has the following format:

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

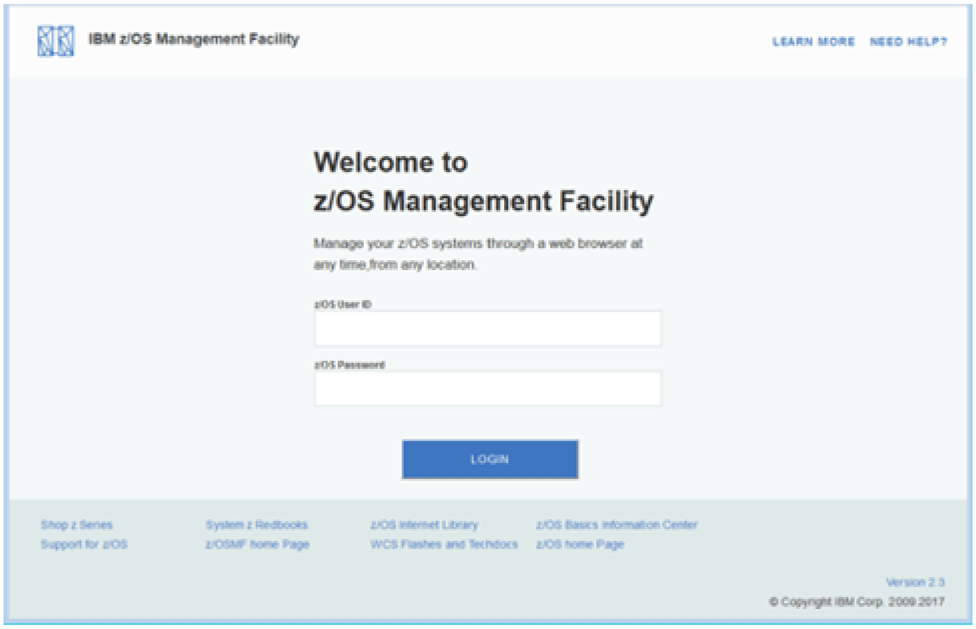
Where:

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

Displaying the Welcome page

Open a web browser to the Welcome page. For the URL, use the one provided by your network administrator for the DVIPA. Or, if you are not using a DVIPA, see message IZUG349I, which was written to the z/OSMF server job log, as described in "Step 4: Verify server initialization" on page 29.

Figure 8 on page 31 shows the Welcome page prior to login. Because the user has not yet authenticated with z/OSMF by logging in, the header displays *Welcome guest*.



Welcome to
z/OS Management Facility

Manage your z/OS systems through a web browser at any time from any location.

© Copyright IBM Corp. 2009 2017

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

If you encounter errors when you open your browser to the Welcome page, you might need to modify your workstation setup. z/OSMF includes an environment checker, which is a tool you can run to check your browser settings and workstation configuration. For more information, see "Verifying your workstation with the environment checker" on page 194.

If you are using the Mozilla Firefox browser, you might see the error message: `Secure Connection Failed`. If so, see "Certificate error in the Mozilla Firefox browser" on page 212 for information.

Step 6: Log into z/OSMF

By default, the z/OSMF configuration process creates security groups for administrator and users. You can use a user ID connected to either group to log in to z/OSMF.

About this task

The user ID that you use to log in to z/OSMF must have been used previously to authenticate on the z/OS system in another way before you can use it to log on to z/OSMF. For example, it can have been used to log on to TSO/E, or to run a batch job.

Procedure

1. In the **z/OS USER ID** field on the Welcome page, enter the z/OS user ID that you used to configure z/OSMF (the installer user ID).
2. In the **z/OS PASSWORD** field, enter the password or pass phrase that is associated with the z/OS user ID.
3. Click **LOG IN**.

Results

If the user ID and password or pass phrase are valid, you are authenticated to z/OSMF. The Welcome to IBM z/OS Management Facility tab opens in the right pane, and the navigation tree is displayed in the left pane. Only the options you are allowed to use are displayed in the navigation area. At the top right of the screen, "Welcome *<your_user_ID>*" is displayed.

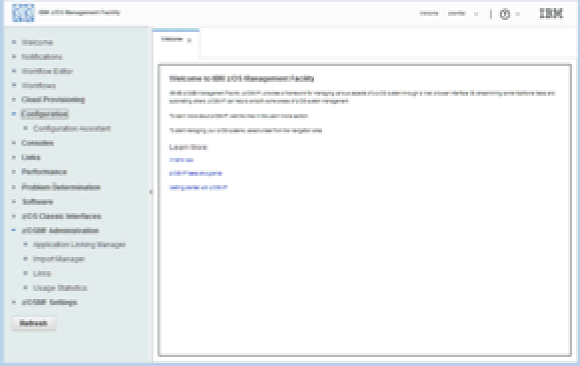


Figure 9. z/OSMF Welcome page (after login)

Figure 9 on page 32 shows the Welcome page as it appears after you log in. Shown are the base functions in the navigation area, such as Notifications and Workflows. The Welcome page work area includes the introductory topics: *What's New*, *z/OSMF tasks at a glance*, and *Getting started with z/OSMF*. For more information about z/OSMF, click any of these links to open the corresponding topic in the online help.

Figure 9 on page 32 shows the Welcome page as it might appear to a user who has access to the z/OSMF Administration and Configuration categories. In the figure, the z/OSMF Administration and Configuration categories are expanded to show the tasks for these categories. A user without access to these tasks would not see the categories.

Later, when you are satisfied with the base configuration, you can add function to z/OSMF through the addition of one or more optional plug-ins, such as the Network Configuration Assistant task. For a summary of the steps, see the project planning checklist "Adding plug-ins to your configuration" on page 10.

What to do next

To log out of z/OSMF, click the down arrow next to your user ID, and select **Log Out** from the drop-down menu.

Stopping and starting z/OSMF manually

Although z/OSMF starts automatically when you start z/OS, you can also stop and start z/OSMF manually.

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

```
STOP IZUSVR1
STOP IZUANG1
```

Figure 10 on page 32 shows an example of the expected results on a system that is running JES2:

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

stop izuang1
CWWKB0073I: THE IZUANG1 ANGEL PROCESS ENDED NORMALLY.
$HASP395 IZUANG1  ENDED
```

Figure 10. Example result from a ***STOP*** *command*

To start the z/OSMF server, you can use the **START** command from the operator console. You can enter the **START** commands for the two started tasks in either order:

```
START IZUANG1
START IZUSVR1,IZUPRM=PREV
```

Specifying IZUPRM=PREV, which is the default, ensures that you use the same set of IZUPRMxx parmlib values that were in effect in the previous instance of z/OSMF.

- The z/OSMF server is available when the following message is displayed: `CWWKF0011I: The server zosmfServer is ready to run a smarter planet`.
- Generally, you should not cancel the z/OSMF angel process because the z/OSMF applications in your system might depend on it. However, in some rare cases, you might find it necessary to cancel the angel process to avoid a system shutdown, such as a re-IPL. If you ever need to cancel the angel process or if the angel process abends, your z/OSMF administrator should cancel the z/OSMF servers with applications dependent on the successful running of the angel process. Otherwise, leaving the servers and applications running can result in a server hang condition.

Displaying the z/OSMF server settings

Use the MODIFY command with the option `'DISPLAY IZU'` to display the settings for a particular z/OSMF server.

The MODIFY command output is derived from the currently active IZUPRMxx parmlib members. This information includes:

- z/OSMF home page URI.
- AUTOSTART group name, if the command is entered for an autostarted z/OSMF server.
- One of the following enablement status values for each of the optional z/OSMF plug-ins:

  STARTED
  Plug-in is enabled.

  STOPPED
  Plug-in is disabled.

  UNSPECIFIED
  Plug-in name is not specified in a currently active IZUPRMxx parmlib member and is therefore not enabled.

For descriptions of the IZUPRMxx parmlib member settings, see "IZUPRMxx reference information" on page 36.

The MODIFY command output also includes the server start time and an indication of how long the server has been running.

The MODIFY command output is displayed in message IZUG013I.

```
F <server-name>,DISPLAY IZU
```

The parameters are:

server-name
Job name of the currently active z/OSMF server started task. By default, the job name is IZUSVR1, but your installation might use a different job name.

DISPLAY IZU
Displays the currently active settings for the z/OSMF server. This is the cumulative set of values that are derived from the IZUPRMxx members that are currently in effect.

If the command is entered incorrectly, an error message from the WebSphere Liberty run-time is displayed to describe the error. The WebSphere Liberty messages are prefixed by CW and are described online at the following link: WebSphere Liberty message descriptions (www.ibm.com/support/knowledgecenter/SS7K4U_8.5.5/com.ibm.websphere.wlp.zseries.doc/ae/rwlp_messages.html).

Example 1

Figure 11 on page 34 shows the command output for an autostarted z/OSMF server named IZUSVR1.

```
F IZUSVR1,DISPLAY IZU

 +CWWKB0004I: z/OSMF PARMLIBs DISPLAY
   IZUG013I The home page of z/OSMF server in SYSTEM(SY1)
   in AUTOSTART_GROUP(IZUDFLT) can be accessed at :
   https://XXXXXX.XXX.XXX:443/zosmf
   IZUG014I The server started at
    and has been running for  0004(hhhh):424681(mm):02(ss)

Current z/OSMF settings
Source
   HOSTNAME(XXXXXX.XXX.XXX)                          IZUPRM3S
   HTTP_SSL_PORT(443)                                    IZUPRM3S
   LOGGING('*=warning:com.ibm.zoszmf.*=info:com.ibm.zoszm
   f.environment.ui=finer')                              IZUPRM3S
   UNAUTH_USER(IZUGUEST)                                 IZUPRM3S
   SEC_GROUPS
       ADMIN(IZUADMIN)                                   IZUPRM3S
       USER(IZUUSER)                                     IZUPRM3S
       SECADMIN(IZUSECAD)                                IZUPRM3S
   SAF_PREFIX(IZUDFLT)                                   IZUPRM3S
   CLOUD_SAF_PREFIX(IYU)                                 IZUPRM3S
   KEYRING_NAME(IZUKeyring.IZUDFLT)                      IZUPRM3S
   SESSION_EXPIRE(495)                                   IZUPRM3S
   WLM_CLASSES
       LONG_WORK(IZUGWORK)                               IZUPRM3S
       DEFAULT(IZUGHTTP)                                 IZUPRM3S
   JAVA_HOME(/usr/lpp/java/J8.0_64)                      IZUPRM3S
   TEMP_DIR(/tmp)                                        IZUPRM3S
   INCIDENT_LOG UNIT(SYSALLDA)                           IZUPRM3S
   RESTAPI_FILE
      ACCT(IZUACCT)                                     IZUPRM3S
      PROC(IZUFPROC)                                    IZUPRM3S
      REGION(65536)                                     IZUPRM3S
  COMMON_TSO
      ACCT(IZUACCT)                                     IZUPRM3S
      PROC(IZUFPROC)                                    IZUPRM3S
      REGION(50000)                                     IZUPRM3S
  AUTOSTART_GROUP(IZUDFLT)                              IZUPRM3S
  AUTOSTART(LOCAL)                                      IZUPRM3S
  SERVER_PROC(IZUSVR1)                                  IZUPRM3S
  ANGEL_PROC(IZUANG1)                                   IZUPRM3S
  USER_DIR(/var/zosmf)                                  IZUPRM3S
  CSRF_SWITCH(ON)                                       IZUPRM3S

Status of z/OSMF plugins

  Configuration Assistant(STARTED)                      IZUPRM3S
  Capacity Provisioning(STARTED)                        IZUPRM3S
  Workload Management(STARTED)                          IZUPRM3S
  Resource Monitoring(STARTED)                          IZUPRM3S
  Incident Log(STARTED)                                 IZUPRM3S
  Software Management(STARTED)                          IZUPRM3S
  WebISPF(STARTED)                                      IZUPRM3S
  Sysplex Management(STARTED)                           IZUPRM3S
+CWWKB0005I: COMMAND RESPONSES COMPLETED SUCCESSFULLY FROM display izu
348
 Command Handler.
+CWWKB0002I: MODIFY COMMAND DISPLAY IZU COMPLETED SUCCESSFULLY.
```

Figure 11. MODIFY command output for an autostarted z/OSMF server

Example 2

Figure 12 on page 35 shows the command output for a standalone z/OSMF server named IZUSVR2.

```
F IZUSVR2,DISPLAY IZU

+CWWKB0004I: z/OSMF PARMLIBs DISPLAY 659
  IZUG013I The home page of z/OSMF server in SYSTEM(SY1)
  https://PEV051.POK.IBM.COM:443/zosmf
  IZUG014I The server started at
   and has been running for  0004(hhhh):424682(mm):02(ss)

  Current z/OSMF settings                               Source

  HOSTNAME(PEV051.POK.IBM.COM)                          IZUPRM3S
  HTTP_SSL_PORT(443)                                    IZUPRM3S
+CWWKB0061I CONTINUATION 1 FOR MESSAGE IDENTIFIER 1862284635  660
  LOGGING('*=warning:com.ibm.zoszmf.*=info:com.ibm.zoszm
  f.environment.ui=finer')                              IZUPRM3S
  UNAUTH_USER(IZUGUEST)                                 IZUPRM3S
  SEC_GROUPS
      ADMIN(IZUADMIN)                                   IZUPRM3S
      USER(IZUUSER)                                     IZUPRM3S
      SECADMIN(IZUSECAD)                                IZUPRM3S
  SAF_PREFIX(IZUDFLT)                                   IZUPRM3S
  CLOUD_SAF_PREFIX(IYU)                                 IZUPRM3S
+CWWKB0061I CONTINUATION 2 FOR MESSAGE IDENTIFIER 1862284635  661
  KEYRING_NAME(IZUKeyring.IZUDFLT)                      IZUPRM3S
  SESSION_EXPIRE(495)                                   IZUPRM3S
  WLM_CLASSES
      LONG_WORK(IZUGWORK)                               IZUPRM3S
      DEFAULT(IZUGHTTP)                                 IZUPRM3S
   JAVA_HOME(/usr/lpp/java/J8.0_64)                      IZUPRM3S
   TEMP_DIR(/tmp)                                        IZUPRM3S
   INCIDENT_LOG UNIT(SYSALLDA)                           IZUPRM3S
   RESTAPI_FILE
 +CWWKB0061I CONTINUATION 3 FOR MESSAGE IDENTIFIER 1862284635  662
       ACCT(IZUACCT)                                     IZUPRM3S
       PROC(IZUFPROC)                                    IZUPRM3S
       REGION(65536)                                     IZUPRM3S
   COMMON_TSO
       ACCT(IZUACCT)                                     IZUPRM3S
       PROC(IZUFPROC)                                    IZUPRM3S
       REGION(50000)                                     IZUPRM3S
   AUTOSTART_GROUP(IZUDFLT)                              IZUPRM3S
   AUTOSTART(CONNECT)                                    IZUPRM3S
 +CWWKB0061I CONTINUATION 4 FOR MESSAGE IDENTIFIER 1862284635  663
   SERVER_PROC(IZUSVR2)                                  IZUPRM3S
   ANGEL_PROC(IZUANG2)                                   IZUPRM3S
   USER_DIR(/var/zosmf)                                  IZUPRM3S
   CSRF_SWITCH(ON)                                       IZUPRM3S

   Status of z/OSMF plugins

   Configuration Assistant(STARTED)                      IZUPRM3S
   Capacity Provisioning(STARTED)                        IZUPRM3S
 +CWWKB0061I CONTINUATION 5 FOR MESSAGE IDENTIFIER 1862284635  664
   Workload Management(STARTED)                          IZUPRM3S
Resource Monitoring(STARTED)                          IZUPRM3S
   Incident Log(STARTED)                                 IZUPRM3S
   Software Management(STARTED)                          IZUPRM3S
   WebISPF(STARTED)                                      IZUPRM3S
   Sysplex Management(STARTED)                           IZUPRM3S
 +CWWKB0005I: COMMAND RESPONSES COMPLETED SUCCESSFULLY FROM display izu
 665
  Command Handler.
 +CWWKB0002I: MODIFY COMMAND DISPLAY IZU COMPLETED SUCCESSFULLY.
```

Figure 12. MODIFY command output for a standalone z/OSMF server

IZUPRMxx reference information

The IZUPRMxx parmlib member specifies options for z/OSMF. SYS1.SAMPLIB contains a copy of the IZUPRMxx member that you can copy to SYS1.PARMLIB and modify.

Syntax rules for IZUPRMxx

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

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

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

```
SESSION_EXPIRE(495)
SESSION_EXPIRE     (495)
SESSION_EXPIRE ( 495 )
```

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

  These values that you set for these parameters might require mixed casing, and therefore should be enclosed in single quotation marks:

  - HOSTNAME
  - INCIDENT_LOG UNIT
  - JAVA_HOME
  - KEYRING_NAME
  - LOGGING
  - SAF_PREFIX
  - CLOUD_SAF_PREFIX
  - CLOUD_SEC_ADMIN
  - TEMP_DIR
  - AUTOSTART_GROUP
  - USER_DIR
- Enclose any value that contains special characters in single quotation marks.
- You can use system symbols in IZUPRMxx. Suppose, for example, that your installation defines a symbol in IEASYMxx for the Java directory, such as `JAVA80='/usr/lpp/java/J8.0_64'`. To reference this symbol on the JAVA_HOME parameter in IZUPRMxx, specify the symbol as follows: `JAVA_HOME(&JAVA80)`. The example in "Syntax format of IZUPRMxx" on page 37 shows the use of a system symbol in IZUPRMxx.
- Enclose any value that is the same as a keyword in single quotation marks so that the system interprets the value as a value and not as a keyword.
- Enclose values in single quotation marks, according to the following rules:
  - Two single quotations next to each other on the same line are processed as a single quotation mark. For example, the system interprets `Jane''s file` as `Jane's file`.

  - If the length of a parameter and its value exceeds 71 characters, it requires multiple lines. Specify the first part of such a value in columns 1-71 and use as many subsequent lines as necessary to complete it. When a value spans multiple lines, place one quotation mark at the beginning of the value, stop the value in column 71 of the line, continue the value in column 1 of the next line, and complete the value with one quotation mark.
- You can specify multiple IZUPRMxx parmlib members on the IZU= parameter of IEASYSxx. If the same statement is used more than once, either in the same member or in multiple members, the value from the last occurrence is used. For example, suppose that your installation uses two members, IZUPRM01 and IZUPRM02. If the HOSTNAME parameter is specified in both IZUPRM01 and IZUPRM02, the system uses the HOSTNAME value from IZUPRM02.

Syntax format of IZUPRMxx

```
HOSTNAME('*')
HTTP_SSL_PORT(443)
INCIDENT_LOG UNIT('SYSALLDA')
JAVA_HOME('&JAVA80_HOME')     /* System symbol used to define Java home directory
*/
KEYRING_NAME('IZUKeyring.IZUDFLT')
LOGGING('*=warning:com.ibm.zoszmf.*=info:com.ibm.zoszmf.environment.ui=finer')
RESTAPI_FILE ACCT(IZUACCT) REGION(65536) PROC(IZUFPROC)
/* Common TSO logon proc, account, and region size, used by all plug-ins by default.     */
COMMON_TSO ACCT(IZUACCT) REGION(50000) PROC(IZUFPROC)
SAF_PREFIX('IZUDFLT')
CLOUD_SAF_PREFIX ('IYU')
CLOUD_SEC_ADMIN(userid)
SEC_GROUPS USER(IZUUSER),ADMIN(IZUADMIN),SECADMIN(IZUSECAD)
SESSION_EXPIRE(495)
TEMP_DIR('/tmp')
CSRF_SWITCH(ON)
SERVER_PROC(IZUSVR1)
ANGEL_PROC(IZUANG1)
AUTOSTART(LOCAL)
AUTOSTART_GROUP('IZUDFLT')
USER_DIR('/global/zosmf/')
UNAUTH_USER(IZUGUEST)
WLM_CLASSES DEFAULT(IZUGHTTP)
            LONG_WORK(IZUGWORK)

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

IBM-supplied defaults for IZUPRMxx

There is no default IZUPRMxx parmlib member. IBM provides a sample IZUPRM00 parmlib member in the SAMPLIB data set.

"Syntax format of IZUPRMxx" on page 37 shows the IBM-supplied IZUPRM00 member. Notice that the PLUGINS statement is commented out; to use it, you must remove the comment characters.

Statements and parameters for IZUPRMxx

HOSTNAME('*hostname*')

Specifies the host name, as defined by DNS, where the z/OSMF server is located. To use the local host name, enter asterisk (*), which is equivalent to @HOSTNAME from previous releases. If you plan to use z/OSMF in a multisystem sysplex, IBM recommends using a dynamic virtual IP address (DVIPA) that resolves to the correct IP address if the z/OSMF server is moved to a different system.

Rules: Must be a valid TCP/IP HOSTNAME or an asterisk (*).

Default: *

HTTP_SSL_PORT(*nnn*)

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

By default, the z/OSMF server uses the SSL protocol SSL_TLSv2 for secure TCP/IP communications. As a result, the server can accept incoming connections that use SSL V3.0 and the TLS 1.0, 1.1 and 1.2 protocols.

The z/OSMF server port uses Java SSL encryption to protect its outbound HTTPS connections. Therefore, it is not necessary (or possible) to configure AT-TLS on the z/OSMF server port. If you attempt to do so, the z/OSMF server will encounter HTTP connection failures and errors, such as the following, in the server logs directory:

- `IZUG476E: The HTTP request to the secondary z/OSMF instance "209" failed with error type "CertificateError" and response code "0"`
- `javax.net.ssl.SSLException: Unrecognized SSL message, plaintext connection?`

Rules: Must be a valid TCP/IP port number.

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

Default: `443`

INCIDENT_LOG UNIT('*device-name*')
Specifies the device to be used for storing data sets and z/OS UNIX files for the FTP jobs that are used for the Incident Log plug-in.

Rules: You must specify a generic name (such as “3390”) or an esoteric name (such as “DISK”). The esoteric name SYSALLDA, which is used by default, is automatically defined by the system to include all direct-access disk devices.

Default: `SYSALLDA`

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

Rules:

- Must be a valid z/OS UNIX System Services path name.
- Must begin with a forward slash (/).
- Must specify a full or absolute path name.

Default: `/usr/lpp/java/J8.0_64`

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

Rules: Must be the name of a valid RACF profile in the DIGTRING class.

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

Default: `IZUKeyring.IZUDFLT`

LOGGING('*trace_specification*')
Initial trace state for the z/OSMF server. These settings are read when the server is started. Changes to this value are provided, when necessary, by IBM Support.

Rules:

- 1 - 2048 characters
- Case sensitive.

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

RESTAPI_FILE ACCT(*account-number*) REGION(*region-size*) PROC(*proc-name*)
Specifies values for the TSO logon procedure that is used internally by the z/OS data set and file REST interface services. Except for the account number, it is recommended that you use the defaults, which

should be adequate for most z/OS installations. If you specify alternative values, you must ensure that the z/OSMF user and z/OSMF administrator security groups are authorized to use the logon procedure name and account number that you specify, and that the region size is at least 65536 kilobytes (KB).

All z/OSMF users must have TSO segments that are defined in the external security manager, such as RACF. Failure to have a TSO segment for each user ID prevents some z/OSMF functions from working.

ACCT(*account-number*)

Account number to be used for the TSO/E logon procedure that is used for the z/OS data set and file REST interface services.

Rules: A valid accounting number for your installation.

Default: IZUACCT

REGION(*region-size*)

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

Value range: 65536 – 2096128

Default: 65536

PROC(*proc-name*)

TSO/E logon procedure to be used for operations with the z/OS data set and file REST interface services. It is recommended that you accept the default procedure, IZUFPROC, which is supplied by IBM as a cataloged procedure in SYS1.PROCLIB.

Rules: Must be a valid partitioned data set member name.

Default: IZUFPROC

COMMON_TSO ACCT(*account-number*) REGION(*region-size*) PROC(*proc-name*)

Specifies values for the TSO/E logon procedure that is used internally for various z/OSMF activities. This setting is applicable if your z/OSMF configuration uses:

- z/OS console REST interface services
- Software Management task
- Workflows task

Except for the account number, it is recommended that you use the default values, which should be adequate for most z/OS installations. If you specify alternative values, you must ensure that the z/OSMF user and z/OSMF administrator security groups are authorized to use the logon procedure name and account number that you specify, and that the region size is at least 50 MB. For more information, see "Updating your system for the z/OSMF REST interfaces" on page 24.

All z/OSMF users must have a TSO segment that is defined in the USER profiles that are used by the external security manager, such as RACF. Failure to have a TSO segment for each user ID prevents some z/OSMF functions from working.

ACCT(*account-number*)

Account number to be used for the common TSO/E logon procedure for z/OSMF.

Rules: A valid accounting number for your installation.

Default: IZUACCT

REGION(*region-size*)

Region size (in kilobytes) to be used for the common logon procedure for z/OSMF.

Value range: 50000 – 2096128

Default: 50000

PROC(*proc-name*)

TSO/E logon procedure to be used for z/OSMF. It is recommended that you accept the default procedure, IZUFPROC, which is supplied by IBM as a cataloged procedure in SYS1.PROCLIB.

Rules: Must be a valid partitioned data set member name.

Default: IZUFPROC

SAF_PREFIX('IZUDFLT')

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

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

Rules:

- Must follow the rules for RACF profile names.
- 1 – 8 characters.

Default: IZUDFLT

CLOUD_SAF_PREFIX('IYU')

SAF profile prefix that is prepended to the names of any groups to be used for authorizing users to IBM Cloud Provisioning and Management for z/OS task activities.

Note: The IZUPRSEC sample job contains commands that include the group name for creating authorizations for IBM Cloud Provisioning and Management for z/OS. The value that is specified here must match the prefix name that you define for Cloud Provisioning authorizations in the IZUPRSEC job or by entering equivalent commands.

Rules:

- Must follow the rules for RACF profile names.
- 1 – 8 characters.

Default: IYU

CLOUD_SEC_ADMIN('*user-id*')

Specifies the security administrator user ID to be used for automatic security management in Cloud Provisioning. When specified, automatic security updates are performed under this user ID. Otherwise, if this value is omitted, security updates for Cloud Provisioning must be performed manually by your security administrator.

The user ID that is specified here must be connected to the z/OSMF security administrator group, which is named IZUSECAD by default. The IZUPRSEC job in SYS1.SAMPLIB contains a commented RACF command for creating this authorization. Minimally, this user ID requires:

- READ access to the ZMFCLOUD class resource profile IZUDFLT.ZOSMF.SECURITY.ADMIN.
- Authorization to manage resource profiles in the ZMFAPLA and ZMFCLOUD resource classes.
- Authorization to manage security groups.

During regular operations with Cloud Provisioning, your installation might periodically update Resource Management domains and tenants to add or remove users. Such changes require updates to your security setup. By specifying a user ID for the CLOUD_SEC_ADMIN keyword, you indicate that *automatic security* is to be used for performing user authorizations. If so, the authorizations are performed automatically by the Resource Management task, by using a security REXX exec that is provided by the external security manager. For example, IBM supplies the REXX exec **`izu.provisioning.security.config.rexx`** for use with RACF.

For more information, see "Automatic security management for Cloud Provisioning" on page 65.

If the CLOUD_SEC_ADMIN value is changed, the new setting applies only to domains that are created after the change. Any existing domains continue to operate with manual or automated security, based on the value that was in effect when these domains were created.

Rules:

- Must follow the rules for z/OS user IDs.

- 1 – 8 characters.

Default: None. If you do not provide a valid z/OS user ID, the Resource Management task does not perform automatic security updates.

SEC_GROUPS USER(*group-name*),ADMIN(*group-name*),SECADMIN(*group-name*)

Specifies group names for the base set of z/OSMF security groups: user, administrator, and z/OS security administrator.

USER(*group-name*)

Security group to be used for the z/OSMF user role. The user IDs that are connected to this group are considered to be z/OSMF users.

Default: IZUUSER

ADMIN(*group-name*)

Security group to be used for the z/OSMF administrator role. The user IDs that are connected to this group are considered to be z/OSMF administrators.

Default: IZUADMIN

SECADMIN(*group-name*

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

Default: IZUSECAD

SESSION_EXPIRE(*nnn*)

Amount of time (in minutes) for the session timeout. z/OSMF user sessions expire when this period elapses. For more information, see "Re-authenticating in z/OSMF" on page 216.

Value range: 30-999999

Default: 495

TEMP_DIR('*path-name*')

Temporary directory for various z/OSMF activities. This setting is applicable if your z/OSMF configuration uses:

- Incident Log task
- Workflows task.

The temporary directory is used, as follows:

- Incident Log task uses this directory for sending z/OS UNIX file attachments through FTP.
- Workflows task uses this directory for storing temporary files.

Users of these z/OSMF tasks require write access to the temporary directory. Otherwise, the task might fail with an authorization error (the user encounters message ICH408I).

In IBM Cloud Provisioning and Management for z/OS provisioning, a number of functions are performed by using workflows. For example, a software template is comprised of one or more workflows. Therefore, any user who is involved in IBM Cloud Provisioning and Management for z/OS provisioning is also a potential user of the Workflows task. You must ensure that these users have write access to the TEMP_DIR location.

Rules:

- Must be a valid z/OS UNIX path name.
- Must specify the full or absolute path name, and a maximum of 255 characters between slashes.

Default: `/tmp`

CSRF_SWITCH(*ON*/*OFF*)

Indicates whether Cross Site Request Forgery (CSRF) custom header checking is enabled for REST API requests. By default, CSRF_SWITCH is set to ON to ensure that your installation is protected against CSRF attacks. However, in some limited cases, such as for testing, you might choose to temporarily disable CSRF checking by setting CSRF_SWITCH=OFF. However, it is recommended that you leave this setting enabled to prevent CSRF attacks. For more information, see IBM z/OS Management Facility Programming Guide.

Default: ON

SERVER_PROC(*proc-name*)

Specifies the name of the started procedure that is used to start the z/OSMF server on this system. It is recommended that you use the default started procedure, which should be adequate for most z/OS installations. If you specify an alternative procedure name, ensure that the z/OSMF user and z/OSMF administrator security groups are authorized to the started procedure name.

Rules: Must specify a valid partitioned data set member name.

Default: IZUSVR1

ANGEL_PROC(*proc-name*)

Specifies the started procedure that is used to start the z/OSMF angel process on this system. It is recommended that you use the default started procedure, which should be adequate for most z/OS installations. If you specify an alternative procedure name, ensure that the z/OSMF user and z/OSMF administrator security groups are authorized to the started procedure name.

With the installation of APAR PI88651, the ANGEL_PROC statement specifies both the name of the angel process and its started procedure name.

Example: ANGEL_PROC(IZUANG1) indicates that both the angel procedure member name and angel process name are IZUANG1.

If you plan to use an alternative angel name, see "Considerations for using a named angel" on page 28 for more information.

Rules: Must specify a valid partitioned data set member name.

Default: IZUANG1

AUTOSTART(LOCAL|CONNECT)

Specifies whether the z/OSMF server is to be started automatically on this system.

The valid settings for AUTOSTART are, as follows:

LOCAL

Indicates that the system is to automatically start the z/OSMF server.

CONNECT

Indicates that the z/OSMF server is not to be autostarted on the local z/OS system.

1. IBM recommends that you specify LOCAL for all systems in a sysplex, or let it default to LOCAL, if you are using shared file systems for the z/OSMF data directory for each AUTOSTART group. If all systems in a sysplex are part of the same AUTOSTART group, the default, `/global/zosmf`, will allow this. z/OSMF will start only on one system in the sysplex, if the sysplex has only one AUTOSTART group.
2. If you have more than one AUTOSTART group in a sysplex, you should use a shared file system for each one, with a unique mount point. For example, if you have AUTOSTART groups that are named ZOSMFA and ZOSMFB, you might use `/global/zosmf/zosmfa` for the first and `/global/zosmf/zosmfb` for the second. In this case, specifying LOCAL on all systems results in z/OSMF starting on one system per AUTOSTART group.
3. When the z/OSMF server has been started automatically on another system in the same AUTOSTART group in the same sysplex, requests for z/OSMF services that originate on the local system are routed to the remote server.
4. When AUTOSTART(CONNECT) is specified for every system in a sysplex, the z/OSMF server is not autostarted on any system in the sysplex. The z/OSMF server can be started using the operator START command or by automation when no other z/OSMF server is active in the system's AUTOSTART group.

If a z/OSMF server fails, it must be restarted to restore z/OSMF operations for the autostart group. The server can be restarted on this system or another system, regardless of whether the system is specified as AUTOSTART(LOCAL) or AUTOSTART(CONNECT), using the START command or through automation.

Default: LOCAL

AUTOSTART_GROUP(IZUDFLT|*nnnnnnnn*)
Associates the local system with other systems that can share an autostarted z/OSMF server. AUTOSTART_GROUP defines a domain for z/OSMF work and associated persistent data within a sysplex. By default, one autostart group that is called IZUDFLT exists per sysplex. To associate the z/OSMF server on this system with a different autostart group, specify the desired name here.

Rules:

- Must consist of 1-32 alphanumeric characters (A-Z, a-z, 0-9) or special characters (#, $, or @).
- Alphabetic characters are case insensitive.

Default: IZUDFLT

USER_DIR
z/OSMF data directory path. By default, the z/OSMF data directory is located in `/global/zosmf`. If you want to use a different path for the z/OSMF data directory, specify that value here, for example: `USER_DIR='/the/new/config/dir'`.

Every autostart group within a sysplex must have a unique specification for USER_DIR. If you plan to use an autostarted z/OSMF server, this file system must be mounted when you IPL the system. Otherwise, the z/OSMF server cannot be autostarted.

If you specify both `USER_DIR=` in IZUPRMxx and `USERDIR=` on the PRC statement of the started procedure, the system uses the path that is specified by `USERDIR=` in the started procedure.

Rules: Must be a valid z/OS UNIX path name.

Default: `/global/zosmf/`

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

Rules:

- Must follow the rules for z/OS user IDs.
- 1 – 8 characters.

Default: IZUGUEST

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

DEFAULT(*class-name*)
WLM transaction class to be used for managing z/OSMF work, except for long-running work. See the description of the LONG_WORK(*class-name*) statement.

Rules: Must specify a valid WLM transaction class name.

Default: IZUGHTTP

LONG_WORK(*class-name*)
WLM transaction class to be used for managing the execution of long-running work.

Rules: Must specify a valid WLM transaction class name.

Default: IZUGWORK

PLUGINS(plugin-id,plugin-id,plugin-id,...)
Specifies the optional plug-ins to be made available in your configuration. Enter one or more of the plug-in identifiers that are shown in Table 8 on page 44.

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

Plug-in ID	Plug-in name
CAPACITY_PROV	Capacity Provisioning
COMMSERVER_CFG	Network Configuration Assistant
INCIDENT_LOG	Incident Log
ISPF	ISPF
RESOURCE_MON	Resource Monitoring
SOFTWARE_MGMT	Software Deployment
SYSPLEX_MGMT	Sysplex Management
WORKLOAD_MGMT	Workload Management
ZERT_ANALYZER	IBM zERT Network Analyzer

After a plug-in is enabled, you might later decide to remove it. To do so, edit the IZUPRMxx parmlib member and remove the plug-in identifier from the PLUGINS statement. Then, restart the z/OSMF server. This action removes the plug-in tasks from the z/OSMF navigation area. Any residual data that is associated with the plug-in is saved in z/OSMF, in case you decide to enable it again later.

Default: No optional plug-ins are enabled by default.

Example of IZUPRMxx parmlib member

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

- Port 30443.
- System symbol for the Java home directory. The symbol must also be defined in your IEASYMxx member.
- On startup, the system autostarts a z/OSMF server.
- The autostarted z/OSMF server processes requests from all systems that are members of the z/OSMF autostart group IZUDFLT.
- These optional plug-ins are selected: Network Configuration Assistant, Software Deployment, and Sysplex Management. The plug-ins are enabled for use when your installation completes the required host system customization. See Chapter 7, “Customizing your z/OS system for the z/OSMF plug-ins,” on page 105.

```
HTTP_SSL_PORT(30443)
JAVA_HOME('&JAVA80_HOME')     /* System symbol used to define Java home */
AUTOSTART(LOCAL)
AUTOSTART_GROUP(IZUDFLT)
PLUGINS(COMMSERVER_CFG,SOFTWARE_MGMT,SYSPLEX_MGMT)
```

IZUSVR reference information

The following parameters are supported for use in the IZUSVR1 procedure.

ROOT='*directory-path*'
z/OSMF root code directory path. This value cannot be changed.

Default: `/usr/lpp/zosmf`

WLPDIR='*directory-path*'
WebSphere Liberty server code path.

The directory path must:

- Be a valid z/OS UNIX path name
- Be a full or absolute path name
- Be enclosed in quotation marks
- Begin with a forward slash ('/').

Default: `/usr/lpp/zosmf/liberty`

OUTCLS='*output-class*'

Suitable output class for writing system output. By default, the z/OSMF procedures use output class `*`.

The value must be in quotation marks.

Default: `*`

USERDIR='*directory-path*'

z/OSMF data directory path. By default, the IZUSVR1 procedure uses the directory `/global/zosmf`. If your installation configured z/OSMF to use another path for the data directory, specify that value here, for example: USERDIR=`'/the/new/config/dir'`.

The directory path must:

- Be a valid z/OS UNIX path name
- Be a full or absolute path name
- Be enclosed in quotation marks
- Begin with a forward slash ('/').

Default: `/global/zosmf`

TRACE='Y | N'

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

Default: `N`

IZUPRM=(PREV|SYSPARM|NONE|*xx*|(*xx*,...,*zz*))

The following values are valid:

PREV

Use the IZUPRMxx suffixes, if any were used by the previous instance of z/OSMF within the current IPL. IZUPRM='PREV' is used as the default in the standard IZUSVR1 procedure. IZUPRM='PREV' behaves like IZUPRM='SYSPARM' when the system encounters it during the initial IPL time (the first use of the IZUSVR1 procedure) because there is no previous instance of z/OSMF to use.

This setting is not valid if the SERVER parameter is set to `STANDALONE`.

SYSPARM

Use the IZUPRMxx suffixes that are specified on the IZU system parameter in IEASYSxx.

This setting is not valid if the SERVER parameter is set to `STANDALONE`.

NONE

No parmlib members are specified and the z/OSMF defaults are used. For the default values, refer to the parameter descriptions in "IZUPRMxx reference information" on page 36.

***xx*|(*xx*,...,*zz*)**

Specify the specific suffixes for the IZUPRMxx parmlib member or members that you want the procedure to use. If you specify a suffix, the member must exist in your parmlib concatenation. Otherwise, the procedure cannot be started. Multiple suffixes must be enclosed in parentheses.

The following syntax forms are valid:

```
IZUPRM=PREV
```

```
IZUPRM=SYSPARM
IZUPRM=(xx,yy,zz)
IZUPRM=xx
IZUPRM=NONE
```

Note: The IZUPRMxx suffixes you specify, explicitly or implicitly, in the IZUPRM parameter of the procedure override any suffixes that are specified by using the IZU system parameter in IEASYSxx.

Default: PREV

SERVER=(AUTOSTART|STANDALONE)
Indicates the start-up behavior of the z/OSMF server, as follows:

AUTOSTART
The z/OSMF server can be started automatically during system IPL. To do so, the system uses the started procedures that you identify on the SERVER_PROC and ANGEL_PROC statements in the active IZUPRMxx parmlib member for this system or uses their defaults. It is also possible to start the server manually, by using the START command, if no other z/OSMF server is active in the system's AUTOSTART group.

STANDALONE
The system does not start the z/OSMF server automatically. It can be started manually by using the START operator command or by automation. The system uses the started procedures that you identify on the SERVER_PROC and ANGEL_PROC statements in the active IZUPRMxx parmlib member for this system or uses their defaults.

- If you choose not to autostart the z/OSMF server, you can use a started procedure similar to IZUSVR2 in SYS1.SAMPLIB for starting the z/OSMF server manually.

Default: AUTOSTART

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

Observe the following considerations:

- The amount of virtual memory that you request above 4G by using IZUMEM can be reduced by an SMFLIMxx or SMFPRMxx member of parmlib, or by an IEFUSI installation exit that lowers the memory limit for the IZUSVR1 started task.
- To indicate no limit to the amount of above-the-bar virtual storage, specify NOLIMIT.

Default: 4G

Configuring the z/OSMF key ring and certificate

The sample job IZUSEC provides RACF commands for creating a certificate authority (CA) and a server certificate. Your installation can use these authorizations for enabling Secure Sockets Layer (SSL) connections between z/OSMF instances. IZUSEC also contains commands for creating a SAF key ring, and storing the CA and server certificate in the key ring.

These constructs are named, as follows:

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

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

z/OSMF creates the CA and the server certificate if you uncomment the following commands for creating certificates in the IZUSEC job. Replace `'XXXX.XXX.XXX.XXX'` with the local host name.

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

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

In your configuration, if the key ring is owned by the z/OSMF server, and the certificate is signed by a local certificate authority (CA), you might find that the commands in IZUSEC are sufficient for your needs. If so, follow the steps in "Key ring and certificate is used by the z/OSMF server only" on page 47 to configure the key ring and certificate. However, if you plan to share key ring and certificate with other z/OSMF or Liberty servers in your enterprise, follow the steps in "Using a shared key ring and certificate for the z/OSMF server" on page 48. For more considerations, see "Tips for proper set-up" on page 49.

This information assumes the use of RACF. If you use another external security manager (ESM), consult the vendor for more information.

Key ring and certificate is used by the z/OSMF server only

In this scenario, you create a certificate and key ring for use by the z/OSMF server. The certificate is signed with local CA.

Follow these steps:

1. Update the parameter KEYRING_NAME in the IZUPRMxx parmlib member.

   ```
   KEYRING_NAME('IZUKeyring.IZUDFLT')
   ```

2. Grant the z/OSMF started task user ID READ access to the key ring and the certificate. By default, the server user ID is IZUSVR.

   ```
   PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(IZUSVR) ACCESS(READ)
   PERMIT IRR.DIGTCERT.LIST CLASS(FACILITY) ID(IZUSVR) ACCESS(READ)
   ```

3. Add the key ring to your external security manager, such as RACF.

   ```
   RACDCERT ADDRING(IZUKeyring.IZUDFLT) ID(IZUSVR)
   ```

4. Add the CA and the certificate. This example shows the use of the local CA. If you want to use a certificate that is signed by another CA, see the topic "Scenario 1: Secure server with a certificate signed by a certificate authority" in *z/OS Security Server RACF Security Administrator's Guide*.

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

   /* Create the server certificate for the z/OSMF server             */
   /* Change HOST NAME in CN field into real local host name          */
   /* Usually the format of the host name is 'XXXX.XXX.XXX.XXX'       */

   RACDCERT ID(IZUSVR) GENCERT SUBJECTSDN(CN('HOST NAME')  O('IBM') OU('IZUDFLT'))
   WITHLABEL('DefaultzOSMFCert.IZUDFLT') SIGNWITH(CERTAUTH LABEL('zOSMFCA'))
   NOTAFTER(DATE(2023/05/17))

   RACDCERT ALTER(LABEL('DefaultzOSMFCert.IZUDFLT')) ID(IZUSVR) TRUST
   ```

5. Connect the certificate to the keyring.

   ```
   RACDCERT ID(IZUSVR) CONNECT (LABEL('DefaultzOSMFCert.IZUDFLT') +
   RING(IZUKeyring.IZUDFLT) DEFAULT)

   RACDCERT ID(IZUSVR) CONNECT (LABEL('zOSMFCA') +
   RING(IZUKeyring.IZUDFLT) CERTAUTH)
   ```

Using a shared key ring and certificate for the z/OSMF server

Suppose that you have an existing key ring and certificate that is shared by multiple Liberty or z/OSMF servers. This scenario shows how to use shared key ring and certificate for the z/OSMF server.

In this scenario:

- Certificate is signed by an external CA.
- Key ring name is RING01.
- Certificate and key ring are owned by BBGSRV, which is the Liberty server user ID.

For information about obtaining this certificate and keyring, see the topic *"Scenario 7: Sharing one certificate among multiple servers"* in *z/OS Security Server RACF Security Administrator's Guide*.

To permit the z/OSMF server ID to access the keyring, certificate, and private key, you can use either the FACILITY class or the RDATALIB class, as follows:

- To use the FACILITY class:
  1. Grant the z/OSMF server user ID UPDATE access to the key ring. Because the key ring is associated with the Liberty server user ID (BBGSRV), not the z/OSMF server user ID (IZUSVR), the z/OSMF server user ID needs this access.

     ```
     PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(IZUSVR) ACCESS(UPDATE)
     ```

  2. If the FACILITY class is not already active, activate and RACLIST it:

     ```
     SETROPTS CLASSACT(FACILITY) RACLIST(FACILITY)
     ```

  3. If the FACILITY class is already active and RACLISTed, refresh it:

     ```
     SETROPTS RACLIST(FACILITY) REFRESH
     ```

  4. Permit the z/OSMF server to access the private key. It needs CONTROL access to IRR.DIGTCERT.GENCERT.

     ```
     PERMIT IRR.DIGTCERT.GENCERT CLASS(FACILITY) ID(IZUSVR) ACCESS(CONTROL)
     ```

- To use the RDATALIB class:
  1. Define the RDATALIB class:

     ```
     RDEFINE RDATALIB BBGSRV.RING01.LST UACC(NONE)
     PERMIT BBGSRV.RING01.LST CLASS(RDATALIB) ID(IZUSVR) ACCESS(CONTROL)
     ```

- If the RDATALIB class is not already active, activate it and RACLIST it, as follows:

  ```
  SETROPTS CLASSACT(RDATALIB) RACLIST(RDATALIB)
  ```

- If the RDATALIB class is already active and RACLISTed, refresh it, as follows:

  ```
  SETROPTS RACLIST(RDATALIB) REFRESH
  ```

To configure the shared key ring for the z/OSMF server, specify it on the KEYRING_NAME parameter in the IZUPRMxx parmlib member. Because the owner is not the z/OSMF started task user ID, you must create an override file that is named **`local_override.cfg`** in the user configuration directory, which is `/global/zosmf/configuration/` by default. In the override file, add the following option:

```
BOOTSTRAP_OPT=izu.ssl.key.store.owner.userid=BBGSRV
```

Tips for proper set-up

Observe the following considerations:

- The IZUSEC sample job provides commands for defining the z/OSMF server certificate and its local signing CERTAUTH certificate (a RACF defined CA). If you prefer, you can use an external CA instead of the local CA. If so, you must import the external CA (which is used to sign the server certificate) into the key ring instead of the local CA.
- The key ring must contain a personal certificate that is owned by the z/OSMF server started task user ID, which is IZUSVR by default. If this is a SITE certificate, the usage must be PERSONAL when it is connected to keyring, and the z/OSMF server started task user ID must have authority to extract the private key. See "Using a shared key ring and certificate for the z/OSMF server" on page 48.
- The certificate must be marked TRUST. A NOTRUST certificate is ignored and is not loaded on server start-up.
- If multiple PERSONAL or SITE certificates exist in the keyring, the last created certificate in the list is used by the z/OSMF server.
- If you use a PERSONAL certificate that is not owned by z/OSMF, you must take one of following actions:
  - Remove the certificate from the keyring.
  - Mark the certificate NOTRUST.
  - Grant update access to the z/OSMF server started task user ID for the following resource in the RDATALIB class:

    ```
    <ringOwner>.<ringName>.LST
    ```

Security protocols and ciphers

By default, the z/OSMF server uses the SSL protocol SSL_TLS V2 for secure TCP/IP communications. As a result, the server can accept incoming connections that use SSL V3.0 and the TLS 1.0, 1.1 and 1.2 protocols.

It is possible to modify z/OSMF to use another security protocol. To do so, indicate which protocol is to be used by specifying it in an editable file called the *override file*. The override file is read at z/OSMF server initialization and its values override the IBM defaults for the z/OSMF configuration properties.

To specify a security protocol for z/OSMF connections, do the following:

1. Create an override file that is named `local_override.cfg` and store it in the z/OSMF configuration directory. For example:

   ```
   /global/zosmf/configuration/local_override.cfg
   ```

2. In the override file, add an entry for the protocol that you want to use, as follows:

   ```
   IZU_SSL_PROTOCOL=<supportedprotocol>
   ```

   For example, to enable only TLS 1.2 connections, specify:

   ```
   IZU_SSL_PROTOCOL=TLSv1.2
   ```

For a list of valid security protocols, see the following website: https://www.ibm.com/support/knowledgecenter/en/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/csec_sslconfigs.html

It is possible to specify a cipher or list of ciphers for z/OSMF connections. To do so, specify the ciphers in your override file by using the following statement:

```
IZU_CIPHERS_LIST=" "
```

The ciphers must be entered on a single line, enclosed in quotes.

In the following example, two ciphers are specified in the override file:

```
IZU_CIPHERS_LIST="SSL_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA“
```

Chapter 4. Preparing to use Cloud Provisioning

This chapter describes how to quickly get started with IBM Cloud Provisioning and Management for z/OS, by using supplied jobs to set up a secure default domain and tenant. Included are descriptions of the key concepts and terms, and the resource profiles that must be defined. The examples in this chapter follow the default security setup for IBM Cloud Provisioning and Management for z/OS. Your installation can choose alternative values for the settings that are shown here.

IBM strongly recommends the use of groups, whenever possible, for ease of security administration. This chapter, the IZUPRSEC sample RACF setup job, and the automatic security management in IBM Cloud Provisioning and Management for z/OS all assume that you will use groups for security administration.

After you perform the initial security setup, you will not need to repeat the steps in this chapter. Instead, the Cloud Provisioning tasks will perform dynamic updates to your security environment, with one exception: The landlord group is maintained manually by your security administrator.

The instructions in this chapter assume that your installation shares its security database across the participating systems in the sysplex. If you use more than one security database, your security administrator must duplicate the Cloud Provisioning authorizations in each security database.

More information is provided in the sections that follow:

What Cloud Provisioning is

With IBM Cloud Provisioning and Management for z/OS, you can perform software provisioning for z/OS middleware. This work includes creating instances of IBM middleware, such as IBM Customer Information Control System (CICS), IBM Db2, IBM Information Management System (IMS), IBM MQ, and IBM WebSphere Application Server, and creating middleware resources, such as MQ queues, CICS regions, and Db2 databases.

Using the Cloud Provisioning tasks, your system programmers and application programmers can perform the following actions:

- System programmers:
  - Define the cloud domain, administrators for the domain, and classes of users (tenants) for the domain.
  - Prepare software services templates that provision z/OS software. Service providers add templates, associate tenants with the templates, create resource pools for the templates, test the templates, then publish them to make them available for consumers.
- System programmers or application programmers:
  - Provision software from templates, creating software services instances.
  - Manage software services instances.

For information about using the Cloud Provisioning tasks, see the online help that ships with z/OSMF. The z/OSMF online help is also available in IBM Knowledge Center. For an overview of Cloud Provisioning, see the following topic: https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zosmfcore.cloudprovisioning.help.doc/izuG00hpCloudProvisioning.html.

The basic procedure for provisioning software is:

1. Define domains and tenants.
2. Create a template, specifying the workflow, action and variables files that were provided by the software vendor.

   The template is added to the software services catalog.
3. Modify the template as needed.
4. Add the template to a tenant.
5. Create the resource pool for the tenant and the template.
6. Approve any approval records. Approval records are created when a workflow or action definition file contains an element that identifies a user ID under which a workflow step or action is to be performed (a runAsUser ID). They can also be defined for the template in general, and for a domain.
7. Test the template and ensure that it successfully creates an instance, that is, that it provisions the software and that the actions defined for the instance perform as expected.
8. Publish the template to make it available to consumers.
9. Run the template to create a software instance.

Terms you should know

Security for Cloud Provisioning is based on resources and user groups. This topic describes the key concepts and terms that security administrators should know when creating authorizations for Cloud Provisioning.

Terms and concepts are described in the following topics:

- “Resources” on page 52
- “User roles” on page 53
- “Objects” on page 54.

For a summary of the required security setup, see “Summary of security requirements for the Cloud Provisioning tasks” on page 67.

Resources

The following are the key resources in the Cloud Provisioning tasks.

Table 9. Resources for Cloud Provisioning

Resource	Description
Domain	Defines the management scope for tenants, services, and resource pools. A domain consists of one or more z/OS systems. A z/OS system can be in a single domain or in multiple domains that are managed by a single instance of z/OSMF. A cloud domain is defined by a z/OS system programmer who acts as the *landlord*. Each cloud domain is assigned one or more middleware system programmers who act as domain administrators. A base z/OSMF configuration includes one domain by default — the default domain.

Table 9. Resources for Cloud Provisioning (continued)

Resource	Description
Resource pool	Identifies the z/OS resources that are required by a z/OS software service. In a cloud domain with multiple tenants, the resource pool defines the scope of resource sharing and resource isolation. For example, a resource pool can define a range of dedicated IP addresses or ports for each tenant.
Tenant	Defines the group of users who have the authority to provision software instances. A tenant consists of a user or group of users that have contracted for the use of specified services and pooled z/OS resources that are associated with the services in a domain. A base z/OSMF configuration includes one tenant by default — the default tenant.

User roles

The following are the key roles in the Cloud Provisioning tasks.

Table 10. User roles for Cloud Provisioning

Role	Performer	Description	Group Name[1]
Landlord	System programmer	Defines the cloud domains and the associated system resources for the cloud. The landlord also designates one or more users as domain administrators.	`IYU`
Domain administrator	System programmer	Manages a domain. The domain administrator is responsible for defining services, tenants, and resource pools for the domain, and managing the relationship across tenants, services, and resource pools.	`IYU0`
Resource pool networking administrator	Network administrator	Manages the resource pool for the networking resources in the cloud, such as ports.	`IYU0RPAN`
Resource pool WLM administrator	Performance administrator	Manages the resource pool for the WLM resources in the cloud, such as WLM policies.	`IYU0RPAW`
Security administrator	Security administrator	Maintains the installation's external security manager. For example, in an installation that uses RACF as its security manager, the security administrator is responsible for creating the RACF profiles and classes that are required for Cloud Provisioning. The security administrator is a member of the z/OSMF security administrator group, which is named IZUSECAD by default. It is assumed that this user has RACF SPECIAL authority. If your installation plans to allow automatic security updates for Cloud Provisioning, you can specify this user ID for the CLOUD_SEC_ADMIN keyword in the active IZUPRMxx parmlib member for your system. For more information, see "IZUSVR reference information" on page 44.	`IZUSECAD`

Table 10. User roles for Cloud Provisioning (continued)

Role	Performer	Description	Group Name[1]
Template approver	System programmer or security administrator	Responsible for approving the templates that include user IDs for provisioning steps or actions.	N/A
Consumer	Application developer	Has access to the software services and resource pools for a tenant. This user can provision a software services from a template, and can manage the lifecycle of the software that was provisioned.	IYU000

The z/OSMF default group names are shown. Your installation can select different values for z/OSMF in the IZUPRMxx parmlib member.

Objects

The following are some basic objects that you work with in the Cloud Provisioning tasks.

Table 11. Objects for Cloud Provisioning

Object	Description
Instance, or software services instance	Represents software that is provisioned by using templates.
Template, or software services template	Represents a z/OS middleware or a z/OS middleware resource service. A template consists of workflows and input variables that can be used to provision z/OS software, actions that can be used with the provisioned software (the instance), and documentation.

For a summary of Cloud Provisioning roles, see Figure 13 on page 54

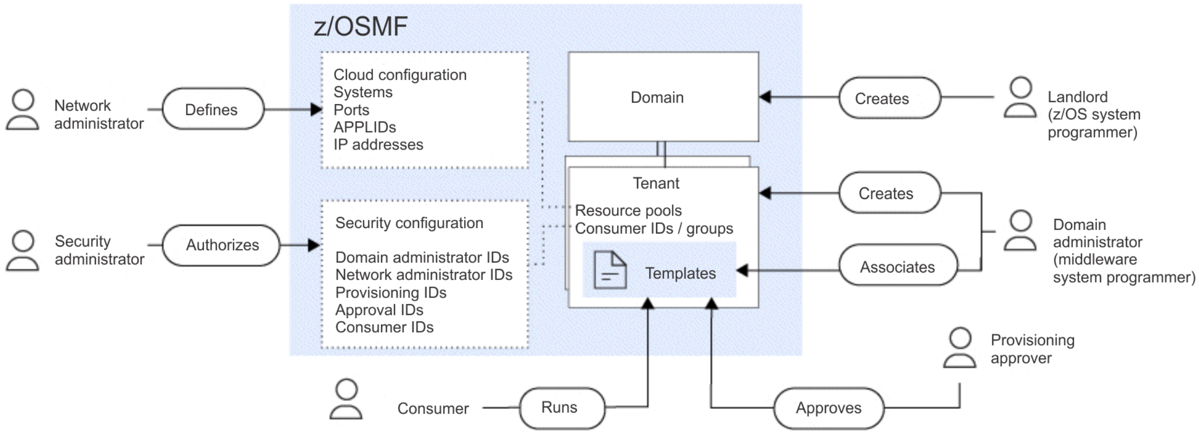


Figure 13. Roles in cloud provisioning

Help with security setup

In SYS1.SAMPLIB, the IZUPRSEC job represents the security definitions and authorizations that are needed for enabling the Cloud Provisioning functions. The job contains sample RACF commands for creating the required security authorizations.

Ask your security administrator to make a copy of this job and edit it for your environment.

Your security administrator can run the job to perform the following security setup actions:

- Define the required SAF resource profiles.
- Create the corresponding SAF security groups.
- Grant the appropriate authorizations.

As an alternative to running the IZUPRSEC job, your security administrator can perform the security setup manually. If so, see "Steps for setting up security" on page 56 for instructions.

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

Prerequisite plug-ins for Cloud Provisioning

Cloud Provisioning uses the services of other z/OSMF plug-ins. Therefore, it is recommended that you enable these plug-ins prior to using Cloud Provisioning.

Cloud Provisioning uses the services of the following z/OSMF plug-ins:

Network Configuration Assistant
Cloud Provisioning uses this plug-in to define network resource pools. Resource pools are sets of z/OS resources that are required by a software service, such as port numbers.

Resource Monitoring
Cloud Provisioning uses this plug-in for metering and capping. Metering helps you manage the use of resources by the tenant. Capping helps you limit the use of resources by the tenant.

Workload Management
Cloud Provisioning uses this plug-in to enable metering and capping, and for defining workload management (WLM) resource pools. A WLM resource pool associates cloud information, such as a tenant name and domain ID, with WLM elements, such as report classes and classification rules. You define domains and tenants with the Resource Management task in the Cloud Provisioning category.

It is recommended that you enable the plug-ins prior to using Cloud Provisioning. To do so, you must do the following:

- In your active IZUPRMxx member, ensure that the PLUGINS statement is uncommented and includes at least the following options:

```
PLUGINS(COMMSERVER_CFG,RESOURCE_MON,WORKLOAD_MGMT)
```

- Create security profiles for the tasks that are associated with each z/OSMF plug-in. IBM provides a set of IZU*nn*SEC jobs in SYS1.SAMPLIB with RACF commands to help with performing these changes. Each IZU*nn*SEC job is associated with a plug-in, as follows:

  IZUCASEC
  Network Configuration Assistant

  IZURMSEC
  Resource Monitoring

  IZUWMSEC
  Workload Management

Modify the IZU*xx*SEC jobs for your environment. The IZUCASEC and IZUWMSEC jobs include commented sections for Cloud Provisioning, which you must uncomment.

Submit the IZU*xx*SEC jobs. Or, manually create the authorizations in your external security manager.

Steps for setting up security

In a z/OSMF base configuration, the initial IBM Cloud Provisioning and Management for z/OS environment includes a default domain and default tenant to help you quickly get started. This topic describes the steps for creating the security authorizations for the default domain and default tenant.

Before you begin

This procedure assumes that your installation has already created a base z/OSMF configuration, as described in "Creating a base z/OSMF configuration" on page 17.

This procedure is presented as an alternative for users who prefer to perform the security updates manually. The authorizations that it creates are equivalent to the security setup that is performed by running the IZUPRSEC job in SYS1.SAMPLIB. If you choose to run the IZUPRSEC job instead, locate the commented sections for Cloud Provisioning and uncomment them. Be sure to review and modify the job as necessary to ensure that its definitions work in your security environment. A summary of the IZUPRSEC authorizations is provided in "Summary of security requirements for the Cloud Provisioning tasks" on page 67.

Regardless of whether you create authorizations manually or through IZUPRSEC, you need to connect one or more z/OS system programmer user IDs to the landlord group, as described in Step "2.d" on page 57 of the procedure. These users, called *landlords*, are responsible for managing the cloud environment.

About this task

Use this procedure to define an initial set of security groups, user IDs, and resource profiles for your Cloud Provisioning environment.

This procedure involves the following changes to your security database:

- Activating the necessary RACF classes
- Creating the required SAF security groups
- Defining the required SAF resource profiles
- Granting the appropriate authorizations
- Refreshing the necessary RACF classes.

The examples in this section show the commands as they would be entered for a RACF installation. If your installation uses a security manager other than RACF, your security administrator can refer to the IZUPRSEC job for examples when creating equivalent authorizations for your system.

The instructions in this procedure assume that your installation shares its security database across the participating systems in the sysplex. If you use more than one security database, your security administrator must duplicate the Cloud Provisioning authorizations in each security database.

This procedure is intended only for your initial security set-up. Later, after you complete this procedure, you use the Software Services task and Resource Management task to maintain your security environment. However, managing the landlord IDs is a manual operation that you perform in your security database. This work involves connecting users to, or removing users from, the landlord group.

Procedure

1. **Activate the ZMFCLOUD resource class and enable the RACLIST and GENERIC profiles.**

```
SETROPTS CLASSACT(ZMFCLOUD) GENERIC(ZMFCLOUD) RACLIST(ZMFCLOUD)
```

2. **Create the landlord identity.**

a) Define the landlord security group.

```
ADDGROUP IYU OWNER(some group)
```

Where IYU is the default SAF profile prefix for Cloud Provisioning. This prefix is used for the landlord group. User IDs with the landlord role have the authority to create domains, delete domains, and assign administrators within domains.

The IYU prefix is used in the examples in this procedure. Your installation can choose a different prefix by specifying it on the CLOUD_SAF_PREFIX keyword in the IZUPRMxx parmlib member. If so, substitute that value in the examples in this procedure.

b) Define the SAF profile to be used for granting users access to the landlord role.

```
RDEFINE ZMFCLOUD (IZUDFLT.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT.IYU) UACC(NONE)
```

Where IZUDFLT is the default SAF profile prefix for z/OSMF. This prefix is used for the z/OSMF resource profiles.

The IZUDFLT prefix is used in the examples in this procedure. Your installation can choose a different prefix by specifying it on the SAF_PREFIX keyword in the IZUPRMxx parmlib member. If so, substitute that value in the examples in this procedure.

c) Grant the landlord group read access to the landlord profile.

```
PERMIT IZUDFLT.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT.IYU +
CLASS(ZMFCLOUD) ID(IYU IZUADMIN) +
ACCESS(READ)
```

If you do not want all z/OSMF administrators to have the landlord role, remove the IZUADMIN group from the ID list.

d) Select a user ID to be the landlord and connect it to the landlord group.

```
CONNECT <user-id> GROUP(IYU)
```

To authorize more landlord users, connect each user ID to the landlord group.

3. **Set up security for the default domain.**

a) Define the domain administrator group for the default domain.

```
ADDGROUP IYU0 SUPGROUP(IYU)
```

Where IYU0 is the group name for domain administrators; it is defined under the Cloud Provisioning group (IYU), which is its RACF superior group.

b) Define the SAF profile to be used for authorizing users to be domain administrators.

```
RDEFINE ZMFCLOUD (IZUDFLT.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT.IYU0) UACC(NONE)
```

c) Grant the landlord group (IYU), domain administrator group for the default domain (IYU0), and z/OSMF administrator group (IZUADMIN) read access to the domain administrator profile for the default domain.

```
PERMIT IZUDFLT.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT.IYU0 +
CLASS(ZMFCLOUD) ID(IYU IYU0 IZUADMIN) ACCESS(READ)
```

If you chose not to allow all z/OSMF administrators to be able to administer the default domain, remove the z/OSMF administrator group from the ID list. If you choose to later expand this authorization, you can use the Resource Management task in Cloud Provisioning to add individual users as domain administrators.

d) Define the resource pool administrator group for networking for the default domain.

```
ADDGROUP IYU0RPAN SUPGROUP(IYU)
```

Where IYU0RPAN is the group name for networking administrators. It is defined as a subgroup of the Cloud Provisioning group.

e) Define the resource pool administrator group for WLM for the default domain.

```
ADDGROUP IYU0RPAW SUPGROUP(IYU)
```

Where IYU0RPAW is the group name for WLM administrators. It is defined as a subgroup of the Cloud Provisioning group.

4. **Set up security for the default tenant.**

a) Define the tenant consumer group for the default tenant.

```
ADDGROUP IYU000 SUPGROUP(IYU0)
```

Where IYU000 is the group name for tenant consumers. It is defined as a subgroup of the domain administrator group.

b) Define the SAF profile to be used for authorizing users to be consumers in the default tenant.

```
RDEFINE ZMFCLOUD (IZUDFLT.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT.IYU000) +
UACC(NONE)
```

c) Grant the tenant consumer group read access to the tenant consumer profile for the default tenant.

```
PERMIT IZUDFLT.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT.IYU000 +
CLASS(ZMFCLOUD) ID(IYU000) ACCESS(READ)
```

5. **Define the SAF profile to be used for authorizing users to be template approvers for the default domain.**

```
RDEFINE ZMFCLOUD (IZUDFLT.ZOSMF.TEMPLATE.APPROVERS.IYU0) UACC(NONE)
```

6. **Authorize users to be WLM administrators for the default domain.**

a) Define the SAF profile to be used for authorizing users to be resource pool administrators for WLM.

```
RDEFINE ZMFCLOUD (IZUDFLT.ZOSMF.RESOURCE_POOL.WLM.IYU0) UACC(NONE)
```

b) Grant the WLM administrator group and the z/OSMF administrator group (IZUADMIN) read access to the WLM administrator profile.

```
PERMIT IZUDFLT.ZOSMF.RESOURCE_POOL.WLM.IYU0 +
CLASS(ZMFCLOUD) ID(IYU0RPAW IZUADMIN) ACCESS(READ)
```

c) Grant the z/OSMF server user ID access to the WLM administrator profile.

```
PERMIT IZUDFLT.ZOSMF.RESOURCE_POOL.WLM.IYU0 +
CLASS(ZMFCLOUD) ID(IZUSVR) ACCESS(READ)
```

Where IZUSVR is the default user ID for the z/OSMF server, which in turn has a default name of IZUSVR1. If you assigned a different user ID to the z/OSMF server started task, specify that user ID instead.

7. **Authorize users to be network administrators for the default domain.**

a) Define the SAF profile to be used for authorizing users to be resource pool administrators for the network.

```
RDEFINE ZMFCLOUD (IZUDFLT.ZOSMF.RESOURCE_POOL.NETWORK.IYU0) UACC(NONE)
```

b) Grant the network administrator group and the z/OSMF administrator group (IZUADMIN) read access to the network administrator profile.

```
PERMIT IZUDFLT.ZOSMF.RESOURCE_POOL.NETWORK.IYU0 +
CLASS(ZMFCLOUD) ID(IYU0RPAN IZUADMIN) ACCESS(READ)
```

c) Grant the z/OSMF server user ID access to the network administrator profile.

```
PERMIT IZUDFLT.ZOSMF.RESOURCE_POOL.NETWORK.IYU0 +
CLASS(ZMFCLOUD) ID(IZUSVR) ACCESS(READ)
```

Where IZUSVR is the default user ID for the z/OSMF server, which in turn has a default name of IZUSVR1. If you assigned a different user ID to the z/OSMF server started task, specify that user ID instead.

8. **Define the ZMFAPLA profiles for the Cloud Provisioning, Workflows, Workflow Editor, and System Variables resources.**

a) Define the SAF profile to be used for authorizing users to the Software Services task.

```
RDEFINE ZMFAPLA (IZUDFLT.ZOSMF.PROVISIONING.SOFTWARE_SERVICES) UACC(NONE)
```

b) Define the SAF profile to be used for authorizing users to the Resource Management task.

```
RDEFINE ZMFAPLA (IZUDFLT.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT) UACC(NONE)
```

c) Define the SAF profile to be used for authorizing users to the Workflows task.

```
RDEFINE ZMFAPLA (IZUDFLT.ZOSMF.WORKFLOW.WORKFLOWS) UACC(NONE)
```

d) Define the SAF profile to be used for authorizing users to the Workflow Editor task.

```
RDEFINE ZMFAPLA (IZUDFLT.ZOSMF.WORKFLOW.EDITOR) UACC(NONE)
```

e) Define the SAF profile to be used for authorizing users to the System Variables resource.

```
RDEFINE ZMFAPLA (IZUDFLT.ZOSMF.VARIABLES.SYSTEM.ADMIN) UACC(NONE)
```

9. **Grant z/OSMF access to the landlord, default domain administrator, and the default tenant consumer groups.**

```
PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IYU IYU0 IYU000) ACC(READ)
```

10. **Grant the resource administrator groups access to z/OSMF.**

```
PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IYU0RPAN IYU0RPAW) ACCESS(READ)
```

11. **Grant the user groups access to the Software Services, Workflows, and Workflow Editor tasks.**

```
PERMIT IZUDFLT.ZOSMF.PROVISIONING.SOFTWARE_SERVICES +
CLASS(ZMFAPLA) ID(IYU IYU0 IYU000) ACCESS(READ)

PERMIT IZUDFLT.ZOSMF.WORKFLOW.WORKFLOWS +
CLASS(ZMFAPLA) ID(IYU IYU0 IYU000) ACCESS(READ)

PERMIT IZUDFLT.ZOSMF.WORKFLOW.EDITOR +
CLASS(ZMFAPLA) ID(IYU IYU0 IYU000) ACCESS(READ)
```

12. **Grant administrators access to the Resource Management task.**

```
PERMIT IZUDFLT.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT +
CLASS(ZMFAPLA) ID(IYU IYU0) ACCESS(READ)
```

13. **Grant the resource administrator groups access to the Workflows task and Software Services task.**

    ```
    PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ID(IYU0RPAN IYU0RPAW) ACCESS(READ)

    PERMIT IZUDFLT.ZOSMF.PROVISIONING.SOFTWARE_SERVICES +
    CLASS(ZMFAPLA) ID(IYU0RPAN IYU0RPAW) ACCESS(READ)

    PERMIT IZUDFLT.ZOSMF.WORKFLOW.WORKFLOWS +
    CLASS(ZMFAPLA) ID(IYU0RPAN IYU0RPAW) ACCESS(READ)
    ```

14. **Grant the z/OSMF administrator group the authority to modify or delete system variables by using the Systems task or a z/OSMF REST service.**

    ```
    PERMIT IZUDFLT.ZOSMF.VARIABLES.SYSTEM.ADMIN +
    CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)
    ```

15. **Create the z/OSMF security administrator role if it does not exist already.**

    These users can perform automatic security updates in the Resource Management task.

    a) Define the z/OSMF security administrator group.

    ```
    ADDGROUP IZUSECAD
    ```

    Where IZUSECAD is the default group name.

    b) Define the SAF profile to be used for authorizing users to be z/OSMF security administrators.

    ```
    RDEFINE ZMFCLOUD (IZUDFLT.ZOSMF.SECURITY.ADMIN) UACC(NONE)
    ```

    Where IZUDFLT is the z/OSMF SAF profile prefix.

    c) Grant the security administrator group read access to the security administrator profile.

    ```
    PERMIT IZUDFLT.ZOSMF.SECURITY.ADMIN CLASS(ZMFCLOUD) +
    ID(IZUSECAD) ACCESS(READ)
    ```

    Only users with read access to this profile can be selected as domain security administrators by the landlord.

16. **Enable the z/OSMF server to perform authorization checks for ZMFCLOUD class resources.**

    a) Create the SERVER class profile.

    ```
    RDEFINE SERVER (BBG.SECCLASS.ZMFCLOUD) UACC(NONE)
    ```

    b) Grant the z/OSMF server user ID access to the SERVER class profile.

    ```
    PERMIT BBG.SECCLASS.ZMFCLOUD CLASS(SERVER) ID(IZUSVR) +
    ACCESS(READ)
    ```

    Where IZUSVR is the default user ID for the z/OSMF server, which in turn has a default name of IZUSVR1. If you assigned a different user ID to the z/OSMF server started task, specify that user ID instead.

    c) Connect the z/OSMF started task user ID to the z/OSMF security administrator group (by default, IZUSECAD).

    ```
    CONNECT IZUSVR GROUP(IZUSECAD)
    ```

17. **Refresh the RACF classes to make the preceding changes effective.**

    ```
    SETROPTS RACLIST(ZMFAPLA ZMFCLOUD SERVER) REFRESH
    ```

What to do next

To verify that you configured IBM Cloud Provisioning and Management for z/OS correctly, you can use the supplied IVP template in the default domain. For the steps to follow, see "Verify that security is set up for the domain administrator" on page 61.

Verify that security is set up for the domain administrator

You can verify that security is set up correctly for the domain administrator role in IBM Cloud Provisioning and Management for z/OS. To do so, you can add an IBM-supplied template to the Software Services catalog and test run the template. This verification is referred to as performing the *installation verification procedure* or IVP for IBM Cloud Provisioning and Management for z/OS.

Before you begin

The IVP is supplied by IBM in the following location on your system: `/usr/lpp/samples/cpm-sample-ivp/`

The IVP contains the following parts:

cloud-provisioning-ivp-workflow.xml
Workflow definition file for the provisioning workflow.

cloud-provisioning-ivp.properties
Contains values for the console command and unsolicited message.

cloud-provisioning-ivp-actions.xml
Actions file that defines only a deprovision action.

cloud-provisioning-ivp-AdministratorDoc.pdf
Documentation file for the IVP.

cloud-provisioning-ivp.mf
Manifest file. This file provides a shortcut when you create the template. Rather than specifying each of the aforementioned files in the template individually, you can specify just the manifest file, then click **Load** to supply values for the other files.

About this task

The IVP contains a template that runs a provisioning workflow under your user ID.

The workflow consists of two steps:

- If Step 1 completes successfully, your user ID is set up correctly for issuing operator commands. This step issues the START command to start a non-existent job (IZUTEST), which results in an unsolicited message (IEFC452I) when the job is not found. To issue the command, the step uses a REST service.
- If Step 2 completes successfully, your user ID is set up correctly for reading messages that are written to the operations console. This step checks the result of the previous step for the presence of unsolicited message IEFC452I.

To perform the IVP, your user ID must be authorized as a domain administrator. If your installation defined security as described in "Steps for setting up security" on page 56 or by using the IZUPRSEC sample job, the user IDs in the IZUADMIN group are authorized as domain administrators.

Procedure

1. **Add the sample template to the software services catalog.**
   a) Log in to z/OSMF with a domain administrator user ID.
   b) Expand the Cloud Provisioning category in the navigation area, then select **Software Services**.
   c) Select the **Templates** tab.
   d) In the *Templates* table, click **Add Template**, then select **Standard** to use a standard template.

If **Add Template** is not available, it might be because you are not a domain administrator. If so, contact your system programmer or security administrator for assistance.

e) On the page that is displayed, supply the required values, as follows:

   1) For *Template source file*, specify the absolute z/OS UNIX path of the template manifest file for the IVP: `/usr/lpp/zosmf/samples/cpm-sample-ivp/cloud-provisioning-ivp.mf`
   2) Click **Load** to supply values for other fields on the window.
   3) Specify a template name, for example, `SampleIVP`.
   4) Optionally, select the Workflows disposition and Jobs disposition to delete the workflow and job on completion. The default is *keep*, which means that the workflow and job are preserved. You can remove them later, if you prefer.
   5) Click **OK**. The template is added to the software services catalog.

2. **Associate the template with the default tenant and create a resource pool.**

   a) In the *Templates* table, select the template by clicking the check box for the template that you created, then click **Actions** > **Associate Tenant**.

   b) On the **Associate Tenant** window, accept the defaults. For resource pool selection, ensure that **Create a dedicated resource pool** is selected.

   A *dedicated resource pool* is allocated only to this template. In contrast, a *shared resource pool* can be used by multiple templates.

   c) Click **OK**.

   The Resource Management task opens to the *Add Template and Resource Pool for Tenant* window.

   d) On the *Add Template and Resource Pool for Tenant* window, enter the following values:

   - For the software services instance name prefix, specify a meaningful value, such as `IVP`.
   - For the maximum number of software services instances, specify a low value, such as `10`.
   - The instance runs under `Job Class A`, which is the IBM default. If this job class is defined and active at your installation, you can use it. Otherwise, you must include a JOB statement with a valid job class job in the *Add Template and Resource Pool for Tenant* window. You can optionally include other JCL values on the JOB statement, such as the accounting information.

   e) Click **OK**.

   If message IYURP0013I is displayed, click **OK** to continue.

   The resource pool for the template is created with no network or workload management resources.

   f) Having used the Resource Management task to add a template to the tenant, return now to the Software task. Click the **Software Services** tab.

3. **Test run the template to provision a software instance.**

   a) In the *Templates* table, select the template that you created.

   Notice that the template is in *Draft* state, which means that the template is ready to be provisioned.

   b) Click **Actions**, then select **Test Run**.

   c) Click **OK**.

   Message IYUSC0032I is displayed to indicate that the software services instance is started.

   If you used the suggested values, the instance name is `ConsoleCommand_IVP00`.

4. **Verify that the template is provisioned.**

   a) Click the **Instances** tab.

   b) In the *Instances* table, check the state of your instance.

   - If the template state is **Being Provisioned**, click **Refresh** to refresh the table display. Provisioning might take several minutes to complete.
   - If the template state is **Provisioning-Failed**, your user ID needs an extra security authorization. Proceed to **Step 5** and **Step 6** for actions to take to resolve the problem.
   - If the template state is **Provisioned**, you started the instance successfully. Skip to **Step 7**.

5. **Determine which step failed.**
   a) In the *Instances* table, click the instance name.

      The **Instance details** tab is shown, which includes the following details about the instance:

      - Domain name (*default*)
      - Tenant name (*default*)
      - Name of the provisioning workflow. The workflow name follows the convention `ConsoleCommand_<prefix><instance-count>provision<generated string>`.

   b) Click the workflow name to navigate to the workflow.

   c) In the workflow, check for the following results:

      1) Step 1 is *Complete* or *Failed*.
      2) Step 2 is *Complete* or *Failed*.

6. **Resolve the step failure.**
   a) Work with your system programmer or security administrator to add the missing authorizations to your user ID.

      - If Step 1 failed, your user ID is not authorized to issue console commands.
      - If Step 2 failed, your user ID is not authorized to a console for viewing the unsolicited message.

      For the required authorizations, see "Resource authorizations for the z/OS console REST interface" on page 302.

   b) Repeat Steps 1-4 of this procedure.

7. **Deprovision the instance.**
   a) In **Software Services**, select the Instances tab.

   b) In the *Instances* table, select the instance that you created.

   c) Click **Actions** > **Perform** > **Deprovision**.

   d) In the Perform deprovision window, click **OK**.

What to do next

For a more advanced test of your security setup, you can create and test run a template that requires approval from a specified approver. In a production environment, the approver might be a middleware system programmer or a security administrator.

To perform this test, you create a new template based on the one you created previously. This time, you modify the workflow input variable file that was supplied with the IVP to add a performer (a *runAsUser*) and an approver for the template. You repeat some of the steps you performed in the previous procedure.

Follow these steps:

1. In the *Templates* table, select your template.
2. Create another template based on the one you created previously:
   a. Click **Actions** > **CreateBased on**.

      1) For Template name, specify the name of a new template, for example `SampleIVP2`.
      2) For Target file path, specify the name of an empty or non-existent directory, for example: `/tmp/`*`xxx`*. If the directory does not exist, z/OSMF attempts to create it.
      3) For Domain, select default to use the default domain.

   b. Click **OK** to create the template. The template is created in a draft state.
3. Associate the template with the default tenant and create a resource pool, as you did in **Step 2** of the previous procedure. If message IYURP0013I is displayed, click **OK** to continue.
4. Specify a run-as-user and an approver for the template, as follows:
   a. Select **Templates** > **Modify** > **Edit path**, which opens the Workflow Editor.

b. In the Workflow Editor, click the Input Properties tab, then specify your own user ID for the properties CONSOLE_ADMIN and CONSOLE_APPROVER.

   Tip: In Cloud Provisioning, when a template specifies a user ID under which a step must be performed, an approval record is created. Here, the user ID is referred to as the *runAsUser ID* for the step. Approval records must be approved by the approvers before the template can be run or published.

   In the example that follows, IBMUSER is specified for both properties.

```
# Licensed Materials - Property of IBM
# 5650-ZOS
# Copyright IBM Corp. 2018
#
# Status = HSMA230
#----------------------------------------------------------------------------
#
# This is the command that will be issued
# via the z/OSMF REST Consoles API
#
CONSOLE_CMD = S IZUTEST#
# This is  the unsolicited keyword that
# z/OSMF REST Consoles API should expect
# in the response to the CONSOLE_CMD.
#
UNSOL_KEY_TO_DETECT = IEFC452I#
# This is the console Administrator user ID
# that should be used to issue the
# z/OSMF REST Consoles API if the user ID
# running the template does not have appropriate
# authorization.
#
CONSOLE_ADMIN = ibmuser
#
# This is the console Approval user ID used
# for approving the usage of the console
# Administrator user ID specified by
# the ADMIN_CONSOLE variable.
#
CONSOLE_APPROVER = ibmuser
```

c. Click **Save** to save the input properties file.

d. Close the Workflow Editor window.

5. In the **Templates** > **Modify** page, click **OK**.
6. In the *Templates* table, check the state of the template:
   - If the template state is **Pending security update**, click **Refresh** to refresh the table display.
   - If the state is **Draft pending approval**, the template requires approval. Resolving this state requires the approver user ID that you specified earlier to approve the template.
7. Approve the template:

   a. In the *Templates* table, select the template that is in **Draft pending approval** state, then click **Actions** > **Approvals**.

   b. In the Approvals window, review the item to approve.

   c. To approve the template, select the row, then click **Actions** > **Approve**.

   d. Return to the *Templates* table. Notice that the template is now **Draft approved**.
8. Test run the template by clicking **Actions**, then **Test Run**.
9. In the *Instances* table, check the state of your instance:
   - If the template state is **Being Provisioned**, click **Refresh** to refresh the table display. Provisioning might take several minutes to complete.
   - If the template state is **Provisioning-Failed**, resolve the errors for any failed steps and test run the template again.
   - If the template state is **Provisioned**, you started the instance successfully.
10. Deprovision the instance.

You can remove the template from the software services catalog when you are done.

Exploring this function further: Try running the IVP with other user IDs specified for the CONSOLE_ADMIN and CONSOLE_APPROVER properties. When these user IDs do not match, Cloud Provisioning automatically generates an additional approval record for your security administrator to approve. This behavior helps to ensure that security is maintained when provisioning is performed under different user IDs.

In the Workflow Editor:

- For CONSOLE_ADMIN, specify the user ID under which the template is to run. This user ID requires the authority to enter commands from the z/OS operations console. Typically, this person is a middleware system programmer who provisions templates at your company.
- For CONSOLE_APPROVER, specify the user ID of the person who must approve the provisioning of the template.

Avoid using a functional user ID for the approver. The approver user ID must be able to log in to z/OSMF.

Automatic security management for Cloud Provisioning

During regular operations with Cloud Provisioning, your installation periodically adds or removes users for domains and tenants. Such changes require immediate updates to your security setup. If you select *automatic security* for Cloud Provisioning in the Resource Management task, or accept the default, these changes are performed for you automatically.

Automatic security management can be performed by using the following methods:

- Security REXX exec that is provided by the vendor of the ESM. For example, IBM supplies the REXX exec **`izu.provisioning.security.config.rexx`** for use with RACF.

Automatic security is enabled by default. It uses the z/OS service **`R_SecMgtOper`** to perform security operations directly and synchronously. In contrast, the REXX exec is run by a Resource Management workflow.

This method requires that a valid user ID be specified for the CLOUD_SEC_ADMIN keyword in the IZUPRMxx parmlib member.

Using a REXX exec for automatic security processing

This method of automatic security uses the security REXX exec from IBM or one that you have obtained from another vendor. When installed, the security REXX exec is owned by the z/OSMF server user ID (by default, IZUSVR) and is intended for use by security administrators only. The exec can be updated only by users in the z/OSMF security administrator group (by default, IZUSECAD).

If your installation uses a security manager other than RACF, you must obtain a REXX exec with equivalent security commands from your vendor and store it on your system.

Then, do the following:

1. Ensure that a security REXX exec is installed on your system. The IBM-supplied REXX exec for RACF is already included in the following directory on your system:

   ```
   /global/zosmf/configuration/workflow/izu.provisioning.security.config.rexx
   ```

   For other security managers, you must obtain an equivalent REXX exec from your vendor and install it on your system.
2. Recycle the z/OSMF server to ensure that the security configuration properties file is created with the default IBM content and the correct ownership and permission settings.

   From the operator console, enter the operator commands in the following sequence: **STOP IZUSVR1** > **START IZUSVR1** > **STOP IZUSVR1**.

   It is not necessary to stop or restart the z/OSMF angel process (IZUANG1).

3. With the z/OSMF server stopped, ask your security administrator to do the following:

   a. Locate the security configuration properties file on your system:

      ```
      /global/zosmf/configuration/workflow/izu.provisioning.security.config.properties
      ```

      Locate the following property:

      ```
      security-configuration-rexx-location=
      ```

      By default, the property identifies the location of the IBM-supplied security REXX exec.

   b. To use a different REXX exec, edit the property so that it refers to the location of the replacement REXX exec. The location can be a sequential data set, partitioned data set (PDS), or z/OS UNIX path and file name.

      If the REXX exec resides in a data set, observe the following naming conventions:

      - Enter the fully qualified data set name, including the member name if you are using a PDS.
      - Do not enclose the data set name in quotation marks.

      Example:

      ```
      security-configuration-rexx-location=SYS1.REXX(ZOSMFSEC)
      ```

      If the REXX exec resides in a z/OS UNIX file, observe the following naming conventions:

      - Enter the full path name, beginning with the forward slash (/) and including the file name, or a relative path.
      - The name cannot contain any path segments, such as `/./` or `/../`

      Example:

      ```
      security-configuration-rexx-location=/u/cloud/zosmf/workflow/
      izu.provisioning.security.config.rexx
      ```

   c. Save the properties file.

4. Restart the z/OSMF server. From the operator console, enter the START command for the z/OSMF server started task: `START IZUSVR1`

Applying service to the IBM-supplied REXX exec

IBM can ship service updates to Cloud Provisioning, which might include updates to the **`izu.provisioning.security.config.rexx`** exec. If you use the IBM exec, it is recommended that you apply the PTFs to stay current with the latest level of the exec.

If your installation uses a modified version of the IBM-supplied security REXX exec for RACF security:

- Ensure that the security configuration properties file identifies the location of the exec on your system. See the procedure for updating the properties file in "Using a REXX exec for automatic security processing" on page 65.
- Work with your security administrator to reconcile any differences between your copy of the exec and a new version from IBM.

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

Summary of security requirements for the Cloud Provisioning tasks

This topic describes the resources that must be defined, and the groups that must be permitted to the resources.

The security configuration requirements for Cloud Provisioning are described in the sections that follow. Typically, these permissions are created by your security administrator.

- "Select the Legacy Special user ID" on page 67
- "Group name prefix for Cloud Provisioning user groups" on page 67
- "Class activation for Cloud Provisioning" on page 67
- "Resource authorizations for security administrators" on page 68
- "Resource authorizations for network administrators" on page 68
- "Resource authorizations for WLM administrators" on page 68
-
- "Resource authorizations for the Cloud Provisioning user roles" on page 69
- "Resource authorizations for the z/OSMF server user ID" on page 71.

Select the Legacy Special user ID

During configuration, you select a user ID to use for authorizing groups to the domain. This user ID, which is referred to as the *Legacy Special* user ID, requires RACF SPECIAL authority. It must also be connected to the z/OSMF security group for z/OSMF security administrators (IZUSECAD, by default). Typically, this user is a security administrator.

The Legacy Special user is the first landlord to be defined for your configuration. After Cloud Provisioning is configured, remember the Legacy Special user ID and keep it active for future operations. For example, with the Legacy Special user ID, you can authorize other users to be landlords, or use the Resource Management task to create more domains and add default domain administrators.

Group name prefix for Cloud Provisioning user groups

Your installation must define a SAF group name to be used for Cloud Provisioning groups. The group name is prepended to the names of the groups that represent the various roles in Cloud Provisioning, such as landlords, domain administrators, and tenants. The group name prefix is used in the RACF commands for defining groups.

By default, the value IYU is the group name prefix for Cloud Provisioning groups. Your installation can select a different SAF group prefix. To do so, specify the value in the IZUPRMxx parmlib member. For more information, see the description of the CLOUD_SAF_PREFIX statement in "IZUPRMxx reference information" on page 36.

Your installation can select a different group name prefix for user groups. If so, substitute that value in the examples. If you plan to use a different value, ensure that it is 1-3 characters (alpha-numeric, uppercase, or the following special characters: $, and @).

Class activation for Cloud Provisioning

For a RACF installation, the security class ZMFCLOUD must be active when you configure Cloud Provisioning. The RACF commands for activating the class (with generic profile checking activated) are included in the IZUSEC job. If your installation uses an external security manager other than RACF, ask your security administrator to create equivalent commands for your environment.

The ZMFCLOUD class requires the RACLIST option. If you change the profiles, you must refresh the ZMFCLOUD class to have the changes take effect.

Table 12 on page 68 describes the class activation for Cloud Provisioning.

Table 12. Class activation for Cloud Provisioning

Class	Purpose	RACF command for activating

ZMFCLOUD	Allow the user to use the z/OSMF core functions and tasks that are related to Cloud Provisioning. z/OSMF defines a resource name for each core function and task that is related to Cloud Provisioning.	`SETROPTS CLASSACT(ZMFCLOUD) GENERIC(ZMFCLOUD) +`
		`RACLIST(ZMFCLOUD)`

Resource authorizations for security administrators

Users who perform security administration tasks should be members of the z/OSMF security administrator group (IZUSECAD, by default). This group requires an OMVS group ID (GID).

Security administrators require access to the system resources that are used by the Cloud Provisioning tasks. For more information, see Table 13 on page 69.

Resource authorizations for network administrators

Network administrators require access to the Network Configuration Assistant task, and to system resources that are used by the Network Configuration Assistant task. For more information, see Table 13 on page 69.

Resource authorizations for WLM administrators

WLM administrators require access to resources, such as those that are protected by the profile MVSADMIN.WLM.POLICY. For more information, see "Updating z/OS for the Workload Management plug-in" on page 146 and Table 13 on page 69.

Resource authorizations for application developers

z/OSMF includes the Swagger interface, which allows application developers and other users to display format descriptions of the Cloud Provisioning REST APIs. To enable the use of Swagger at your installation, define the Swagger resources in your external security manager, and grant READ access to the appropriate users and groups.

On a system with RACF as the security manager, you can use the following commands:

1. Define the allAuthenticatedUsers resource profile:

```
RDEFINE EJBROLE IZUDFLT.com.ibm.ws.management.security.resource.allAuthenticatedUsers UACC(NONE)
```

   The profile includes the z/OSMF SAF profile prefix, which is IZUDFLT, by default. Your installation can select a different SAF profile prefix for z/OSMF in the IZUPRMxx parmlib member.

2. To give users and administrators access to Swagger, grant them READ access to the allAuthenticatedUsers resource profile:

```
PERMIT IZUDFLT.com.ibm.ws.management.security.resource.allAuthenticatedUsers CLASS(EJBROLE)
ID(IZUUSER IZUADMIN) ACCESS(READ)
```

   By default, the user and administrator groups for z/OSMF are `IZUUSER` and `IZUADMIN`.

3. Create an administrator role for Swagger by defining the Administrator resource profile:

   ```
   RDEFINE EJBROLE IZUDFLT.com.ibm.ws.management.security.resource.Administrator UACC(NONE)
   ```

4. Assign the administrator role to the z/OSMF administrator group, which is IZUADMIN by default:

   ```
   PERMIT IZUDFLT.com.ibm.ws.management.security.resource.Administrator CLASS(EJBROLE)
   ID(IZUADMIN) ACCESS(READ)
   ```

For more information about the Cloud Provisioning REST services, see *IBM z/OS Management Facility Programming Guide*.

Resource authorizations for the Cloud Provisioning user roles

Table 13 on page 69 describes the authorization requirements for the common user roles in Cloud Provisioning. The IZUSECPR job includes sample RACF commands for creating these authorizations on your system. A procedure for creating these authorizations manually is shown in "Steps for setting up security" on page 56.

Table 13. Security setup requirements for Cloud Provisioning user roles

Resource class	**Resource name**	**Who needs access?**	**Type of access required**	**Why**
DATASET	*your_stack_include_dataset*	TCP/IP stack started task ID.	READ	Allows the TCP/IP stack to read the include data set when the TCP/IP stack is started. This definition is applicable only when your installation uses discrete or generic profiles to protect data set access.
DATASET	*your_stack_dynamic_update_dataset*	TCP/IP stack started task ID.	READ	Allows the TCP/IP stack to read the VARY OBEY data set that IBM Cloud Provisioning and Management uses to dynamically update the TCP/IP stack. This definition is applicable only when your installation uses discrete or generic profiles to protect data set access.
EJBROLE	*<SAF-prefix>* .IzuManagementFacilityProvisioning .izuUsers	• z/OSMF users group (IZUUSER) • z/OSMF administrators group (IZUADMIN)	READ	Allow the user to connect to the Software Services and Resource Management tasks.
EJBROLE	*<SAF-prefix>* .com.ibm.ws.management.security.resource.Administrator	• z/OSMF users group (IZUUSER) • z/OSMF administrators group (IZUADMIN)	READ	Allow the user to act as administrator for the Swagger function in z/OSMF.

Table 13. Security setup requirements for Cloud Provisioning user roles (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
EJBROLE	*<SAF-prefix>* .com.ibm.ws.management. security.resource.allAuthenticatedUsers	z/OSMF administrators group (IZUADMIN)	READ	Allow the user to use Swagger to display information about the z/ OSMF REST APIs. For information about the REST services, see *IBM z/OS Management Facility Programming Guide*. .
ZMFAPLA	*<SAF-prefix>*.ZOSMF.IBM_ CLOUDPORTAL.MARKETPLACE. CONSUMER	Consumers and domain administrators	READ	Allow the user to use the marketplace to provision and manage software services.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.IBM_ CLOUDPORTAL. MARKETPLACE. ADMIN	Domain administrators	READ	Allow the user to control which services are published to the marketplace, and manage the services to which consumers have subscribed.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.PROVISIONING. RESOURCE_MANAGEMENT	• Landlord group • Domain group • Resource pool network administrator group • Resource pool WLM administration group • z/OSMF security administrators group (IZUSECAD)	READ	Allow the user to access the Resource Management task.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.PROVISIONING. SOFTWARE_SERVICES	• Landlord group • Domain group • Tenant group • Resource pool network administrator group • Resource pool WLM administration group • z/OSMF security administrators group (IZUSECAD) • Consumers and domain administrators	READ	Allow the user to access the Software Services task.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.VARIABLES. SYSTEM.ADMIN	z/OSMF administrators group (IZUADMIN)	READ	Allow the user to access the system variable definitions.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.WORKFLOW. EDITOR	• Landlord group • Domain group • Tenant group	READ	Allow the user to access the Workflow Editor task in z/OSMF.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.WORKFLOW. WORKFLOWS	• Landlord group • Domain group • Tenant group • z/OSMF users group (IZUUSER) • z/OSMF administrators group (IZUADMIN)	READ	Allow the user to access the Workflows task in z/OSMF.

Table 13. Security setup requirements for Cloud Provisioning user roles (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
ZMFAPLA	*<SAF-prefix>*.ZOSMF. WORKLOAD_MANAGEMENT. WORKLOAD_MANAGEMENT.ENWRP	- z/OSMF administrators group (IZUADMIN) - WLM resource pool administration group	READ	Allow the user to access the WLM Resource Pooling (WRP) functions of z/OSMF. Using a WRP definition, the user can associate cloud information (tenant name, domain ID, template type, service levels supported) with WLM elements (report classes and classification rules).
ZMFCLOUD	*<SAF-prefix>*.ZOSMF.PROVISIONING. RESOURCE_MANAGEMENT. *tenantGroupID*	Tenant group	READ	Allow the user to act as a tenant.
ZMFCLOUD	*<SAF-prefix>*.ZOSMF.PROVISIONING. RESOURCE_MANAGEMENT. *domainGroupID*	Domain group	READ	Allow the user to act as a domain administrator.
ZMFCLOUD	*<SAF-prefix>*.ZOSMF. RESOURCE_POOL.NETWORK. *domainGroupID*	Resource pool network administration group	READ	Allow the user to act as a network resource pool administrator.
ZMFCLOUD	*<SAF-prefix>*.ZOSMF. RESOURCE_POOL.WLM.*domainGroupID*	Resource pool WLM administration group	READ	Allow the user to act as a WLM resource pool administrator.
ZMFCLOUD	*<SAF-prefix>*.ZOSMF.SECURITY.ADMIN	z/OSMF security administrators group (IZUSECAD)	READ	Allow the user to access the security administration resource.
ZMFCLOUD	*<SAF-prefix>*.ZOSMF.TEMPLATE. APPROVERS.*domainGroupID*	Template approvers	READ	Allow the user to act as a cloud domain level template approver.
ZMFCLOUD	*<SAF-prefix>*.ZOSMF.TEMPLATE. APPROVERS.*domainGroupID*. *templateName*	Template approvers	READ	Allow the user to approve the specified template.
ZMFCLOUD	*<SAF-prefix>*.ZOSMF.TEMPLATE. INSTANCE.*domainGroupID*. *templateInstanceName*	Template instance owner	READ	Allow the user to access the specified template registry instance.

Resource authorizations for the z/OSMF server user ID

Table 14 on page 71 describes the Cloud authorizations that you must create for the z/OSMF server. By default, the server user ID is IZUSVR1. However, your installation might have selected a different user ID for the server during z/OSMF configuration. The IZUSEC job includes sample RACF commands for creating these authorizations on your system.

Table 14. Authorizations required for the z/OSMF server user ID

Resource class	Resource name	Type of access required	Why
DATASET	*your_stack_include_dataset*	ALTER	Allows the Network Configuration Assistant task to write to the configured include data sets when a network resource is provisioned or deprovisioned. There is one include data set for each stack that is defined for IBM Cloud Provisioning and Management for z/OS. This definition is applicable only when your installation uses discrete or generic profiles to protect data set access.

Table 14. Authorizations required for the z/OSMF server user ID (continued)

Resource class	Resource name	Type of access required	Why
DATASET	*your_stack_dynamic_update_dataset*	ALTER	Allows the Network Configuration Assistant task to write to the configured dynamic updates data sets when a network resource is provisioned or deprovisioned. There can be one dynamic update data set for each stack that is defined for IBM Cloud Provisioning and Management for z/OS. This definition is applicable only when your installation uses a discrete or generic profile to protect data set access.
OPERCMDS	MVS.VARY.TCPIP.OBEYFILE	CONTROL	Allows the Network Configuration Assistant task to issue the **VARY TCPIP OBEYFILE** command for IBM Cloud Provisioning and Management for z/OS. This definition is applicable only when your installation uses the OPERCMDS class to restrict access to the **VARY TCPIP OBEYFILE** command.
OPERCMDS	MVS.MCSOPER.ZCDPLM*	READ	Allows the Network Configuration Assistant task to issue various operator commands for IBM Cloud Provisioning and Management for z/OS. The console name for this extended MCS console is the text string ZCDPLM that is appended with the MVS sysclone value of the system of the z/OSMF instance.
OPERCMDS	MVS.DISPLAY.XCF	READ	Allows the Network Configuration Assistant task to issue the display XCF operator command for IBM Cloud Provisioning and Management for z/OS. This definition is applicable only when your installation uses the OPERCMDS class to restrict access to the display XCF operator command.
OPERCMDS	MVS.ROUTE.CMD.*sysname*	READ	Allows the Network Configuration Assistant task to issue the **ROUTE** operator command for IBM Cloud Provisioning and Management for z/OS. This definition is applicable only if the installation uses this profile to restrict the use of the **ROUTE** command.
SERVAUTH	EZB.NETWORKUTILS.CLOUD.*mvsname*	READ	Allows the Network Configuration Assistant task to issue operator commands for IBM Cloud Provisioning and Management for z/OS. *mvsname* is the name of the system where z/OSMF is running.
SERVAUTH	EZB.NETSTAT.*mvsname.tcpprocname*.CONFIG	READ	Allows the Network Configuration Assistant task to issue the command **NETSTAT CONFIG**. This definition is applicable only when your installation uses the SERVAUTH class to restrict usage of the **NETSTAT** command. When this definition is applicable, IZUSVR must be authorized for each stack defined for IBM Cloud Provisioning and Management for z/OS.
SERVAUTH	EZB.NETSTAT.*mvsname.tcpprocname*.VIPADCFG	READ	Allows the Network Configuration Assistant task to issue the command **NETSTAT VIPADCFG**. This definition is applicable only when your installation uses the SERVAUTH class to restrict usage of the **NETSTAT** command. When this definition is applicable, IZUSVR must be authorized for each stack that is defined for IBM Cloud Provisioning and Management for z/OS.

Table 14. Authorizations required for the z/OSMF server user ID (continued)

Resource class	Resource name	Type of access required	Why
SERVER	BBG.SECCLASS.ZMFCLOUD	READ	Allows the z/OSMF server to perform access checks in the ZMFCLOUD class.
ZMFCLOUD	*<SAF-prefix>*.ZOSMF. RESOURCE_POOL.NETWORK. *domainGroupID*	READ	Allows the z/OSMF server to access to the network administrator profile.
ZMFCLOUD	*<SAF-prefix>*.ZOSMF. RESOURCE_POOL.WLM.*domainGroupID*	READ	Allows the z/OSMF server to access the WLM administrator profile.

Cloud provisioning marketplace

Cloud Provisioning includes a sample marketplace, which makes software services available to marketplace consumers, and also includes functions for marketplace administrators. The sample marketplace is created when you import the Cloud Portal application into z/OSMF. Doing so adds the Marketplace and Marketplace Administration tasks to the z/OSMF navigation area.

The marketplace is provided as-is, and is intended as a sample for learning purposes only.

If you plan to configure the marketplace, you have system customization to perform, as described in the following topics:

- "Creating SAF authorizations for the marketplace tasks" on page 73
- "Creating role-based authorizations for the marketplace tasks" on page 74
- "Adding or removing the marketplace tasks" on page 74
- "Configuring the marketplace tasks" on page 74
- "Creating and managing subscriptions" on page 75
- "Modifying the Cloud Portal application" on page 75

Creating SAF authorizations for the marketplace tasks

To enable the marketplace on your system, ask your security administrator to create the authorizations that are shown in Table 15 on page 73.

Table 15. User authorization requirements for the marketplace tasks

Resource class	Resource name	Who needs access?	Type of access required	Why
ZMFAPLA	*<SAF-prefix>*.ZOSMF.IBM_CLOUDPORTAL .MARKETPLACE. CONSUMER	Consumers and domain administrators	READ	Allows the user to use the marketplace to provision and manage software services.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.IBM_CLOUDPORTAL .MARKETPLACE. ADMIN	Domain administrators	READ	Allows the user to control which services are published to the marketplace, and manage the services to which marketplace consumers have subscribed.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.PROVISIONING .SOFTWARE_SERVICES	Consumers and domain administrators	READ	Allows the user to access the Software Services task.

Creating role-based authorizations for the marketplace tasks

To perform tasks in the marketplace, users require the following authorizations:

- To associate a domain with the marketplace, the user must be defined to the domain as a domain administrator.
- To publish services to the marketplace, the user must be defined as either a domain administrator or a consumer in the domain that is associated with the marketplace.
- To subscribe to a published service, the user must be permitted to the template that is associated with the service.

Adding or removing the marketplace tasks

The Cloud Portal application is included with z/OSMF in the following location:

```
/usr/lpp/zosmf/samples/cloudportal
```

To add the marketplace tasks to z/OSMF, follow these steps:

1. Open the Import Manager task in z/OSMF.
2. Specify the following properties file as input:

   ```
   /usr/lpp/zosmf/samples/cloudportal/cloudportal.properties
   ```

3. Click **Import**.

Later, if you want to remove the marketplace tasks from z/OSMF, you can do so by using a property file to remove the tasks.

Follow these steps:

1. Open the Import Manager task in z/OSMF.
2. Specify the following properties file as input:

   ```
   /usr/lpp/zosmf/samples/cloudportal/cloudportaldelete.properties
   ```

3. Click **Import**.

If the removal is successful, the tasks are removed from z/OSMF. If an error occurs, resolve the error and import the property file again.

For more information, see the online help for the Import Manager task.

Configuring the marketplace tasks

When you access the marketplace for the first time, you are prompted as a marketplace administrator to supply information about the marketplace domain and its published services.

Specifically, you must provide the following information:

- On the **Settings** tab, specify the domain name for the marketplace. Specify one domain name only. Changing the domain name causes the deletion of any services that are published to the marketplace.

  Also, on the **Settings** tab, you can indicate whether instances that are provisioned outside of the marketplace can be displayed in the **My Subscriptions** tab and **Manage Subscriptions** tab for marketplace consumers. By default, only entries that are provisioned in the marketplace can be displayed to marketplace consumers.

- On the **All Services** tab, select which services are to be published to the marketplace. You can add any of the templates that are listed in the Published Service Catalog to which you are permitted in the domain for the marketplace.

Creating and managing subscriptions

When a service is published, marketplace consumers can subscribe to it, which causes the service to be provisioned. In the Marketplace task, consumers can use the **All Services** tab to subscribe to any services to which they are permitted.

The marketplace provides the following functions for viewing and managing subscriptions:

- On the **My Subscriptions** tab, marketplace consumers can view their subscriptions. The tab shows which services are provisioned both within and outside of the marketplace, and allows consumers to take actions on the services.
- On the **Manage Subscriptions** tab, marketplace administrators can view all subscriptions in the marketplace domain to which they are permitted. The tab allows the administrator to manage the services to which marketplace consumers have subscribed.

The **All Services** tab has different functions, depending on whether you access the tab as a consumer (from the Marketplace task) or an administrator (from the Marketplace Administration task). In the Marketplace Administration task, the **All Services** tab allows the user (an administrator) to select which services are to be published to the marketplace.

Modifying the Cloud Portal application

The Cloud Portal application is provided as-is; you can modify it according to your needs. To modify the application, copy it to a local directory, and make changes to the copy.

To copy the application to another directory, you can use a command like the following, where /myuserdir is a local directory of your choice:

```
cp -R /usr/lpp/zosmf/samples/cloudportal /myuserdir/
```

To add or remove the modified Cloud Portal application from z/OSMF, you can use the Import Manager task, as described in "Adding or removing the marketplace tasks" on page 74. As input, specify the following properties file:

```
/myuserdir/cloudportal/cloudportal.properties
```

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

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

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

The core functions of z/OSMF include the following:

- Welcome task
- Notifications and Notification Settings tasks
- Workflows task
- Workflow Editor task
- Application Linking Manager task
- Import Manager task
- Links task
- FTP Servers task
- Resource Management task
- Software Services task
- Systems task
- Usage Statistics task
- z/OS Operator Consoles task
- z/OSMF online help system.

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

You can add significant function to z/OSMF through the addition of optional plug-ins. To help you decide, this chapter provides a functional overview of each plug-in.

Enabling an optional plug-in involves the following activities:

- In your active IZUPRMxx member, ensure that the PLUGINS statement is uncommented and includes the plug-in ID for the required plug-in. See "Statements and parameters for IZUPRMxx" on page 37.
- Create security profiles for the tasks that are associated with the plug-in. IBM provides a set of IZU*nn*SEC jobs in SYS1.SAMPLIB with RACF commands to help with performing these changes. Each IZU*nn*SEC job is associated with a plug-in, as described in Chapter 6, "Setting up security for the z/OSMF plug-ins," on page 101.
- Perform the various z/OS system customization updates that are associated with each plug-in, as described in Chapter 7, "Customizing your z/OS system for the z/OSMF plug-ins," on page 105.

Note: After a plug-in is enabled, you might later decide to remove it. To do so, edit the IZUPRMxx parmlib member and remove the plug-in identifier from the PLUGINS statement. Then, restart the z/OSMF server. This action removes the plug-in tasks from the z/OSMF navigation area. Any residual data that is associated with the plug-in is saved in z/OSMF, in case you decide to enable it again later.

Table 16 on page 78 shows which optional plug-ins are available for configuration in z/OSMF. By default, z/OSMF does not include any of the optional plug-ins.

Table 16. z/OSMF optional plug-ins and associated tasks

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

Your decision on which plug-ins to configure will depend in part on your installation's readiness to perform the various z/OS system customization updates associated with each plug-in. When planning for the plug-ins, review the system setup requirements for each plug-in, as described in Chapter 7, “Customizing your z/OS system for the z/OSMF plug-ins,” on page 105.

External plug-ins

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

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

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

Overview of z/OSMF system management tasks

Depending on the plug-ins that your installation selects during configuration, z/OSMF offers various system management tasks (functions). Brief overviews of each task are provided in the following sections:

- "Capacity Provisioning task overview" on page 79
- "IBM zERT Network Analyzer task overview" on page 81
- "Incident Log task overview" on page 82
- "ISPF task overview" on page 83
- "Network Configuration Assistant task overview" on page 85
- "Notifications in z/OSMF" on page 86
- "Notification Settings task overview" on page 87
- "Resource Monitoring task overview" on page 88
- "Resource Management task overview" on page 89
- "Software Services task overview" on page 90
- "Software Management task overview" on page 91
- "Sysplex Management task overview" on page 92
- "System Status task overview" on page 93
- "Usage Statistics task in z/OSMF" on page 94
- "Workflows task overview" on page 95
- "Workload Management task overview" on page 96
- "z/OS Operator Consoles task overview" on page 98.

For authenticated users, context sensitive help is accessible always to assist with these tasks. In each page, you can click on the help link to open a new window with help information for the page. Similarly, each message that is displayed in the interface includes a link to the help for that message.

To allow users in your installation to access z/OSMF, your security administrator must authorize the users to resources on the z/OS system. As an aid to your security administrator, z/OSMF includes sample REXX programs with RACF commands for authorizing users. More information about security is provided in Chapter 6, "Setting up security for the z/OSMF plug-ins," on page 101.

When you implement z/OSMF in your environment, it is recommended that your installation follow the concept of *roles* to group similar users for managing user access to tasks. z/OSMF supports your installation's security requirements for specific user permissions for each of the tasks. Role definitions can be managed entirely through your external security manager, such as RACF, based on your requirements and policies. Information about the z/OSMF profiles and resources is provided in Chapter 6, "Setting up security for the z/OSMF plug-ins," on page 101.

Capacity Provisioning task overview

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

Figure 14 on page 80 shows the main page for the Capacity Provisioning task.

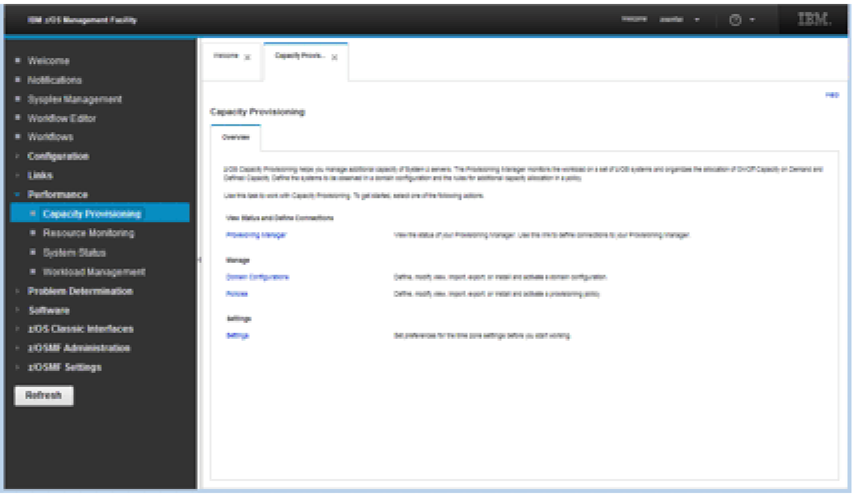


Figure 14. Capacity Provisioning task main page

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

Key features

With the Capacity Provisioning task, you can:

- **Manage domain configurations and policies.** You can manage domain configurations and policies. Specifically, you can define new domain configurations and policies, or view or modify existing domain configurations or policies.
- **Install domain configurations and policies.** You can transfer a domain configuration or policy from the z/OSMF repository to the domain configuration or policy repository of your domain.
- **Activate domain configurations and policies.** You can:
  - Change the domain configuration that the provisioning manager uses to control the domain. To do so, select a different configuration from the domain configuration repository.
  - Activate policies from the policy repository.

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

- Active policy. This report contains information about the active policy and its status. You can view detailed information about each policy element.

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

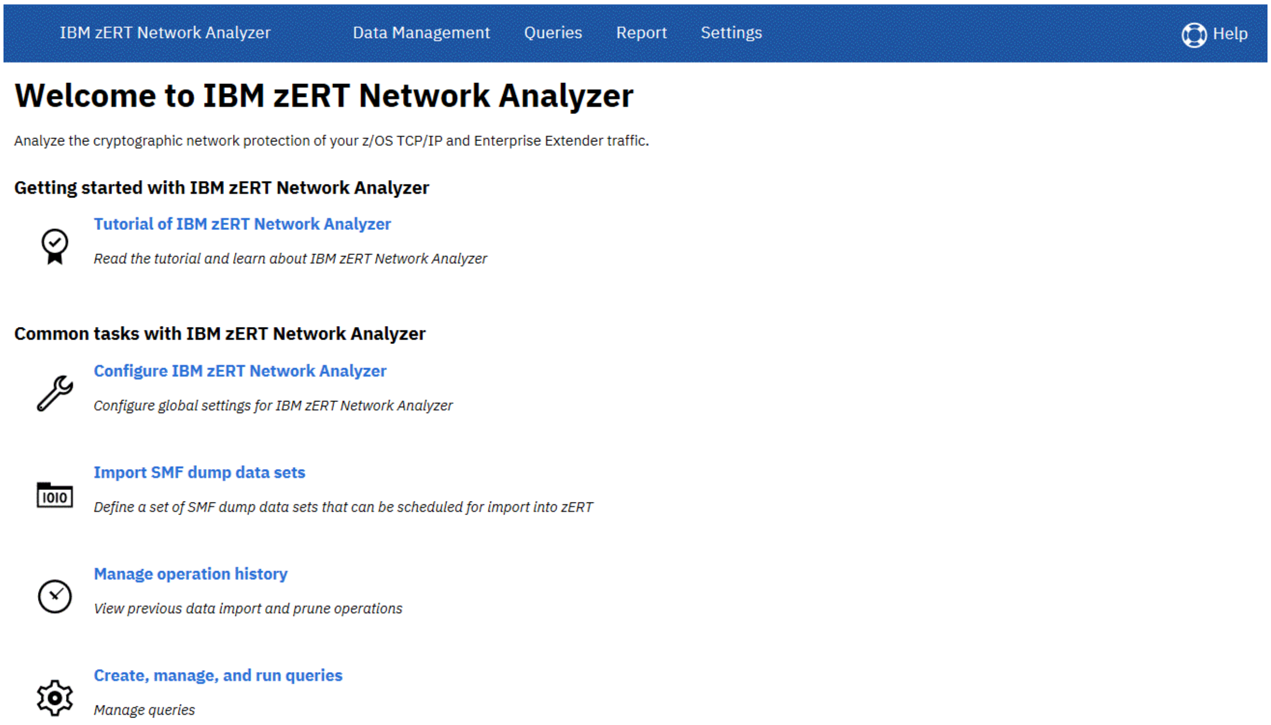
IBM zERT Network Analyzer task overview

The IBM z/OS Encryption Readiness Technology (zERT) Network Analyzer task can help you quickly analyze SMF data to identify the cryptographic protection characteristics of TCP and Enterprise Extender (EE) connections with local endpoints on your z/OS system.

Use one of the following options to open the IBM zERT Network Analyzer task:

- When using the z/OSMF traditional view, expand the **Analysis** category in the navigation area, and select **IBM zERT Network Analyzer**.
- When using the z/OSMF desktop view, click the **IBM zERT Network Analyzer** icon .

The main page for the IBM zERT Network Analyzer task is displayed, as shown in Figure 15 on page 81.



Welcome to IBM zERT Network Analyzer

Analyze the cryptographic network protection of your z/OS TCP/IP and Enterprise Extender traffic.

Getting started with IBM zERT Network Analyzer

Tutorial of IBM zERT Network Analyzer

Read the tutorial and learn about IBM zERT Network Analyzer

Common tasks with IBM zERT Network Analyzer

Configure IBM zERT Network Analyzer

Configure global settings for IBM zERT Network Analyzer

Import SMF dump data sets

Define a set of SMF dump data sets that can be scheduled for import into zERT

Manage operation history

View previous data import and prune operations

Create, manage, and run queries

Manage queries

Figure 15. IBM zERT Network Analyzer task main page

Key features

With the IBM zERT Network Analyzer task, you can:

- Import one or more SMF dump data sets into the IBM zERT Network Analyzer database. The IBM zERT Network Analyzer task inspects the SMF records in the data sets, extracts information from zERT Summary (type 119, subtype 12) SMF records, and organizes the extracted SMF information by security sessions. zERT Summary records report interval-based statistical and cryptographic protection information about security sessions which are used by TCP and EE connections.
- Create queries to filter the security sessions in the IBM zERT Network Analyzer database by date, system, connection, or cryptographic characteristics.

- Run your queries and examine the results in a tabular output. You can view the results at a summary level, or you can drill down and view individual security session information at a more granular level of detail.
- Prune unwanted security session information from the IBM zERT Network Analyzer database.
- Export the results of your queries to a comma-separated values (CSV) format file, which you can then further manipulate by using the spreadsheet or analysis tool of your choice.

For more information, see the **Welcome** page in the IBM zERT Network Analyzer task. The **Welcome** page provides extensive help that can be referenced at any time.

To experience the functions provided by IBM zERT Network Analyzer, see the **Tutorial** page in the IBM zERT Network Analyzer task.

You can also find more detailed information about the IBM zERT Network Analyzer task at the IBM Knowledge Center for z/OS Communications Server:

Incident Log task overview

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

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

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

Figure 16 on page 82 shows a sample view from the Incident Log task.

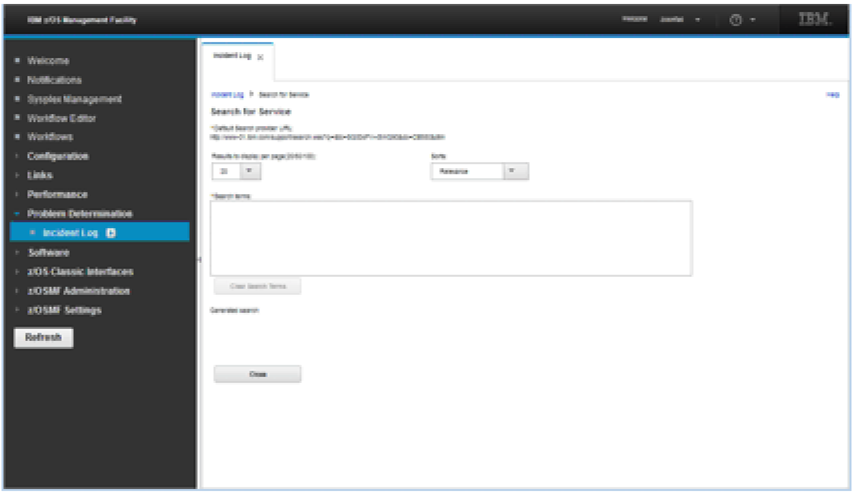


Figure 16. Incident Log task sample view

Key features

With the Incident Log task, you can:

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

- **Browse the logs collected for an incident.** When an incident occurs, the Incident Log task collects and saves the associated SVC dumps and diagnostic log snapshots. You can browse the error log, error log summary, and operations log.
- **Allow the next dump of an incident with the same MVS symptom string.** The Incident Log task provides the ability to update the DAE data set so that you can capture the next instance of an SVC dump being suppressed by DAE.
- **Send diagnostic data and attachments to IBM or another vendor for further diagnostics.** The Incident Log task provides a wizard that you can use to send diagnostic data and additional attachments to IBM or another vendor. You can send files using standard FTP or SFTP, or using the z/OS Problem Documentation Upload Utility (PDUU), which supports parallel FTP and encryption. For more information about PDUU, see z/OS MVS Diagnosis: Tools and Service Aids.
- **Associate the incident with problems recorded in other problem management systems.** The Incident Log task allows you to correlate an incident with an IBM problem number, an ISV problem number, or with a problem record in your installation's problem management system.
- **Track additional information with an incident.** The Incident Log task allows you to specify additional information that you want to track about an incident, such as who is assigned to resolve the issue, which business applications are impacted, which component is the source of the issue, and which solution has been implemented.
- **Monitor the status of an FTP or SFTP job.** An FTP or SFTP job is created when you send diagnostic data to IBM or another vendor. The Incident Log task allows you to browse or cancel these jobs and view or delete the status of these jobs.

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

ISPF task overview

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

Through the ISPF task, you can:

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

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

To open the ISPF task, in the navigation area, expand the z/OS Classic Interfaces category and select **ISPF**. The main page for the ISPF task is displayed, as shown in Figure 17 on page 84.

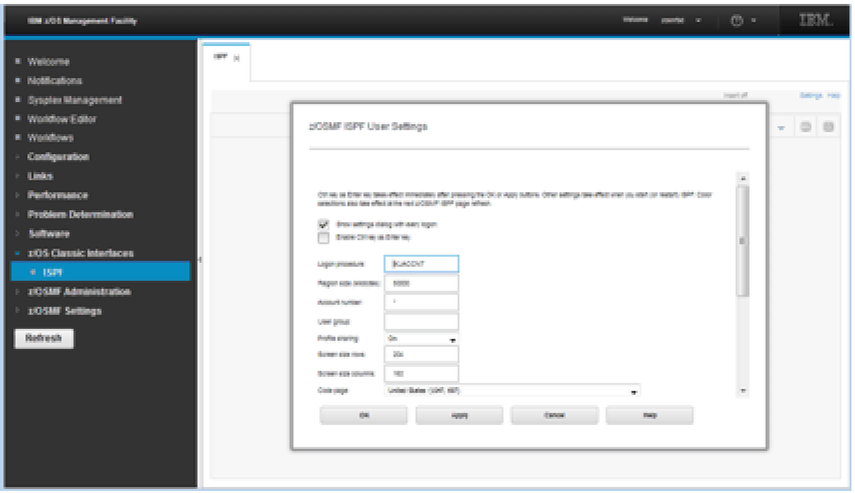


Figure 17. ISPF task main page

Usage considerations for ISPF task users

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

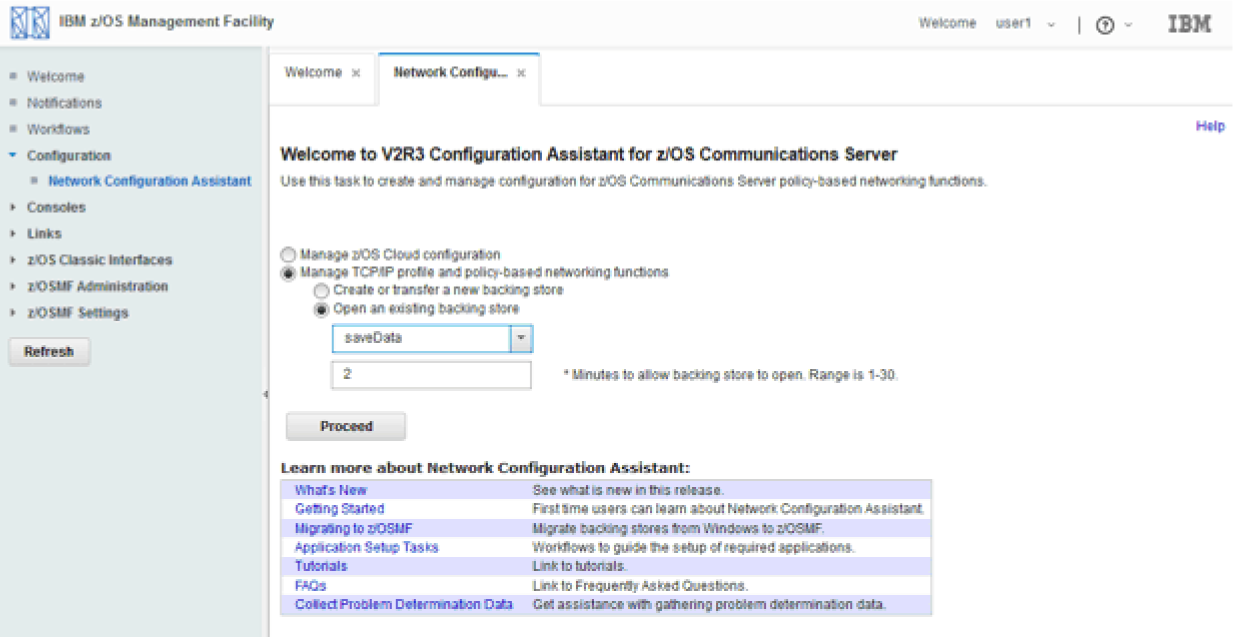
- z/OS creates an address space for each ISPF task session that is started. An individual z/OSMF user can have up to ten active ISPF task sessions. To conserve system resources, your system is limited to a total of 50 active ISPF task sessions at any one time.
- In some situations, logon pre-prompt exits IKJEFLD and IKJEFLD1 that set the Don't Prompt control switch bit on can prevent z/OSMF ISPF users from logging on, or might not work with z/OSMF ISPF.
- z/OSMF users can be canceled by the MVS operator, based on user ID, and ASID if needed. In some cases, however, these operations might have to be performed twice to take affect.
- An ISPF task user cannot:
  - Switch to TSO/E native mode from within a z/OSMF ISPF session.
  - Log in remotely to TSO/E on another z/OS system from z/OSMF ISPF.
  - Log in without specifying a valid TSO/E account number in the Account Number field of the ISPF task.
  - Use full-screen applications that run outside of ISPF, such as OMVS, TELNET, or GDDM.
  - Receive TSO/E messages, such as messages from MVS operators or users in TSO/E native mode.
  - Use commands that are not allowed in traditional ISPF, such as TSOLIB and LOGON.
- Most VTAM terminal macros used by full screen applications, such as GTTERM or STFSMODE, are not supported under z/OSMF ISPF. However, you can use the GTSIZE macro or GETDEVSZ macro to obtain the screen size.
- Broadcast messages are not displayed at log on. You can view these messages in the TSO Messages window, which is displayed by clicking the TSO Messages link in the ISPF task main page.
- Session Manager is not available; do not specify ADFMDF03 in your logon procedure. Your logon procedure should use the IBM-supplied terminal monitor program, IKJEFT01, which is specified on the PGM= operand of the EXEC statement.
- In some cases, the Attention button might appear to be unresponsive. If so, try clicking the Attention button again. If the request times out, click Cancel to interrupt the process. Doing so should have the same effect as clicking the Attention button.
- The REXX and CLIST system terminal ID (SYSTERMID) variable is blank for z/OSMF ISPF task sessions.

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

Network Configuration Assistant task overview

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

To open the Network Configuration Assistant task, in the navigation area, expand the Configuration category and select **Network Configuration Assistant**. The main page for the Network Configuration Assistant task is displayed, as shown in Figure 18 on page 85.



Welcome to V2R3 Configuration Assistant for z/OS Communications Server

Use this task to create and manage configuration for z/OS Communications Server policy-based networking functions.

○ Manage z/OS Cloud configuration
● Manage TCP/IP profile and policy-based networking functions
  ○ Create or transfer a new backing store
  ● Open an existing backing store
    saveData
    2 * Minutes to allow backing store to open. Range is 1-30.

Learn more about Network Configuration Assistant:

What's New	See what is new in this release.
Getting Started	First time users can learn about Network Configuration Assistant.
Migrating to z/OSMF	Migrate backing stores from Windows to z/OSMF.
Application Setup Tasks	Workflows to guide the setup of required applications.
Tutorials	Link to tutorials.
FAQs	Link to Frequently Asked Questions.
Collect Problem Determination Data	Get assistance with gathering problem determination data.

Figure 18. Network Configuration Assistant task main page

Key features

With the Network Configuration Assistant task, you can:

- Create and manage policies for the following TCP/IP, policy-based networking disciplines:
  - IP Security, including IKE
  - Network Security Services (NSS)
  - Defense Manager daemon (DMD)
  - Application Transparent TLS (AT-TLS)
  - Intrusion Detection Services (IDS)
  - Policy-based Routing (PBR)
  - Quality of Service (QoS)
  - TCP/IP Profile configuration
  - Import of existing TCP/IP configuration
  - Cloud Policy (Cloud)
- Provide Application Setup Task within the z/OSMF Workflow. Review Application Setup Task using the z/OSMF Workflow Tutorial in Network Configuration Assistant Help.
- Provision network resources using the IBM Cloud Provisioning and Management for z/OS services.

The Network Configuration Assistant task is used for managing network resources in the IBM Cloud Provisioning and Management for z/OS provisioning tasks. For setup considerations, see Chapter 4, “Preparing to use Cloud Provisioning,” on page 51.

For information about getting started, see the Welcome page in the Network 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 Network Configuration Assistant task at the z/OS Communications Server web site: http://www.ibm.com/software/network/commserver/zos/support/.

Notifications in z/OSMF

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

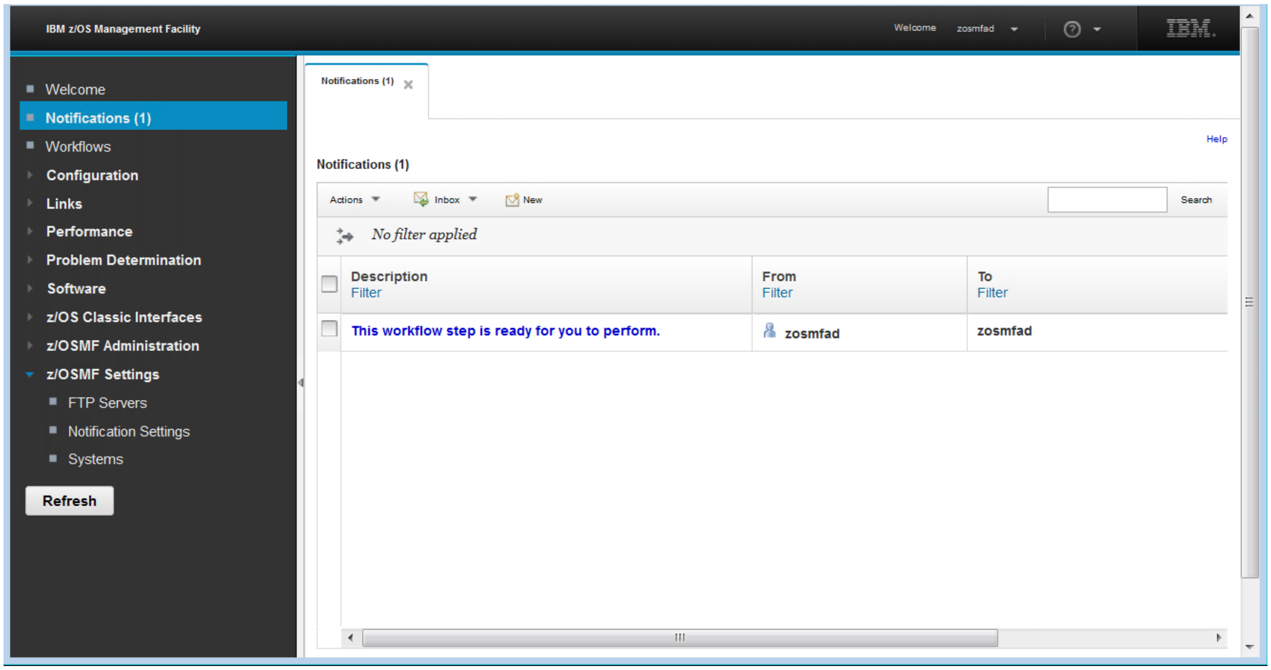
When you have unread notifications, the Notifications task is shown in bold in the navigation area with the number of unread notifications in the form '(*x*).' For example, **Notifications (3)** indicates that you have three unread notifications. When no unread notifications await your attention, the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

You might receive notifications that have been assigned to:

- Your user ID specifically
- A SAF security group to which your user ID is connected, as defined through your security management product, such as RACF
- One of the predefined z/OSMF roles to which your user ID can be assigned:
  - z/OSMF User
  - z/OSMF Administrator
  - z/OS Security Administrator.

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

To display the Notifications task, select **Notifications** in the navigation area. The Notifications task main page is displayed, as shown in Figure 19 on page 86. The Notifications task is displayed for all authenticated users. Unauthenticated guest users cannot access this task.



Notifications (1)

□	Description Filter	From Filter	To Filter
□	This workflow step is ready for you to perform.	zosmfad	zosmfad

Figure 19. Notifications main page

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

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

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

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

Notification Settings task overview

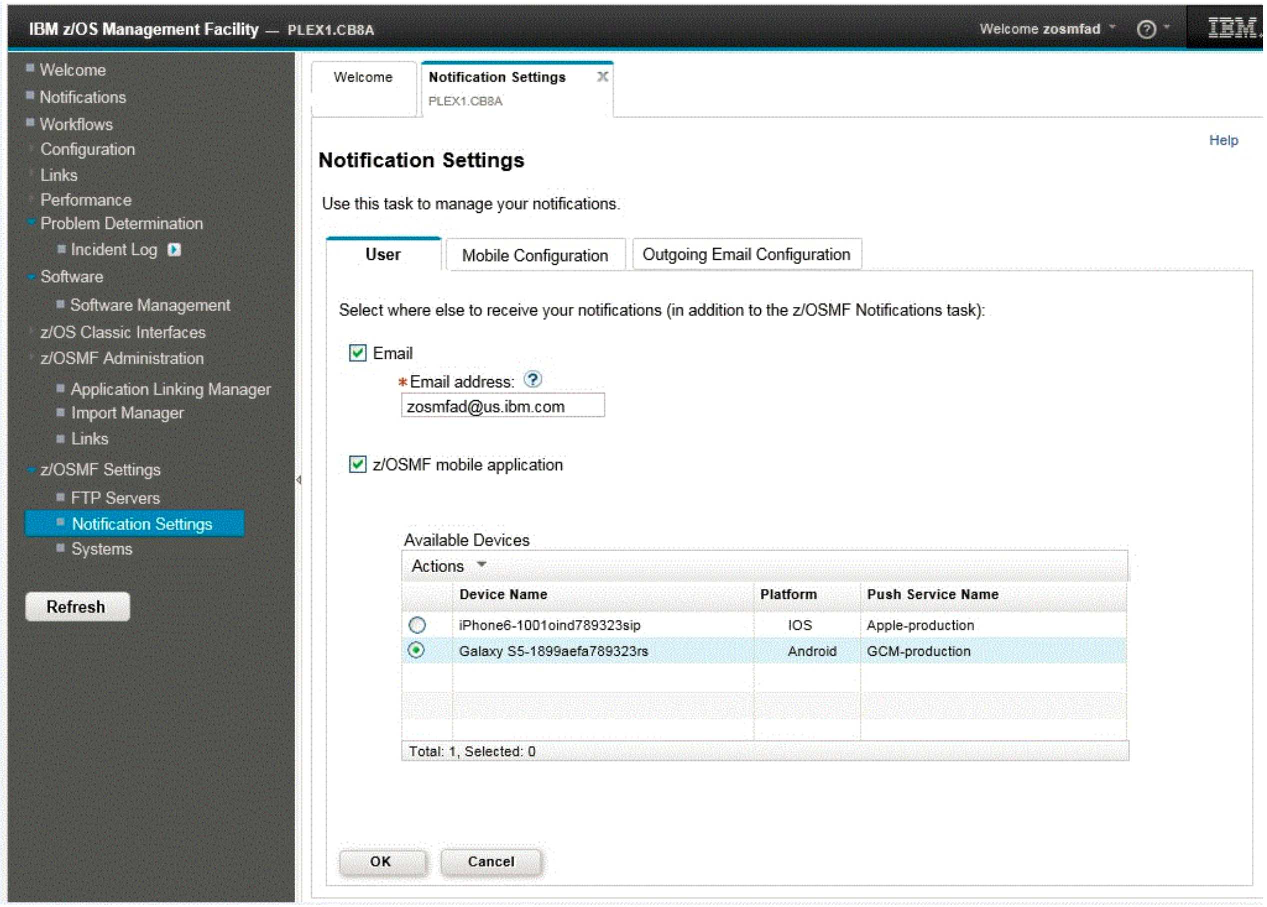
Through the z/OSMF notification framework, users can send different forms of notifications to multiple recipients. A notification can be sent to a user's email account or mobile phone. These notifications are received through the Notifications task. You can use the Notification Settings task to define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

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

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

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

Outgoing Email Configuration
Set the mail server properties.



Notification Settings

Use this task to manage your notifications.

Select where else to receive your notifications (in addition to the z/OSMF Notifications task):

☑ Email

*Email address: zosmfad@us.ibm.com

☑ z/OSMF mobile application

Available Devices

	Device Name	Platform	Push Service Name
○	iPhone6-1001oind789323sip	IOS	Apple-production
●	Galaxy S5-1899aefa789323rs	Android	GCM-production

Total: 1, Selected: 0

Figure 20. Notification Settings main page

You can use the Notification Settings task to:

- Add a mobile device in z/OSMF and link it with any z/OSMF user ID.

- Manage the mobile devices in groups.
- Define and manage push services and encryption keys in z/OSMF.
- Manage the mapping of product and eventGroup to mobile device or groups of mobile devices.

To display the Notification Settings task, expand the z/OSMF Settings category and select **Notification Settings** in the navigation area. The Notification Settings task main page is displayed, as shown in Figure 20 on page 87.

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

Resource Monitoring task overview

The Resource Monitoring task provides a web-based user interface that you can use to monitor the performance of the z/OS, AIX, Linux, and Windows systems in your enterprise. With the Resource Monitoring task, you can monitor most of the metrics supported by Resource Measurement Facility (RMF) Monitor III, create and save custom views of the metrics, and display real-time data as bar charts.

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

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

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

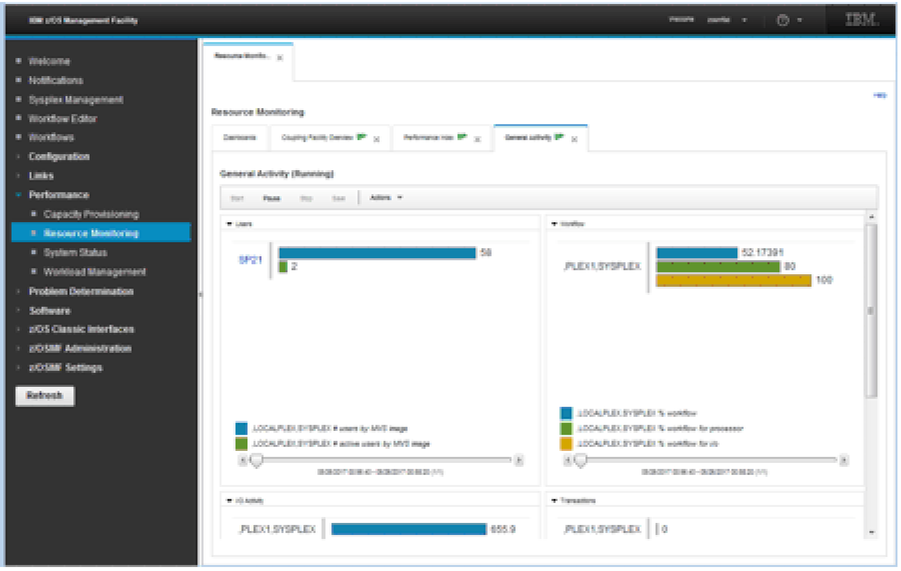


Figure 21. Resource Monitoring task sample view

When the Workload Management plug-in is enabled on your system, the Resource Monitoring task can link automatically to the Workload Management task for additional data. Thus, when the Resource Monitoring task shows performance data related to a WLM workload, service class, or report class, you can view the corresponding WLM service definition in your z/OSMF session.

To display the Resource Monitoring task, expand the Performance category in the navigation area and select **Resource Monitoring**. Figure 21 on page 88 shows a sample view from the Resource Monitoring task.

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

- **Create monitoring dashboards.** You can create monitoring dashboards or custom views that you can use to monitor the performance of the sysplexes, system complexes, or images in your environment.
- **Save monitoring dashboards.** You can save monitoring dashboards. Doing so allows you to reuse the monitoring dashboard or template so that you can easily view performance data for your monitored sysplexes, system complexes, or images from the same angle.
- **Work with multiple monitoring dashboards.** You can work with multiple monitoring dashboards simultaneously. To do so, open the dashboards with which you want to work in a new tab in the z/OSMF work area or in a new browser tab or window.
- **Monitor multiple resources simultaneously.** You can collect data for multiple resources at the same time. To do so, associate the metrics in a dashboard with different resources.
- **Create dashboards that are not associated with a specific sysplex.** Doing so streamlines the number of dashboards that you have to create because you can create one dashboard and use it for all of the sysplexes in your installation.
- **Monitor the performance over time.** The Resource Monitoring task provides controls that you can use to browse through the samples that have been collected for the metric groups contained in a monitoring dashboard. Up to 100,000 samples are collected for a dashboard. To browse the samples, use the slider and the backward and forward arrows provided in each metric group.
- **Retrieve historical data.** You can retrieve and view performance data that the RMF Distributed Data Server has collected in the past for the metric groups contained in a monitoring dashboard.
- **Export performance data to spreadsheet files.** You can export the data collected in monitoring dashboards into CSV format files on your local workstation. Doing so allows you to do further data evaluation using a spreadsheet application.

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

Resource Management task overview

The Resource Management task provides function for IBM Cloud Provisioning and Management for z/OS. Use it along with the Software Services task to provision z/OS software and to manage the provisioned software.

Figure 22 on page 89 shows the main page for the Resource Management task.

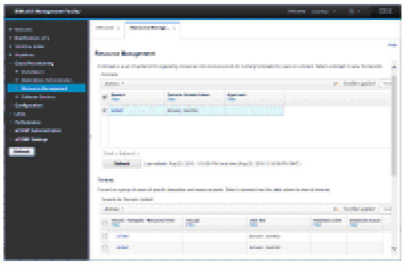


Figure 22. Resource Management task main page

To open the Resource Management task, in the navigation area, expand the Cloud Provisioning category and select **Resource Management**.

Key features

With the Resource Management task, you can:

Create and manage domains

A domain defines the management scope for tenants, services, and resource pools. It consists of a z/OS system or set of systems in a sysplex. To create a domain, you must be defined as a landlord. For each domain, the landlord can assign one or more domain administrators.

Create and manage tenants

A tenant consists of a user or group of users that have contracted for use of specified services and pooled z/OS resources that are associated with the services in a domain.

Add resource pools and software services templates to tenants

A resource pool defines the scope of shared z/OS resources within a domain that has multiple tenants. Adding resource pools to tenants may require the participation of other users, such as network or WLM administrators. You also add software services templates, which are defined with the Software Services task, to tenants.

Use a tenant with Container Pricing for IBM Z

You can define a tenant as a container for Container Pricing for IBM Z, by specifying a solution ID for the tenant. Any software that you provision for that tenant is treated as part of the solution. This approach simplifies the setup that is required for Container Pricing for IBM Z, because the Resource Management task does the z/OSMF Workload Management work for you, including creating the tenant resource group, tenant report class, and classifications.

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

Software Services task overview

The Software Services task provides function for IBM Cloud Provisioning and Management for z/OS. Use it along with the Resource Management task to provision z/OS software and to manage the provisioned software.

Figure 23 on page 90 shows the overview page for the Software Services task. It shows summary information about provisioned software (software instances) and the software templates that can be used to provision software.

Figure 23. Software Services task main page

To open the Software Services task, in the navigation area, expand the Cloud Provisioning category and select **Software Services**.

Key features

With the Software Services task, you can:

Add and customize software services templates

Templates consist of z/OSMF workflows and associated actions and variables that can be used to provision z/OS software. Typically, the original source of the workflow, actions, and variable definitions is the software vendor. You can modify the vendor-supplied files for your installation.

Make software services templates available to consumers

After you have prepared a software services template, you publish it to make it available to consumers. For example, you might make the published template available as an offering in a consumer marketplace such as the sample Marketplace task provided by IBM.

Use software services templates to provision software

A **Run** action provisions software from a software services template.

Manage software services instances

The provisioned software is shown in a table of software services instances. You can manage the instances with actions, which invoke commands or workflows. The actions typically include deprovision.

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

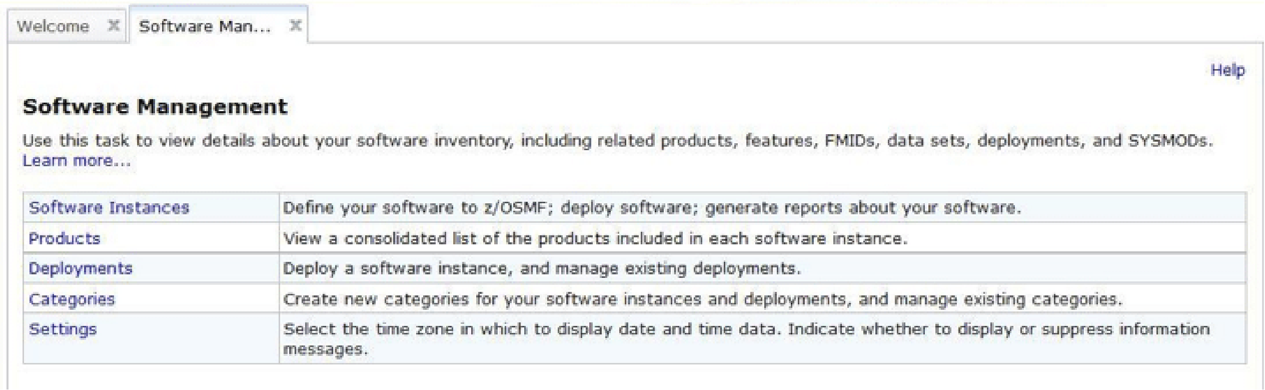
Software Management task overview

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

Getting started

To display the Software Management task, in the navigation area, expand the Software category and select Software Management. Figure 24 on page 91 depicts the main page in the Software Management task.

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



Software Management

Use this task to view details about your software inventory, including related products, features, FMIDs, data sets, deployments, and SYSMODs.
Learn more...

Software Instances	Define your software to z/OSMF; deploy software; generate reports about your software.
Products	View a consolidated list of the products included in each software instance.
Deployments	Deploy a software instance, and manage existing deployments.
Categories	Create new categories for your software instances and deployments, and manage existing categories.
Settings	Select the time zone in which to display date and time data. Indicate whether to display or suppress information messages.

Figure 24. Software Management page

Key features

With the Software Management task, you can:

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

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

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

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

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

  You might perform a deployment to prepare to upgrade one or more of the contained products in a software instance to a new product release level or a higher maintenance level. Or, to create a copy of a software instance so that it can run in a different environment, such as test, development, or production.
- **Organize your software instances and deployments.** The Software Management task provides a category feature that you can use to organize your software instances and deployments. You can, for example, categorize them by product, subsystem, geography, or business unit.

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

Sysplex Management task overview

Use the Sysplex Management task to view sysplex resources and visualize their relationships.

To open the Sysplex Management task, in the navigation area, expand the Sysplex category and select **Sysplex Management**. This displays a topology view, as shown in Figure 25 on page 92.

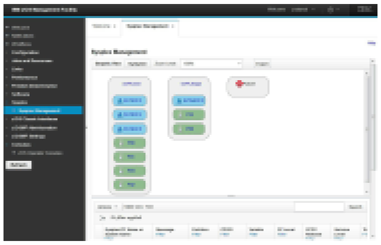


Figure 25. Sysplex Management task topology view

Key features

With the Sysplex Management task, you can use graphic or table views, which offer complimentary ways to work with your sysplex resources. In addition to the topology view, the Sysplex Management task offers many other views, including:

Physical view
This view shows CPCs, systems, coupling facilities, and couple data sets. A single point of failure condition is indicated by a yellow warning icon, which you can click to display details. From the physical view, you can view coupling facility structures.

Connectivity view
Use this view to manage physical connections between systems and coupling facilities.

Connectivity details
See details of connectivity between a coupling facility and a system. In addition to physical connections for the connectivity, it shows which channel path identifier (CHPID) and port are used for connectivity.

Coupling facility structures
You can view coupling facility structures by type and by coupling facility.

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

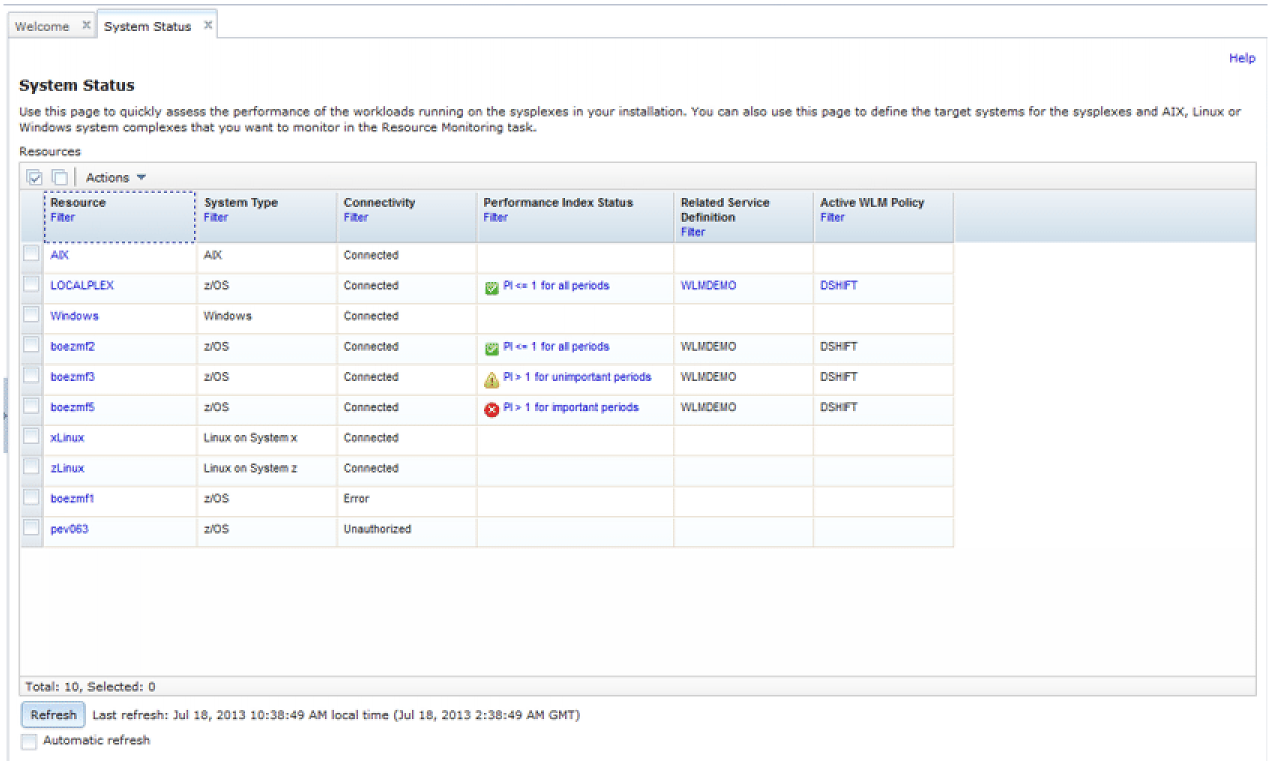
System Status task overview

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

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

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

To display the System Status task, expand the Performance category in the navigation area and select **System Status**. Figure 26 on page 94 shows a sample view from the System Status.



System Status

Use this page to quickly assess the performance of the workloads running on the sysplexes in your installation. You can also use this page to define the target systems for the sysplexes and AIX, Linux or Windows system complexes that you want to monitor in the Resource Monitoring task.

Resources

	Resource Filter	System Type Filter	Connectivity Filter	Performance Index Status Filter	Related Service Definition Filter	Active WLM Policy Filter
□	AIX	AIX	Connected			
□	LOCALPLEX	z/OS	Connected	✓ PI <= 1 for all periods	WLMDEMO	DSHIFT
□	Windows	Windows	Connected			
□	boezmf2	z/OS	Connected	✓ PI <= 1 for all periods	WLMDEMO	DSHIFT
□	boezmf3	z/OS	Connected	⚠ PI > 1 for unimportant periods	WLMDEMO	DSHIFT
□	boezmf5	z/OS	Connected	✗ PI > 1 for important periods	WLMDEMO	DSHIFT
□	xLinux	Linux on System x	Connected			
□	zLinux	Linux on System z	Connected			
□	boezmf1	z/OS	Error			
□	pev063	z/OS	Unauthorized			

Total: 10, Selected: 0

Last refresh: Jul 18, 2013 10:38:49 AM local time (Jul 18, 2013 2:38:49 AM GMT)

□ Automatic refresh

Figure 26. System Status sample view

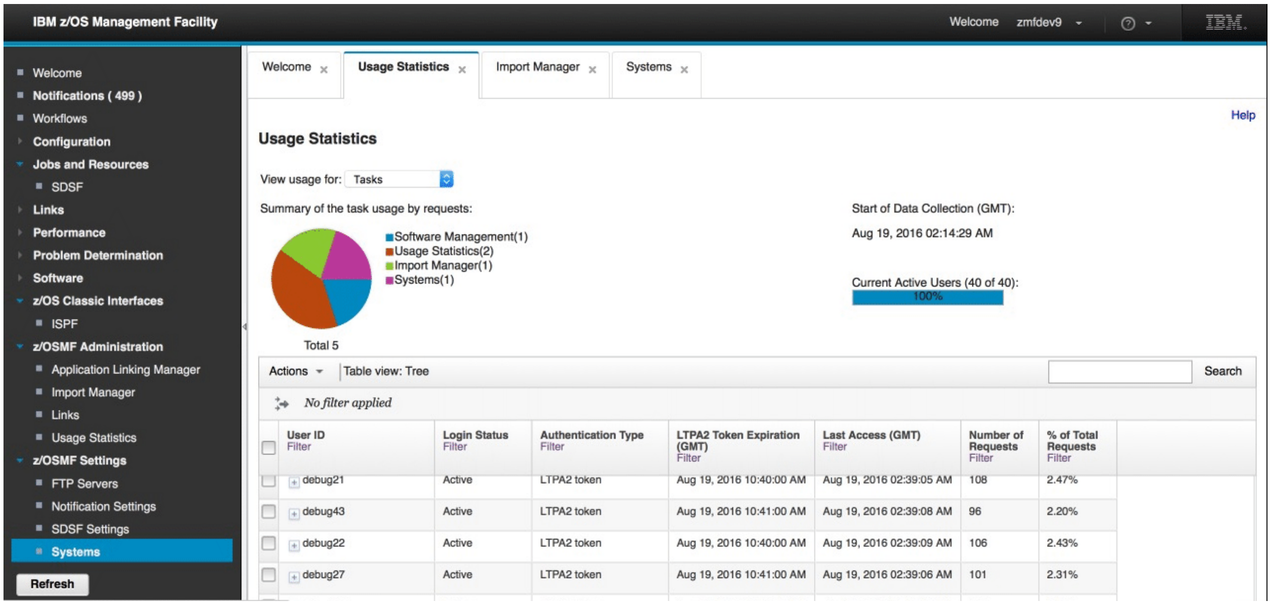
For information about using this task, see the online help.

Usage Statistics task in z/OSMF

The Usage Statistics task provides administrators with options for collecting usage statistics about z/OSMF.

A z/OSMF administrator can use the Usage Statistics task to:

- See which users are currently logged in to z/OSMF. You might use this information to send a notification to all of the logged on users, perhaps to inform them of an upcoming event on the system.
- Monitor the usage of each installed plug-in to see which plug-ins are used most often
- Select whether you would like to view usage for z/OSMF tasks or REST services.
- Display a chart that shows the statistical data for the tasks that are currently being used, based on whether you chose to view usage for z/OSMF tasks or REST services.
- Display the month, day, year, and time that the data usage collection started.



Usage Statistics

View usage for: Tasks

Summary of the task usage by requests:

Software Management(1)
Usage Statistics(2)
Import Manager(1)
Systems(1)

Total 5

Start of Data Collection (GMT):
Aug 19, 2016 02:14:29 AM

Current Active Users (40 of 40):
100%

Table view: Tree

No filter applied

User ID Filter	Login Status Filter	Authentication Type Filter	LTPA2 Token Expiration (GMT) Filter	Last Access (GMT) Filter	Number of Requests Filter	% of Total Requests Filter
debug21	Active	LTPA2 token	Aug 19, 2016 10:40:00 AM	Aug 19, 2016 02:39:05 AM	108	2.47%
debug43	Active	LTPA2 token	Aug 19, 2016 10:41:00 AM	Aug 19, 2016 02:39:08 AM	96	2.20%
debug22	Active	LTPA2 token	Aug 19, 2016 10:40:00 AM	Aug 19, 2016 02:39:09 AM	106	2.43%
debug27	Active	LTPA2 token	Aug 19, 2016 10:41:00 AM	Aug 19, 2016 02:39:06 AM	101	2.31%

Figure 27. Usage Statistics main page

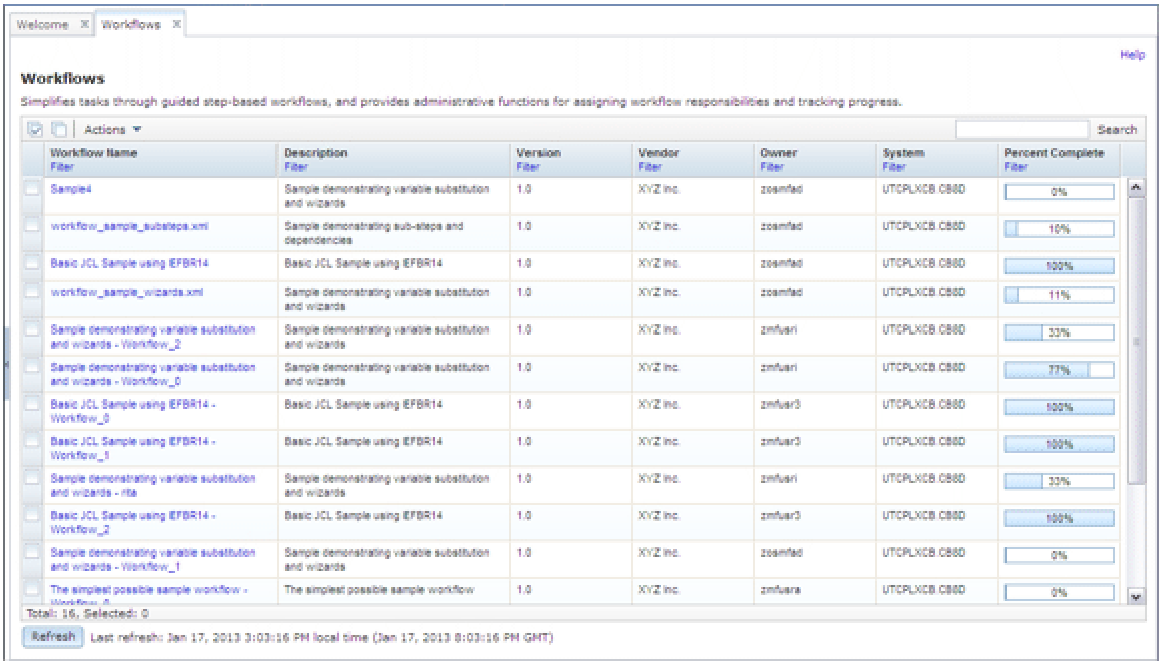
To display the Usage Statistics task, expand the z/OSMF Administration and select Usage Statistics. The Usage Statistics task main page is displayed, as shown in Figure 27 on page 95.

More information about the Usage Statistics task is available in the online help.

Workflows task overview

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

To display the Workflows task, select **Workflows** in the navigation area. The Workflows task main page is displayed, as shown in Figure 28 on page 96.



Workflows

Simplifies tasks through guided step-based workflows, and provides administrative functions for assigning workflow responsibilities and tracking progress.

Workflow Name	Description	Version	Vendor	Owner	System	Percent Complete
Sample4	Sample demonstrating variable substitution and wizards	1.0	XYZ Inc.	zosmfad	UTCPLXCB.CB8D	0%
workflow_sample_substeps.xml	Sample demonstrating sub-steps and dependencies	1.0	XYZ Inc.	zosmfad	UTCPLXCB.CB8D	10%
Basic JCL Sample using IEFBR14	Basic JCL Sample using IEFBR14	1.0	XYZ Inc.	zosmfad	UTCPLXCB.CB8D	100%
workflow_sample_wizards.xml	Sample demonstrating variable substitution and wizards	1.0	XYZ Inc.	zosmfad	UTCPLXCB.CB8D	11%
Sample demonstrating variable substitution and wizards - Workflow_2	Sample demonstrating variable substitution and wizards	1.0	XYZ Inc.	zmfusri	UTCPLXCB.CB8D	33%
Sample demonstrating variable substitution and wizards - Workflow_0	Sample demonstrating variable substitution and wizards	1.0	XYZ Inc.	zmfusri	UTCPLXCB.CB8D	77%
Basic JCL Sample using IEFBR14 - Workflow_0	Basic JCL Sample using IEFBR14	1.0	XYZ Inc.	zmfusr3	UTCPLXCB.CB8D	100%
Basic JCL Sample using IEFBR14 - Workflow_1	Basic JCL Sample using IEFBR14	1.0	XYZ Inc.	zmfusr3	UTCPLXCB.CB8D	100%
Sample demonstrating variable substitution and wizards - rita	Sample demonstrating variable substitution and wizards	1.0	XYZ Inc.	zmfusri	UTCPLXCB.CB8D	33%
Basic JCL Sample using IEFBR14 - Workflow_2	Basic JCL Sample using IEFBR14	1.0	XYZ Inc.	zmfusr3	UTCPLXCB.CB8D	100%
Sample demonstrating variable substitution and wizards - Workflow_1	Sample demonstrating variable substitution and wizards	1.0	XYZ Inc.	zosmfad	UTCPLXCB.CB8D	0%
The simplest possible sample workflow - Workflow_0	The simplest possible sample workflow	1.0	XYZ Inc.	zmfusra	UTCPLXCB.CB8D	0%

Total: 16, Selected: 0

Refresh Last refresh: Jan 17, 2013 3:03:16 PM local time (Jan 17, 2013 8:03:16 PM GMT)

Figure 28. Workflows task main page

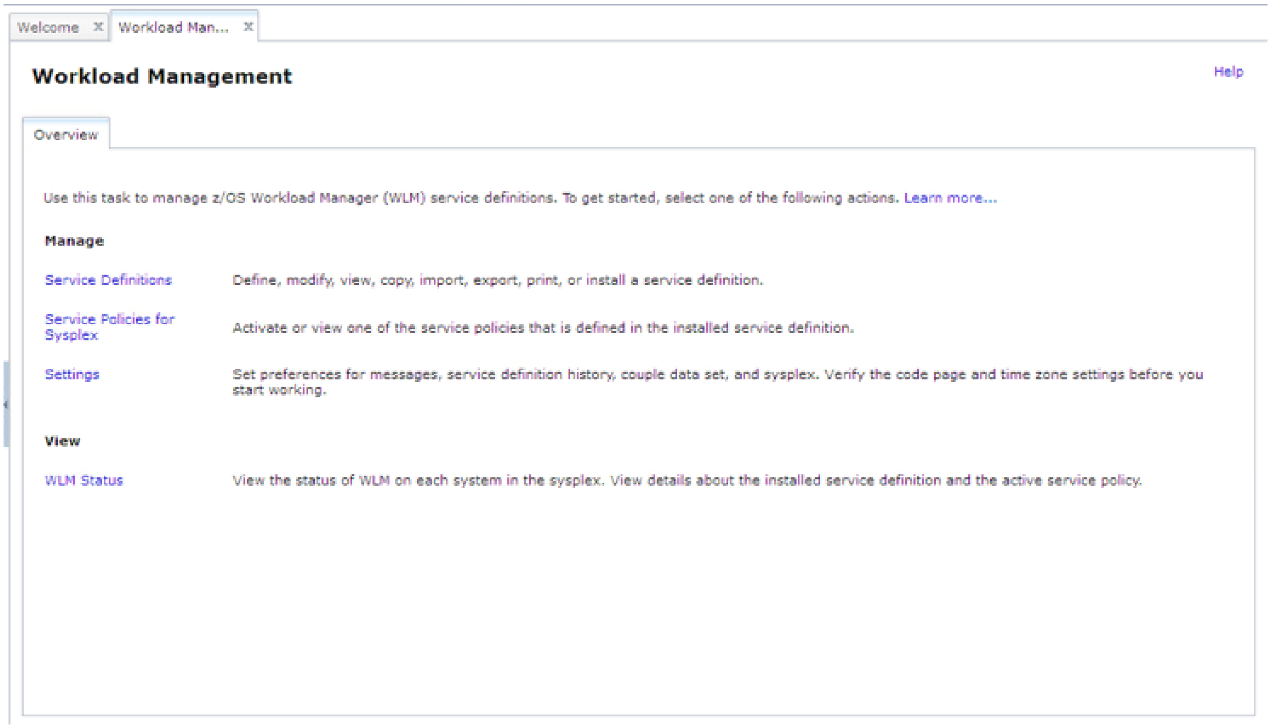
The Workflows task allows you to assign individual work items in the workflow (the "steps") to performers and track their progress. Based on the workflow, the Workflows task can offer wizards to assist your team with creating system objects (UNIX files and z/OS data set members) and submitting work to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

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

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

Workload Management task overview

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



Workload Management

Use this task to manage z/OS Workload Manager (WLM) service definitions. To get started, select one of the following actions. Learn more...

Manage

Service Definitions	Define, modify, view, copy, import, export, print, or install a service definition.
Service Policies for Sysplex	Activate or view one of the service policies that is defined in the installed service definition.
Settings	Set preferences for messages, service definition history, couple data set, and sysplex. Verify the code page and time zone settings before you start working.

View

WLM Status	View the status of WLM on each system in the sysplex. View details about the installed service definition and the active service policy.

Figure 29. Workload Management task main page

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

To display the Workload Management task, expand the Performance category in the navigation area and select **Workload Management**. Figure 29 on page 97 shows the main page for the Workload Management task.

The **Overview** tab serves as the launch point for the actions that your user ID is authorized to access within the Workload Management task. To start using the Workload Management task, select one of the actions listed in the **Overview** tab.

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

- Display list of service definitions. The Workload Management task provides a list of the WLM service definitions that are defined in z/OSMF along with history information (such as when the service definition was installed or modified), messages, and user activity. The list of service definitions is retrieved from the service definition repository, which refers to the directory in the z/OSMF user file system in which the data for the Workload Management task is stored.
- Work with multiple service definitions. In the Workload Management task, you can work with multiple service definitions simultaneously. To do so, open the service definitions with which you want to work in its own **View**, **Modify**, **Copy**, or **Print Preview** tab. You can also define multiple service definitions at the same time by opening several **New** tabs.
- Install service definitions. The Workload Management task provides features that you can use to install a service definition into the WLM couple data set for the z/OSMF host sysplex.
- Extract the installed service definition. The Workload Management task automatically extracts the service definition from the WLM couple data set for the z/OSMF host sysplex and stores it in the service definition repository so that you can view it, modify it, or activate one of its service policies.
- Import and export service definitions. The Workload Management task provides features that you can use to import a service definition from or export a service definition to your local workstation or a sequential data set on the z/OSMF host system. The exported service definition is formatted so that it can be opened with the z/OS WLM Administrative Application (also called the WLM ISPF application).

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

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

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

z/OS Operator Consoles task overview

The z/OS Operator Consoles task provides function to work with z/OS consoles. You can view system messages and enter system commands.

To use the z/OS Operator Consoles task, in the navigation area, expand the Consoles category and select z/OS Operator Consoles. The z/OS Operator Consoles task Overview page is displayed, showing a table of systems and the associated consoles. By selecting a console in the table, you can display a page for entering system commands and viewing system messages, as shown in Figure 30 on page 98.

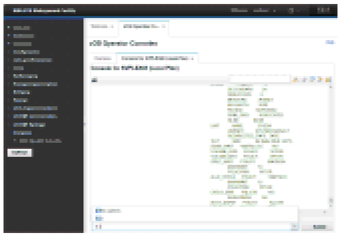


Figure 30. z/OS Operator Consoles page

Key features

With the z/OS Operator Consoles task, you can:

Select a console from a list of systems in the sysplex
The Overview tab shows the sysplexes and systems that are available for the z/OS Operator Consoles function, and the associated consoles.

See a system activity summary
The summary provides a graphic view of system message activity. The activity is represented as a bar graph. The colors in the bars reflect the colors of the messages that are displayed in the console.

Work with system messages
The console view shows system messages. You can search and filter the messages, and lock the console.

Enter system commands
At the command line, you can enter a system command. Type the command text in the command line, or select a command from the list of previously entered commands.

Search and Filter
You can search on keywords from received system messages and filter messages by particular fields, such as time, job name, system name, and message color.

Automatically retrieve and display message help
Message help can be displayed by hovering your cursor over the message ID. To use this function, you must ensure that the LookAt message lookup function in Knowledge Center for z/OS (KC4z) is configured. For more information, see *IBM Knowledge Center for z/OS Configuration and User Guide*.

Retrieve messages from OPERLOG or SYSLOG
For any messages that occur prior to starting the console, you can retrieve the messages from OPERLOG or SYSLOG. The messages are displayed in the same window with messages that are received by the console.

REST APIs are available for client programs
REST APIs are provided so that client programs can issue system commands and retrieve command responses. For more information, see IBM z/OS Management Facility Programming Guide.

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

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

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

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

IZUxxSEC jobs in SYS1.SAMPLIB

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

Each of the other IZU*xx*SEC jobs is associated with a z/OSMF plug-in, as follows:

IZUCASEC
Network Configuration Assistant

IZUCPSEC
Capacity Provisioning

IZUDMSEC
Software Deployment

IZUGCSEC
z/OS Operator Consoles

IZUILSEC
Incident Log

IZUISSEC
ISPF

IZUPRSEC
IBM Cloud Provisioning and Management for z/OS

IZURMSEC
Resource Monitoring

IZUSPSEC
Sysplex Management

IZUWMSEC
Workload Management

IZUNASEC
IBM z/OS Encryption Readiness Technology (zERT) Network Analyzer

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

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

Though the z/OS Operator Consoles task is a core function of z/OSMF, your security administrator must grant users access to it. IBM provides job **IZUGCSEC** in SYS1.SAMPLIB to assist you with performing these updates. The job contains RACF commands for creating the required security authorizations. For more information, see "Security setup for the z/OS Operator Consoles task" on page 150.

Managing user access to z/OSMF tasks and links

Your installation determines which z/OS users can perform the z/OSMF tasks, and creates authorizations for the users.

Figure 31 on page 102 shows a simplified view of SAF user authorizations in z/OSMF. To conserve space, this figure includes only a subset of the available tasks.

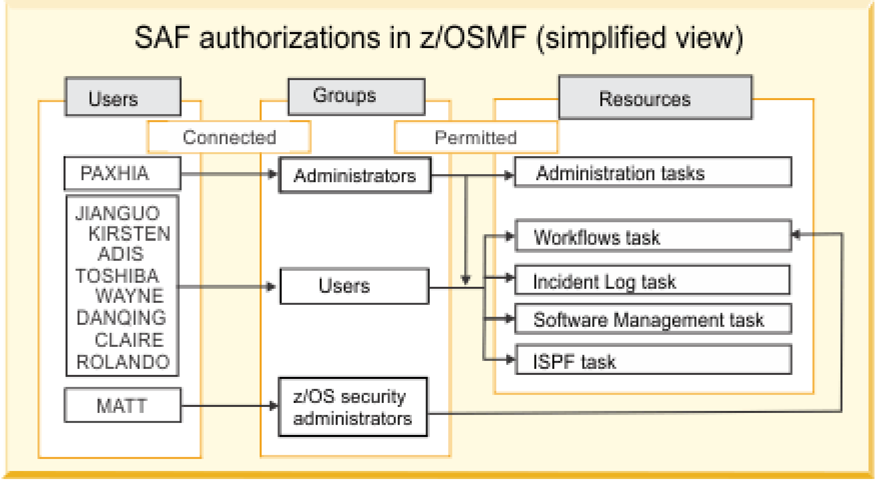


Figure 31. SAF authorizations in z/OSMF: A simplified view

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

The IZUxxSEC jobs contain sample RACF commands for:

- Creating ZMFAPLA resource class profiles for each of the z/OSMF tasks to be enabled on your system
- Creating groups and permitting those groups to the ZMFAPLA resource class profiles. By default, z/OSMF creates the groups IZUADMIN and IZUUSER, which correspond to the administrator and user roles. z/OSMF also creates the group IZUSECAD, which is used to allow a person such as your z/OS security administrator to perform the security-related steps in the Workflows task.

If your installation uses a security manager other than RACF, you must create equivalent commands for your environment. If so, you can refer to the IZUxxSEC jobs for the authorizations that are needed. For the security structures that are created by the IZUxxSEC jobs, see Appendix A, "Security configuration requirements for z/OSMF," on page 287.

Your security administrator can use the job SYS1.SAMPLIB(IZUAUTH) to authorize users to tasks and links. When used as provided, the IZUAUTH job connects the supplied user ID to the z/OSMF user group (IZUUSER). The job also contains commented commands for connecting the user to the z/OSMF administrator group and the z/OS Security Administrator group. Each group is permitted to a default set of z/OSMF resources (tasks and links). For the specific group permissions, see Appendix A, "Security configuration requirements for z/OSMF," on page 287.

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

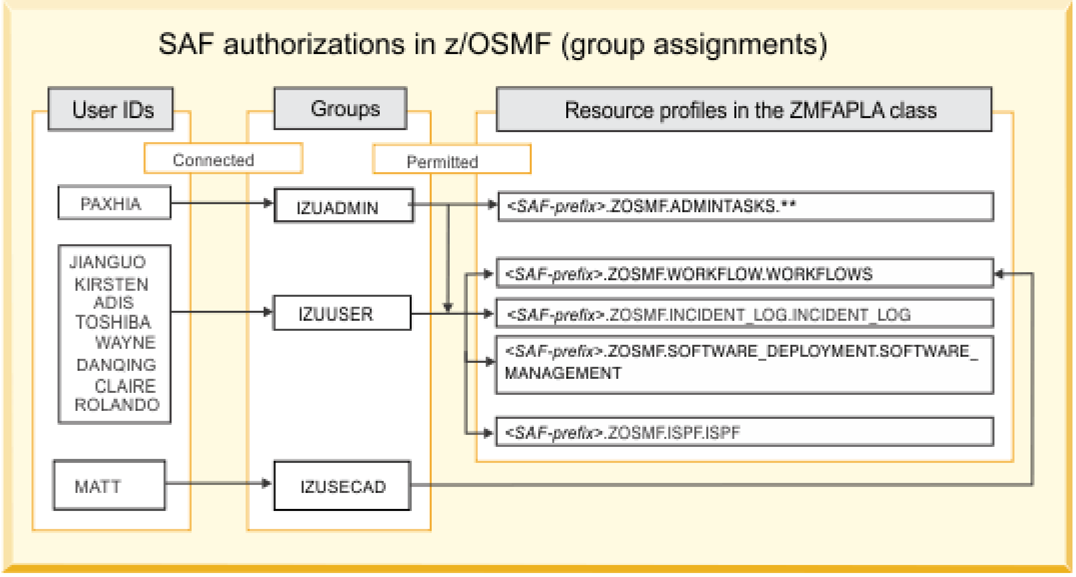

SAF authorizations in z/OSMF (group assignments)
User IDs
Groups
Resource profiles in the ZMFAPLA class
Connected
Permitted
PAXHIA
IZUADMIN
<SAF-prefix>.ZOSMF.ADMINTASKS.**
JIANGUO
KIRSTEN
ADIS
TOSHIBA
WAYNE
DANQING
CLAIRE
ROLANDO
IZUUSER
<SAF-prefix>.ZOSMF.WORKFLOW.WORKFLOWS
<SAF-prefix>.ZOSMF.INCIDENT_LOG.INCIDENT_LOG
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT
<SAF-prefix>.ZOSMF.ISPF.ISPF
MATT
IZUSECAD

Figure 32. SAF authorizations in z/OSMF: A typical setup

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

Figure 32 on page 103 shows the relationship between users, groups, and z/OSMF resource profiles in a typical z/OSMF security environment. To conserve space, this figure includes only a subset of the available tasks. In the figure, the group names and profiles are shown with the z/OSMF defaults. For the complete set of profiles that are created during the z/OSMF configuration process, and the groups that are permitted to the z/OSMF resources by default, see Appendix A, “Security configuration requirements for z/OSMF,” on page 287.

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

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

As shown in Figure 32 on page 103, the IZUDMSEC job provides a default authorization for the Software Management task through profile `<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT`. Your installation can create more granular authorizations for this task through more profiles, such as:

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.PRODUCT_INFO_FILE.RETRIEVE
```

For more information, see “Creating access controls for the Software Management task” on page 135.

Managing guest user access in z/OSMF

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

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

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

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

Chapter 7. Customizing your z/OS system for the z/OSMF plug-ins

This chapter describes the z/OS system customization steps that are required for enabling the optional plug-ins in z/OSMF. Which steps you will need to complete depend on which plug-ins you plan to deploy on your system.

Review the system setup requirements for each plug-in, as described in this topic. When doing the work, you might find it easier to start with plug-ins that require little or no system customization, such as Network Configuration Assistant or ISPF, and then progress to plug-ins with more extensive requirements, such as Incident Log.

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

- “Using FTP in your network” on page 105
- “Reviewing your CIM server setup” on page 105
- “Updating z/OS for the Capacity Provisioning plug-in” on page 107
- “Updating z/OS for the IBM zERT Network Analyzer Plug-in” on page 150
- “Updating z/OS for the Incident Log plug-in” on page 110
- “Updating z/OS for the ISPF plug-in” on page 127
- “Updating z/OS for the Network Configuration Assistant plug-in” on page 128
- “Updating z/OS for the Resource Monitoring Plug-in” on page 129
- “Updating z/OS for the Software Deployment plug-in” on page 135
- “Updating z/OS for the Sysplex Management plug-in” on page 143
- “Updating z/OS for the Workload Management plug-in” on page 146
- “Updating z/OS for the z/OS Operator Consoles task” on page 150

Note: After a plug-in is enabled, you might later decide to remove it. To do so, edit the IZUPRMxx parmlib member and remove the plug-in identifier from the PLUGINS statement. Then, restart the z/OSMF server. This action removes the plug-in tasks from the z/OSMF navigation area. Any residual data that is associated with the plug-in is saved in z/OSMF, in case you decide to enable it again later.

Using FTP in your network

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

For considerations, see the online help for the Task Settings task.

Reviewing your CIM server setup

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

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

- Capacity Provisioning
- Incident Log

- Workload Management.

Ensure that the administrator role is authorized to the CIM server

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

If your installation does not plan to run the CFZSEC job, your security administrator can perform these tasks manually, as follows:

1. Grant the z/OSMF administrator group UPDATE access to the CIMSERV profile in the WBEM class. This access can be granted through an explicit PERMIT command, or, if the CIM administrator group is already permitted with UPDATE access, you can connect the z/OSMF administrator user ID to the group. If necessary, refresh the WBEM class.
2. Ensure that the user ID under which the CIM server is running has SURROGAT access for the z/OSMF administrator group. If a generic BPX.SRV.** profile is already authorized in the SURROGAT class, no additional action is required. Otherwise, define a discrete profile for the z/OSMF administrator group and authorize it. If necessary, refresh the SURROGAT class.

These updates should be made before logging in to z/OSMF as the administrator, as described in “Step 6: Log into z/OSMF” on page 31.

Customizing the administrator role for running CIM commands

The CIM server commands are UNIX style programs that run in the z/OS UNIX shell. To ensure that the z/OSMF administrator can use the CIM commands, verify that the administrator role is properly set up for the z/OS UNIX shell environment, as described in this topic.

The file **profile.add**, which is shipped with the CIM server, provides the environment variables that you need to define for the administrator; see `/usr/lpp/wbem/install/profile.add`. If your installation used the job CFZRCUST from the installation SAMPLIB to customize the file systems and directories used by the CIM server, this setup is already done.

If your installation did not run the CFZRCUST job, you can perform this setup manually. Copy the contents of the **profile.add** file to the .profile file in the home directory of the z/OSMF administrator user ID. Modify the appropriate settings if you do not plan to use the defaults. The .profile file should be owned by the z/OSMF administrator; this person requires read-write-execute access to the file.

Or, you can use the following command to include the CIM profile settings for the duration of a shell session: `. /usr/lpp/wbem/install/profile.add`

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

Ensure that the CIM server is started

If your configuration includes a plug-in that uses the CIM server, ensure that the CIM server is active on your system when using z/OSMF. You can verify that the CIM server is started by entering a command like the following from the operator console:

```
D A,CFZCIM
```

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

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

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

Updating z/OS for the Capacity Provisioning plug-in

If you have selected to configure the Capacity Provisioning plug-in, you might have system customization to perform, as described in this topic. These actions are needed to ensure that users of the Capacity Provisioning task have access to the capacity provisioning domain.

This topic contains the following information:

- “System customization for the Capacity Provisioning task” on page 107
- “Enabling PassTicket creation for Capacity Provisioning task users” on page 108
- “Establishing secure communications with the CIM server” on page 109.

IBM provides job IZUCPSEC in SYS1.SAMPLIB to assist you with performing these updates. The job contains RACF commands for creating the required security authorizations.

System customization for the Capacity Provisioning task

Table 17 on page 107 describes the z/OS system changes that are required or recommended. Some of this work might already be done on your system, or might not be applicable. If so, you can skip the particular setup action.

Table 17. z/OS setup actions for the Capacity Provisioning task

	z/OS setup action	**Check when task is completed**
1	Ensure that a Capacity Provisioning Domain is implemented in your enterprise. For information about setting up and implementing Capacity Provisioning, see z/OS MVS Capacity Provisioning User's Guide.	
2	Ensure that potential users of the Capacity Provisioning task are defined to the Provisioning Manager query security group on the provisioning system (by default, the CPOQUERY group). On a system with RACF, you can query the users in a group through the LISTGRP command. For example: `LISTGRP CPOQUERY`	
3	Determine whether the CIM server on the provisioning system is currently configured to use PassTicket authentication. If so, proceed to Step 4. Otherwise, you must perform this set-up, following the steps described in z/OS MVS Capacity Provisioning User's Guide.	

Table 17. z/OS setup actions for the Capacity Provisioning task (continued)

	z/OS setup action	Check when task is completed

4	Determine whether the Provisioning Manager is running in the same security domain as the z/OSMF system. If so, grant the z/OSMF started task user ID at least UPDATE access authority to the profile IRRPTAUTH.CFZAPPL.* in the PTKTDATA class. On a system with RACF, you can create this authorization through the PERMIT command.
	For example:
	`PERMIT IRRPTAUTH.CFZAPPL.* CLASS(PTKTDATA)`
	`ID(passticket_creator_userid) ACCESS(UPDATE)`
	`SETROPTS RACLIST(PTKTDATA) REFRESH`
	where `passticket_creator_userid` is the z/OSMF started task user ID. By default, this is IZUSVR.
	Otherwise, if the Provisioning Manager is running in a different security domain, follow the steps in "Enabling PassTicket creation for Capacity Provisioning task users" on page 108.	

5	Ensure that communication between the Capacity Provisioning task and the CIM server is protected. Follow the steps in "Establishing secure communications with the CIM server" on page 109.	

Enabling PassTicket creation for Capacity Provisioning task users

Use the following procedure to ensure that Capacity Provisioning task users on the z/OSMF system can access the CIM server on the provisioning system.

About this task

In this procedure, you do the following:

- Ensure that PassTickets are enabled for every user who might require access to the provisioning system
- Verify that the z/OSMF started task user ID is authorized to generate PassTickets.

The procedure shows how this setup can be done for a system that uses RACF as its security manager. Included are the definitions for using the secured signon function and generating PassTickets. This setup must be done on both systems, as follows:

- System on which the PassTicket is to be verified (the provisioning system). This work is assumed to be done; otherwise, you must set up authentication on the provisioning system, as described in *z/OS MVS Capacity Provisioning User's Guide*.
- System on which the PassTicket is to be generated (the z/OSMF system), which is described here.

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

Procedure

1. On the z/OSMF system, activate the security class PTKTDATA, if it is not already active. If you plan to use generic profiles for the PTKTDATA class, include the GENERIC option on the **SETROPTS** command, for example:

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

2. Define the profile CFZAPPL in the PTKTDATA class and associate a secret secured signon key with the profile. The key must be the same on both the system on which the PassTicket is to be generated (the

z/OSMF system) and the system on which the PassTicket is to be verified (the provisioning system). For example:

```
RDEFINE PTKTDATA CFZAPPL SSIGNON(KEYMASKED(key))
APPLDATA('NO REPLAY PROTECTION')
SETROPTS RACLIST(PTKTDATA) REFRESH
```

where *key* is a user-supplied 16-digit value that is used to generate the PassTicket.

If a common cryptographic architecture (CCA) product is installed on the systems with the secured signon function, you can encrypt the secured signon key by using a KEYENCRYPTED value. If not, you can mask the secured signon key by using the SSIGNON option and a 64-bit KEYMASKED value, as shown in the preceding example.

If you plan to use a KEYENCRYPTED value, note that additional authorizations are required, including security profiles in the CSFSERV class and profiles for PassTicket creation and validation. Review the RACF setup requirements for the CCA product.

3. To enable PassTicket creation for Capacity Provisioning task users, define the profile IRRPTAUTH.CFZAPPL.* in the PTKTDATA class and set the universal access authority to NONE. For example:

   ```
   RDEFINE PTKTDATA IRRPTAUTH.CFZAPPL.* UACC(NONE)
   SETROPTS RACLIST(PTKTDATA) REFRESH
   ```

4. Grant the z/OSMF started task user ID permission to generate PassTickets for users. For example:

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

   where *passticket_creator_userid* is the z/OSMF started task user ID. By default, this user ID is IZUSVR.
5. Activate the changes, for example: `SETROPTS RACLIST(PTKTDATA) REFRESH`

Establishing secure communications with the CIM server

You must ensure that communication between the Capacity Provisioning task and the CIM server is protected. For secure network communications, it is recommended that you use Application Transparent Transport Layer Security (AT-TLS) and Transport Layer Security (TLS), as described in this topic.

Before you begin

Ensure that the basic setup for the Policy Agent and the certificate is done. For information, see *z/OS Common Information Model User's Guide* .

About this task

Use this procedure to establish secure communications between the Capacity Provisioning task and the CIM server.

This setup is not required for other z/OSMF tasks that use the CIM server, such as Incident Log or Workload Management.

Procedure

1. **Enable the HTTPS connection port.**

   For information, see the topic *Configuring the CIM server HTTPS connection using AT-TLS* in *z/OS Common Information Model User's Guide* with attention to the example called *SSL protection only*.
2. **Activate AT-TLS communication for the CIM server.**

   This means creating a policy in Policy Agent, creating client and server certificates, and then activating the policy. For information, see *z/OS Common Information Model User's Guide* .
3. **Refresh the Policy Agent to have your changes take effect.**

You can use the following command to refresh the Policy Agent:

```
F PAGENT,REFRESH
```

4. **Select the communications protocol and port number.**

   Do the following:

   a) In the z/OSMF navigation area, expand the Performance category and select Capacity Provisioning.

   b) Select the **Provisioning Manager** tab.

   c) In the Connections Table, select the following values for the **Host Address**:

   - For **Protocol**, select HTTPS
   - For **Port**, specify 5989.

   d) Click **OK** to confirm these settings.

Updating z/OS for the Incident Log plug-in

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

The Incident Log task requires that a number of z/OS components and facilities be enabled on your system. Much of this work might already be done on your system; for instructions, see the sections that follow.

System components used by the Incident Log task

As shown in Figure 33 on page 110, a number of base z/OS functions are involved when the Incident Log task is used to manage diagnostic data for your system.

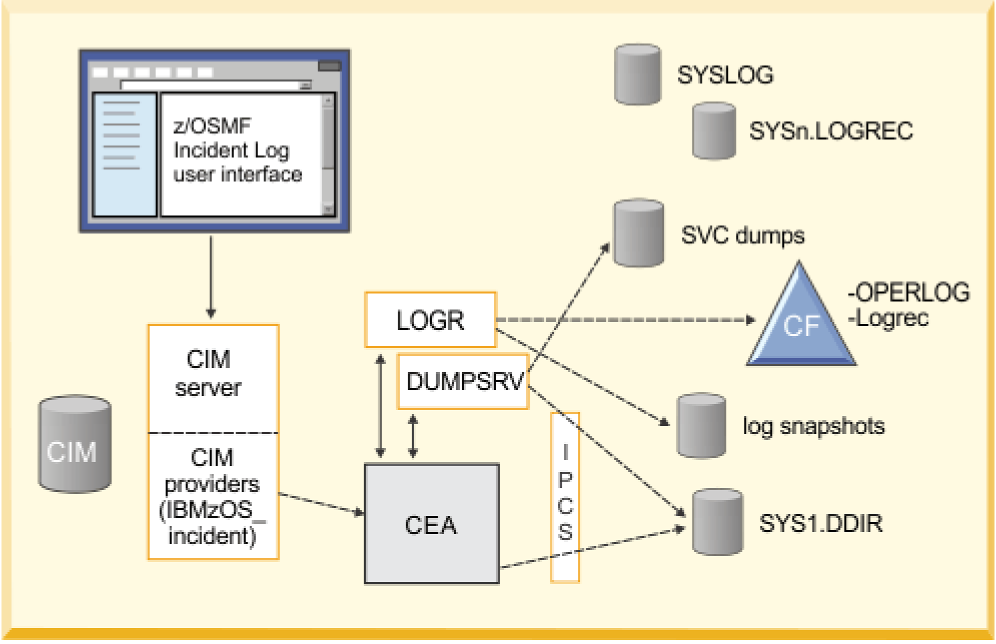


Figure 33. z/OS components that are used in Incident Log task processing

Specifically, z/OSMF and the Incident Log task interact with z/OS system functions in the following ways:

- Common Information Model (CIM) server for handling requests made by z/OSMF
- SDUMP component for managing the capture of OPERLOG, SYSLOG, and logrec snapshots
- IPCS dump directory services for managing the inventory of dumps related to incidents

- System Logger to capture log snapshots when sysplex-scope recording is requested through the OPERLOG or logrec system logger streams
- Dump analysis and elimination (DAE) for enabling the *Take Next Dump* function of the Incident Log task
- Environmental Record Editing and Printing (EREP) program for formating the logrec data
- Common Event Adapter (CEA) for providing the data that is subsequently displayed in the Incident Log task user interface.

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

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

- Is started automatically during z/OS system initialization
- Supports a set of operator commands for interaction, such as `MODIFY CEA`
- Issues WTO messages (prefixed with CEA)
- Supports an abend code for handling incorrect actions (`1D0`)
- Requires security profile setup (through the CEA resource profile)
- Supports a variety of reason codes to indicate errors in CEA processing. Reason codes that might appear during z/OSMF operations are listed in Appendix C, "Common event adapter (CEA) reason codes," on page 315.

The role of CEA in z/OSMF processing can be summarized, as follows:

- When CEA becomes active, it establishes an association with your installation's sysplex dump directory (typically SYS1.DDIR), which contains the inventory of SVC dumps taken in your sysplex, plus relevant information about each dump incident. This processing is done for SVC dumps taken on behalf of system abends, as well as those taken through the DUMP command and SLIP traps.
- Whenever an SVC dump is written to a data set, the DUMPSRV address space (on behalf of SVC dump processing) creates a new entry in the sysplex dump directory and informs CEA that the new incident has arrived. Then, CEA attempts to capture log snapshots, as follows:
  - If the system hardcopy log is recorded to the OPERLOG log stream, CEA directs the system logger component to create the log snapshot in a DASD log stream for the specified time duration. If the hardcopy is written to SYSLOG (that is, a single system scope), CEA uses spool allocation interfaces to access the SYSLOG data set and obtain the required snapshot, which is written to a DASD data set.
  - Similarly, if the logrec stream is written to a system logger log stream, CEA directs system logger to create a log snapshot of logrec data for the specified time period. If logrec is written to a data set, CEA invokes EREP to create the log snapshot.
  - Associates the snapshots with the corresponding incidents, based on snapshot data set name.
- When you use the Incident Log task to display incidents, CEA is invoked through the CIM server and uses IPCS functions to read the sysplex dump directory to obtain the inventory of SVC dumps taken on your system. CEA then extracts information from all relevant entries and returns it to z/OSMF for display. Similarly, when you use the Incident Log task to display details about an incident, z/OSMF receives those details from CEA, which obtains the information from the sysplex dump directory.
- When you request z/OSMF to send all or selected diagnostic materials to the specified URL, CEA is invoked to prepare the data, with different options, depending on whether you plan to use standard FTP or the z/OS Problem Documentation Upload Utility (PDUU). Here, all binary log data is formatted before being sent to the target system.
- In some instances, CEA performs its processing using System REXX execs, which are invoked through the AXREXX function.

As a result of this processing, your z/OS incidents are managed reliably on the system closest to the source of the information.

System customization needed for the Incident Log task

Table 18 on page 112 summarizes the z/OS system changes that are required or recommended for enabling the Incident Log task. Much of this work might already be done on your system, or might not be applicable. If so, you can skip the particular setup action. Other setup actions might require modifications to an existing setting, for example, if your installation has already defined a couple data set for the system logger component, you might need to increase the space allocation for system logger log stream records. For assistance with these setup actions, see the procedures referenced in the ***Where described*** column of Table 18 on page 112.

Table 18. z/OS setup actions for the Incident Log task

	z/OS setup action	Where described	Check when task is complete d
1	Ensure that the Common Information Model (CIM) server is configured on your system, including security authorizations and file system customization.	CIM includes jobs to help you perform these tasks (CFZSEC and CFZRCUST). See the chapter on CIM server quick setup and verification in Quick guide: CIM server setup and verification in *z/OS Common Information Model User's Guide*.	
2	Define a couple data set for the system logger component of z/OS.	See "Defining a couple data set for system logger" on page 113.	
3	Enable message log snapshots on the host system, or, optionally, on a sysplex-wide basis.	See the following topics: • "Setup considerations for log snapshots" on page 115 • "Enabling the operations log (OPERLOG)" on page 115 • "Defining and activating the LOGREC log stream" on page 117 • "Defining diagnostic snapshot log streams" on page 119 • "Enabling SYSLOG for diagnostic snapshots" on page 120.	
4	Enable error log snapshots on the host system, or, optionally, on a sysplex-wide basis.	See the following topics: • "Setup considerations for log snapshots" on page 115 • "Enabling the operations log (OPERLOG)" on page 115 • "Defining and activating the LOGREC log stream" on page 117 • "Defining diagnostic snapshot log streams" on page 119 • "Enabling SYSLOG for diagnostic snapshots" on page 120.	

Table 18. z/OS setup actions for the Incident Log task (continued)

	z/OS setup action	Where described	Check when task is complete d
5	Set up and configure automatic dump data set allocation (auto-dump).	See "Configuring automatic dump data set allocation" on page 120.	
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 121.	
7	Verify that a sysplex dump directory is defined for your system. If not, create a sysplex dump directory.	See "Creating the sysplex dump directory" on page 122.	
8	Ensure that the common event adapter (CEA) component is configured on your system, including security authorizations. Usually, the CEA address space is started automatically during z/OS initialization.	IBM provides the CEASEC job to help you create the security authorizations for CEA; see member CEASEC in SYS1.SAMPLIB. For information about running CEA, see "Ensure that common event adapter (CEA) is configured and active" on page 124.	
9	Ensure that System REXX (SYSREXX) is set up and active on your system.	See "Ensuring that System REXX is set up and active" on page 126.	
1 0	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 127.	

Defining a couple data set for system logger

The Incident Log task requires that a couple data set be defined for the system logger component of z/OS to represent the diagnostic log snapshots. If your installation has not already defined the system logger data set, this topic describes the steps for doing so.

How to check if this step is done

To display LOGR couple data sets on a system, enter the following command:

```
D XCF,COUPLE,TYPE=LOGR
```

Figure 34 on page 114 shows the expected results:

```
IXC358I  15.15.26  DISPLAY XCF 038
LOGR COUPLE DATA SETS
PRIMARY    DSN: UTCXCF.SVPLEX6.LOGRR13.PRI
           VOLSER: X6CPLP     DEVN: 3D09
           FORMAT TOD         MAXSYSTEM
           10/21/2012 12:05:59       32
           ADDITIONAL INFORMATION:
            LOGR COUPLE DATA SET FORMAT LEVEL: HBB7705
             LSR(2000) LSTRR(1000) DSEXTENT(10)
             SMDUPLEX(1)
ALTERNATE  DSN: UTCXCF.SVPLEX6.LOGRR13.ALT
           VOLSER: X6CPLA     DEVN: 3E08
           FORMAT TOD         MAXSYSTEM
           10/21/2012 12:17:05       32
           ADDITIONAL INFORMATION:
            LOGR COUPLE DATA SET FORMAT LEVEL: HBB7705
             LSR(2000) LSTRR(1000) DSEXTENT(10)
             SMDUPLEX(1)
LOGR IN USE BY ALL SYSTEMS
```

Figure 34. Expected results from the ***D XCF,COUPLE,TYPE=LOGR*** *command*

If this step is not already done

Define or update the system logger couple data set (LOGR CDS) with a large enough log stream records (LSR) value to allow sufficient space for managing the DASD-only log streams that will be created for capturing diagnostic log snapshots. The LSR value must be large enough to allow for two snapshot log streams for each dump recorded in z/OSMF, plus two model log streams, which are used as templates for defining the storage attributes for the snapshots. For information about modifying and reformatting a couple data set, see z/OS MVS Setting Up a Sysplex.

System logger supports shared sysplex-scope (coupling facility resident) log streams and single-system DASD-only log streams, as follows:

- Coupling facility (CF) log streams are sysplex-wide in scope; any system in the sysplex can write to these log streams.
- DASD-only log streams can be written to by the local system only. When a DASD-only log stream is closed, it can be read from other systems in the sysplex if it resides on DASD that is shared by the other systems in the sysplex.

The system creates DASD-only log streams for the operations log (OPERLOG) and the sysplex logrec diagnostic snapshots. You do not need to predefine the DASD-only log streams. For the model used, see sample job CEASNPLG, which is supplied by IBM in SYS1.SAMPLIB(CEASNPLG).

Use shared DASD as the target for OPERLOG and logrec snapshots, so that the Incident Log task can access the log snapshots from any system in the sysplex.

In planning the space requirements for your system logger couple data set, plan for two DASD-only log streams per incident. To allow up to 100 incidents, for example, you must allow enough space for 200 log streams.

IBM recommends that you allow space for up to 1000 DASD-only log streams (or 500 incidents). To do so, use the IXCL1DSU format utility, for example:

```
//FMTLGCDS JOB  MSGLEVEL=(1,1)
//         EXEC PGM=IXCL1DSU
//* S SUBMIT,JOB=LOGGER.ZOS17.JCL(FORMAT17)
//* SETXCF COUPLE,ACOUPLE=(LOGGER.OSR13.LARGE.INVNTRY,LOGR3),TYPE=LOGR
//* SETXCF COUPLE,PSWITCH,TYPE=LOGR
//SYSPRINT DD   SYSOUT=*
//SYSIN    DD   *
 DEFINEDS SYSPLEX(PLEX1) DSN(LOGGER.OSR13.LARGE.INVNTRY) VOLSER(LOGR3)
   DATA TYPE(LOGR)
     ITEM NAME(LSR)      NUMBER(2000)
     ITEM NAME(LSTRR)    NUMBER(25)
     ITEM NAME(DSEXTENT) NUMBER(15)
```

```
      ITEM NAME(SMDUPLEX) NUMBER(1)
//
```

If the system logger couple data set lacks sufficient space to contain the diagnostic snapshots, the system issues message CEA0600I to indicate that the log streams could not be created.

To allow the Incident Log task to access diagnostic log snapshots on other systems in the sysplex, the log streams must reside on shared DASD. DASD-only log streams are expected to be written to SMS-managed DASD.

Related information

For more information, see z/OS MVS Setting Up a Sysplex, which explains the following concepts:

- DASD-only log streams
- Setting up an SMS environment for DASD data sets
- Adding the data sets to the GRSRNL inclusion list
- Managing system logger log stream data sets
- Defining authorization.

Setup considerations for log snapshots

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

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

This section describes the system setup to be completed, based on the scope of data collection that you require.

- When message data is collected on a sysplex-wide basis, z/OSMF uses the operations log (OPERLOG) as the source for message data. This processing requires the following system setup:
  - Enabling OPERLOG on each system for which message data is to be collected. See “Enabling the operations log (OPERLOG)” on page 115.
  - Defining log streams for log snapshots to be obtained by the common event adapter (CEA) component of z/OS. See “Defining diagnostic snapshot log streams” on page 119.
  - Defining a couple data set for sysplex-wide logging through system logger. See “Defining a couple data set for system logger” on page 113.

  If you do not enable message data collection on a sysplex wide basis, z/OSMF collects message data for the z/OS host system only, using the system log (SYSLOG) as the source for creating diagnostic snapshots. See “Enabling SYSLOG for diagnostic snapshots” on page 120.
- When error log data is collected on a sysplex-wide basis, z/OSMF uses the logrec log stream as the source for error data. This processing requires that you set up system logger so that logrec data is written to a logger log stream. See “Defining and activating the LOGREC log stream” on page 117.

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

Enabling the operations log (OPERLOG)

The operations log (OPERLOG) is a sysplex-wide log of system messages (WTOs) residing in a system logger log stream, comparable to SYSLOG, which is a single system message log residing on JES spool.

If OPERLOG is enabled on your system, z/OSMF can use OPERLOG to collect message data on a sysplex wide basis. Here, OPERLOG must be active in a system logger log stream. For the steps to follow, see “Steps for setting up OPERLOG” on page 116.

If you choose to defer this step, z/OSMF collects message data on a single system basis, using the system log (SYSLOG) as the source.

How to check if this step is done

To display the active medium where messages are recorded, enter the following command:

```
D C,HC
```

Figure 35 on page 116 shows the expected results:

```
CNZ4100I 15.19.16 CONSOLE DISPLAY 056
 CONSOLES MATCHING COMMAND: D C,HC
 MSG:CURR=0    LIM=9000 RPLY:CURR=0    LIM=9999  SYS=P02      PFK=00
 HARDCOPY  LOG=(SYSLOG,OPERLOG)  CMDLEVEL=CMDS
       ROUT=(ALL)
 LOG BUFFERS IN USE: 0       LOG BUFFER LIMIT: 9999
```

Figure 35. Expected results from the **D C,HC** *command*

Steps for setting up OPERLOG

The following instructions are a summary of the details found in *IBM Redbook System Programmer's Guide to: z/OS System Logger*, which is available from http://www.redbooks.ibm.com/. For more information about setting up OPERLOG, see the topic on preparing to use system logger applications in z/OS MVS Setting Up a Sysplex.

Before you begin

You must define the logger subsystem.

Procedure

1. Define the OPERLOG coupling facility structure in the CFRM policy. For example:

   ```
   //OPERLOG JOB CLASS=A,MSGCLASS=A
   //POLICY EXEC PGM=IXCMIAPU
   //SYSPRINT DD SYSOUT=A
   //SYSIN DD *
   DATA TYPE(CFRM)
   STRUCTURE NAME(OPERLOG)
   SIZE(40448)
   INITSIZE(40448)
   PREFLIST(FACIL01,FACIL02)
   ```
2. Activate the CFRM policy through the **SETXCF START,POLICY,TYPE=CFRM,POLNAME=***polname* command, or through the COUPLExx parmlib member.
3. Define the log stream to the LOGR policy. The following example is for illustrative purposes only; follow the recommendations in z/OS MVS Setting Up a Sysplex and z/OS MVS Programming: Assembler Services Guide.

   ```
   //OPERLOG JOB CLASS=A,MSGCLASS=A
   //POLICY EXEC PGM=IXCMIAPU
   //SYSPRINT DD SYSOUT=A
   //SYSIN DD *
   DATA TYPE(LOGR)
   DEFINE STRUCTURE NAME(OPERLOG)
   LOGSNUM(1)
   MAXBUFSIZE(4092)
   ```

```
AVGBUFSIZE(512)
DEFINE LOGSTREAM NAME(SYSPLEX.OPERLOG)
STRUCTNAME(OPERLOG)
LS_DATACLAS(LOGR24K)
HLQ(IXGLOGR)
LS_SIZE(1024)
LOWOFFLOAD(0)
HIGHOFFLOAD(80)
STG_DUPLEX(NO)
RETPD(0)
AUTODELETE(No)
```

4. Create the security definitions for RACF (or an equivalent security manager). In the following example, the SYSPLEX.OPERLOG of the LOGSTRM resource CLASS is given READ permission, which allows all users to browse the operations log and *userid1* has UPDATE access level, which allows *userid1* to delete records from the log stream. That is, the user ID associated with the job running the IEAMDBLG program. For example:

   ```
   RDEFINE LOGSTRM SYSPLEX.OPERLOG UACC(READ)
   PERMIT SYSPLEX.OPERLOG CLASS(LOGSTRM) ID(userid1)
   ACCESS(UPDATE) SETROPTS CLASSACT(LOGSTRM)
   ```

   This example is for illustrative purposes only. Follow the guidelines for your installation.
5. Define the hardcopy device as OPERLOG in the HARDCOPY statement of the CONSOLxx parmlib member. You can change this setting using the **V OPERLOG,HARDCPY** command.
6. After you activate OPERLOG, you must manage the way in which records are handled.

   SYS1.SAMPLIB contains a sample program, IEAMDBLG, to read log blocks from the OPERLOG log stream and convert them to SYSLOG format. The program is an example of how to use the services of the system logger component to retrieve and delete records from the OPERLOG log stream. It reads the records created in a given time span, converts them from message data block (MDB) format to hardcopy log format (HCL or JES2 SYSLOG), and writes the SYSLOG-format records to a file. It also has an option to delete from the log stream the records created before a given date.

   When you use the delete option, you might want to first copy the records on alternate media and then conditionally delete the records in a separate JCL step to ensure that you have a copy of the data before deleting. If you do not run them on two separate conditional steps, deletion occurs simultaneously with copy without any guarantee that the copy process was successful.

   For more information, see the topic on managing log data in z/OS MVS Setting Up a Sysplex.

Results

To verify the completion of this work, enter the **DISPLAY CONSOLES,HARDCOPY** command to display the OPERLOG status.

What to do next

If you need to deactivate OPERLOG, you can use the **V OPERLOG,HARDCPY,OFF** command.

Defining and activating the LOGREC log stream

Logrec is the z/OS error log. It contains binary data describing error records that are written on behalf of system abends and other system recording requests. Logrec data is formatted through the batch utility EREP. The single-system version usually resides in a data set named SYS1.LOGREC or *&SYSNAME*.LOGREC. The sysplex version resides in a system logger log stream (the LOGREC log stream).

If the LOGREC log stream is active on your system, z/OSMF uses this log stream to collect logrec data on a sysplex wide basis. For information about defining and activating the LOGREC log stream, see "Steps for setting up the LOGREC log stream" on page 118.

If you choose to defer this step, z/OSMF collects logrec data on a single system basis, using the logrec data set as the source.

How to check if this step is done

To display the active medium for collecting logrec data, enter the following command:

```
D LOGREC
```

Figure 36 on page 118 shows the expected results:

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

Figure 36. Expected results from the D LOGREC operator command

If the medium is DATASET, the logrec data is recorded using a data set. If the medium is LOGSTREAM, the logrec data is recorded in a LOGR logstream.

Steps for setting up the LOGREC log stream

The following instructions are a summary of the details found in *IBM Redbook System Programmer's Guide to: z/OS System Logger*, which is available from http://www.redbooks.ibm.com/. For more information about defining the log stream, see the topic on preparing to use system logger applications in z/OS MVS Setting Up a Sysplex.

Before you begin

You must define the logger subsystem.

Procedure

1. IPL each system using its own logrec data set specified in the IEASYSxx parmlib member. Then, switch to using the log stream through the **SETLOGRC** command. This process allows your installation to fall back to using the data set if needed. To use the log stream immediately from the IPL, specify LOGREC=LOGSTREAM in IEASYSxx, as follows:

   ```
   IEASYSxx with logrec data set:
   LOGCLS=L,
   LOGLMT=010000,
   LOGREC=SYS1.&SYSNAME..LOGREC,   or  LOGREC=LOGSTREAM,
   MAXUSER=128,
   MLPA=00
   ```

2. Define the LOGREC log stream structure definition in the CFRM policy. For example:

   ```
   //LOGREC JOB CLASS=A,MSGCLASS=A
   //POLICY EXEC PGM=IXCMIAPU
   //SYSPRINT DD SYSOUT=A
   //SYSIN DD *
   DATA TYPE(CFRM)
   STRUCTURE NAME(LOGREC)
   SIZE(2048)
   INITSIZE(1024)
   PREFLIST(FACIL01,FACIL02)
   ```

3. Define the system logger policy. For example:

   ```
   //DEFINE EXEC PGM=IXCMIAPU
   //SYSPRINT DD SYSOUT=A
   //SYSIN DD *
   DATA TYPE (LOGR)
   DEFINE STRUCTURE NAME(LOGREC)
   LOGSNUM(1)
   AVGBUFSIZE(4068)
   MAXBUFSIZE(4068)
   ```

```
DEFINE LOGSTREAM NAME(SYSPLEX.LOGREC.ALLRECS)
STRUCTNAME(LOGREC)
LS_DATACLAS(LOGR4K)
HLQ(IXGLOGR)
LS_SIZE(1024)
LOWOFFLOAD(0)
HIGHOFFLOAD(80)
STG_DUPLEX(NO)
RETPD(0)
AUTODELETE(NO)
```

4. Change the logrec recording medium:

   ```
   SETLOGRC {LOGSTREAM|DATASET|IGNORE}
   ```

5. Create the required security definitions. For example:

   ```
   RDEFINE LOGSTRM SYSPLEX.LOGREC.ALLRECS UACC(READ)
   SETROPTS CLASSACT(LOGSTRM)
   ```

Results

To verify the completion of this work, enter the **DISPLAY LOGREC** command to display the current logrec error recording medium.

Defining diagnostic snapshot log streams

For optimal performance of the Incident Log task, it is recommended that your installation define operations log (OPERLOG) and logrec log streams for the CEA component of z/OS. Doing so allows the system logger component to determine the storage characteristics for storing diagnostic snapshots.

How to check if this step is done

To display the OPERLOG logstream, enter the following command:

```
D LOGGER,L,LSN=SYSPLEX.OPERLOG
```

Figure 37 on page 119 shows the expected results:

```
IXG601I   15.26.03  LOGGER DISPLAY 070
INVENTORY INFORMATION BY LOGSTREAM
LOGSTREAM                  STRUCTURE        #CONN  STATUS
---------                  ---------        ------ ------
SYSPLEX.OPERLOG            LOGGER_STR1      000004 IN USE
  SYSNAME: P00
    DUPLEXING: LOCAL BUFFERS
  SYSNAME: P01
    DUPLEXING: LOCAL BUFFERS
  SYSNAME: P02
    DUPLEXING: LOCAL BUFFERS
  SYSNAME: P03
    DUPLEXING: LOCAL BUFFERS
  GROUP: PRODUCTION

NUMBER OF LOGSTREAMS:  000001
```

Figure 37. Expected results from the ***D LOGGER*** *command*

If this step is not already done

To create the log streams, you can use a batch job like sample job CEASNPLG, which is supplied by IBM in SYS1.SAMPLIB(CEASNPLG). The CEASNPLG job deletes and redefines CEA diagnostic snapshot model log streams, using the IBM utility program, IXCMIAPU. For information about the IXCMIAPU utility, see z/OS MVS Setting Up a Sysplex.

Enabling SYSLOG for diagnostic snapshots

If your installation collects messages about programs and system functions (the hardcopy message set) on a single system basis, the Incident Log task uses the system log (SYSLOG) as the source for diagnostic log snapshots.

Here, you must ensure that the proper security permissions exist, so that the JES subsystem can access SYSLOG on behalf of the common event adapter (CEA) component of z/OS. For example, in a system with RACF as the security management product, your security administrator can enter RACF commands like those shown in Figure 38 on page 120, where *CEA_userid* is the user ID that you use to access CEA.

```
RDEFINE JESSPOOL SY1.+MASTER+.SYSLOG.*.* UACC(NONE)
PERMIT SY1.+MASTER+.SYSLOG.*.* CLASS(JESSPOOL) ID(CEA_userid) ACC(READ)
SETROPTS RACLIST(JESSPOOL)
```

Figure 38. RACF commands to enable CEA to access SYSLOG

Your installation might not have defined JESSPOOL under RACF authority; if so, your setting for the SETROPTS command will be different.

For more information about RACF commands, see z/OS Security Server RACF Command Language Reference.

Configuring automatic dump data set allocation

For full functionality, the Incident Log task requires that automatic dump data set allocation (auto-dump) be active on the z/OS host system. If your installation has not already set up auto-dump, this topic describes the steps for doing so. If you choose to defer this step, the Incident Log task runs with limited functionality. If your installation uses automatic dump data set allocation, the Incident Log task uses the resulting dump data set names in the "Send Data" action, which allows your installation to transmit this data to a remote destination through FTP.

To set up automatic dump data set allocation, do the following:

1. Define the dump data set naming convention to be used by the system. Specify it using the “DUMPDS NAME=” command, for example:

   ```
   $sysplex..DUMP.D&date..T&time..&SYSNAME..&S&seq
   ```

2. Determine where the dumps are to be stored. It is recommended that you use an SMS storage class or a shared DASD volume for dumps. Examples:

   DUMPDS ADD,SMS=*class*
   DUMPDS ADD,VOL=(*volser,volser,volser,..*)

   If you use a shared volume, ensure that the volume is managed through a shared catalog for the sysplex. Otherwise, for an incident with multi-system dumps, when deleting the incident, only the primary dump is deleted because the remote dumps are not accessible.

3. Start the function through the following command:

   ```
   DUMPDS ALLOC=ACTIVE
   ```

For more details, see the following information:

- Topic on the DUMPDS command in z/OS MVS System Commands
- Topic on SVC dump in z/OS MVS Diagnosis: Tools and Service Aids.

If your installation does not use automatic dump data set allocation, it is likely that you have defined pre-allocated dump data sets (SYS1.DUMPxx) for the system to use. Typically, an installation archives an SVC dump to another data set as soon as the dump is complete, to avoid having the system overlay the data set with a subsequent dump. The archive data set name is defined by the installation and is not known to the system. If so, the following limitations result:

- Incident Log records identify the pre-allocated dumps. Thus, the same property information is shown for each incident.
- Send Data action does not locate the dump data set because the name is unknown to the Incident Log task. The system, however, continues to process the log snapshots.

To continue using pre-allocated dump data sets, your installation can use an IBM-supplied JCL step to rename the dump data set in the sysplex dump directory, to allow z/OSMF to locate the correct data set. For information, see "Ensuring that dump data set names are correct" on page 127.

Some installations use automatic dump data set allocation, but then, subsequently, copy the dump data sets to another volume (to preserve space in the SMS DASD set). If the copied data set has the same name as the original dump data set, and the data set is cataloged, the Incident Log "Send data" action will locate the copied dump data sets. However, if the copied dump data set has a different name, use the IBM-supplied JCL step to rename the dump data set in the sysplex dump directory, so that the Incident Log task will locate it.

Configuring dump analysis and elimination

To avoid capturing duplicate problems in the Incident Log task display, ensure that dump analysis and elimination (DAE) is running on the z/OS host system. If your installation has not already configured DAE, this topic summarizes the steps for doing so.

IBM recommends that you enable DAE to suppress SVC dumps with duplicate symptoms for all of the systems in the sysplex (or all systems that you want the Incident Log task to represent). Doing so ensures that the Incident Log task displays only the initial instance of a dump-related incident. If necessary, you can use the *Allow next dump* action on the Incident Log page to allow the system to take and report the next dump that occurs for the same symptoms. You might use this option, for example, after you apply a fix for the problem. The *Allow next dump* action allows you to collect diagnostic data for the next new occurrence of the same problem.

To configure DAE processing for Incident Log processing, create a pair of ADYSETxx parmlib members with the appropriate options specified. Use one member to start DAE processing and the other member to stop DAE processing.

Consider using the following steps:

1. Create an ADYSETxx member for starting DAE. To do so, copy the IBM-supplied ADYSET00 member in SYS1.PARMLIB to a new member, for example, ADYSETAA. Do not modify the IBM-supplied member itself.
2. Create an ADYSETxx member for stopping DAE. To do so, copy the IBM-supplied ADYSET01 member in SYS1.PARMLIB to a new member, for example, ADYSETBB. Again, do not modify the IBM-supplied member itself.
3. Edit the new members, as follows:
   - In the DAE start-up member, specify the option SUPPRESSALL on the SVCDUMP parameter to suppress duplicate SVC dumps. Also, include the options SHARE, DSN and GLOBAL to use DAE in a sysplex-wide scope. For example:

     ```
     DAE=START,RECORDS(400),
     SVCDUMP(MATCH,SUPPRESSALL,UPDATE,NOTIFY(3,30)),
     SYSMDUMP(MATCH,UPDATE),
     SHARE(DSN,OPTIONS),DSN(SYS1.DAESH2) GLOBAL(DSN,OPTIONS)
     ```

     In this example, DSN specifies a cataloged data set SYS1.DAESH2 that resides on a DASD volume with shared access to all of the systems in the sysplex.
   - In the DAE shut-down member, include the option GLOBALSTOP on the DAE= parameter. For example:

     ```
     DAE=STOP,GLOBALSTOP
     ```

4. Ensure that the active IKJTSOxx parmlib member includes the program name ADYOPCMD in the AUTHCMD NAMES section. For information, see the topic on accessing the DAE data set in z/OS MVS Diagnosis: Tools and Service Aids.
5. To start DAE processing, enter the MVS command **SET DAE=xx** from the operator console, where *xx* is the suffix of the DAE start-up member. Enter the command for each system in the sysplex, for example, by using the **ROUTE** command to direct the **SET DAE=xx** command to the other systems:

   ```
   RO *ALL,SET DAE=xx
   ```

   To ensure that DAE processing is started automatically at IPL-time, include this command in the COMMNDxx parmlib member for the affected systems. If you choose to defer this step, you will need to manually start DAE on each system after each IPL.
6. Thereafter, for the IPLed systems in the sysplex, starting or stopping DAE on any one system will result in the other participating systems automatically starting or stopping DAE processing with the same options.

For more information about how to set up DAE, see z/OS MVS Diagnosis: Tools and Service Aids. For more information about the IBM-supplied ADYSETxx parmlib members, see z/OS MVS Initialization and Tuning Reference.

Creating the sysplex dump directory

The sysplex dump directory is a shared VSAM data set that contains information about SVC dumps that are 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 occur in the sysplex. If your installation does not already have a sysplex dump directory, this topic describes the steps for creating one.

How to check if this step is done

A sysplex dump directory might already exist for your system. This data set is defined through the SYSDDIR statement, which is typically specified in the parmlib member BLSCUSER. An example of the SYSDDIR statement follows:

```
SYSDDIR SYS1.DDIR ENV(ESAME)
```

IBM recommends that you define the SYSDDIR statement in member BLSCUSER. Alternatively, your installation might have specified this statement in member BLSCECT or BLSCECTX, or another member.

If you locate the SYSDDIR statement, verify that the specified sysplex dump directory data set exists, and is accessible to all of the systems in the sysplex (or all of the systems that you want the Incident Log task to represent).

Otherwise, you must create the sysplex dump directory, as described in the section that follows.

Steps for creating the sysplex dump directory

To create the sysplex dump directory, follow these steps:

1. Run the BLSCDDIR CLIST, which resides in system data set SYS1.SBLSCLI0(BLSCDDIR). For example:

   ```
   EXEC 'SYS1.SBLSCLI0(BLSCDDIR)'
   'DSNAME(SYS1.DDIR) VOLUME(volser) RECORDS(15000)'
   ```

   Where:

   - DSNAME specifies the data set name for the sysplex dump directory. As supplied by IBM, the CLIST specifies the name, SYS1.DDIR.
   - VOLUME specifies the DASD volume. To allow the Incident Log task (running on one system in the sysplex) to deliver a sysplex view of SVC dumps that are taken, select a volume with shared access to all of the systems in the sysplex (or all systems that you want the Incident Log task to represent).
   - RECORDS specifies the data set size in records. The Incident Log task requires a sysplex dump directory data set with at least 15,000 records, which is about 60 cylinders. Approximately 50 directory entries are used for each incident and more are used for multi-system dumps.

   The CLIST creates SYS1.DDIR as a VSAM data set with SHAREOPTIONS(1,3).

   This data set must be cataloged on the current system and any other backup systems that are running the CIM server to allow for access by the Incident Log task.
2. Specify the dump directory name on the SYSDDIR statement in member BLSCUSER. Alternatively, your installation might use another member, such as BLSCECT or BLSCECTX.
3. Recycle the DUMPSRV address space through the command **CANCEL DUMPSRV**. The DUMPSRV address space restarts automatically. This action registers the dump directory name with the DUMPSRV address space.
4. Start BLSJPRMI through the command **START BLSJPRMI**. This action registers the dump directory name to IPCS.

For more information about the BLSCDDIR CLIST, see z/OS MVS IPCS User's Guide.

Considerations for using a sysplex dump directory

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 it writes an entry to the directory for a new SVC dump
  - CEA address space, when it reads or updates 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 that is related to the IPCS session. The sysplex dump directory is used only to save name and symptom data for all SVC dumps taken, and must not be used as an IPCS user local dump directory.
- **Do not access the sysplex dump directory from an IPCS user.** Instead, use a batch job to access the directory.
- If new entries are not being added to the Incident Log task, or if requests are not being satisfied, check for contention on the sysplex dump directory by using the command **D GRS,C**. Verify that no IPCS user is accessing the sysplex dump directory.

Establishing a larger sysplex dump directory

Over time, your sysplex dump directory might become full with the dumps that you save. To create more space for dumps, you can delete old dumps from the directory. However, if you must retain the saved dumps, 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 sysplex dump directory data set through the BLSCDDIR CLIST, for example:

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

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

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

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

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

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

Ensure that common event adapter (CEA) is configured and active

Some z/OSMF tasks require the common event adapter (CEA) component be active on your z/OS system in **full function mode**. CEA provides the ability to deliver z/OS events to clients, such as the CIM server, and create or manage TSO user address spaces under the ISPF task. Usually, the CEA address space is started automatically during z/OS initialization. If your installation has stopped CEA, it is recommended that you restart it. Otherwise, the Incident Log task and the ISPF task are not operational.

Ensure that the common event adapter (CEA) component is configured on your system, including security authorizations. IBM provides the CEASEC job to help you create the security authorizations for CEA; see member CEASEC in SYS1.SAMPLIB.

The common event adapter (CEA) component of z/OS has security profiles for protecting different portions of its processing. For example, users of the Incident Log task require access to the CEA.CEAPDWB* profile in the SERVAUTH class. For the profiles related to CEA, see "Resource authorizations for common event adapter (CEA)" on page 301.

z/OSMF requires that CEA runs in full function mode on your system. In this mode, both internal z/OS components and clients such as CIM providers can use CEA indication functions. For information about how to configure CEA, see z/OS Planning for Installation.

Also, if your installation plans to use the ISPF task, you must ensure that the TRUSTED attribute is assigned to the CEA started task, as described in "Updating z/OS for the ISPF plug-in" on page 127.

How to check if CEA is active

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

```
D A,CEA
```

Figure 39 on page 124 shows the expected results:

```
IEE115I 15.32.17 2010.132 ACTIVITY 109
  JOBS     M/S    TS USERS    SYSAS    INITS   ACTIVE/MAX VTAM     OAS
 00018    00040    00002      00043    00246    00002/03500       00043
  CEA      CEA      IEFPROC  NSWPR*O  A=001A   PER=YES  SMC=000
                                      PGN=N/A  DMN=N/A  AFF=NONE
                                      CT=000.425S  ET=45.32.29
                                      WKL=SYSTEM   SCL=SYSTEM   P=1
                                      RGP=N/A      SRVR=NO  QSC=NO
                                      ADDR SPACE ASTE=05A34680
                                      DSPNAME=CEACTDSP ASTE=1002D600
                                      DSPNAME=CEAPDWB  ASTE=1002D580
                                      DSPNAME=CEACADS  ASTE=7EF42700
                                      DSPNAME=CEACOMP  ASTE=1002D480
```

Figure 39. Expected results from the ***D A,CEA*** *command*

Starting the CEA address space

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

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

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

You can specify multiple CEAPRMxx members, for example:

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

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

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

Identifying the CEAPRMxx member to use at IPL time

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

Modifying the common event adapter (CEA) settings

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

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

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

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

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

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

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

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

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

Ensuring that System REXX is set up and active

For full functionality, the Incident Log task requires that the System REXX (SYSREXX) component be set-up and active on your z/OS system.

This topic contains the following information:

- "Ensuring that System REXX is set-up properly" on page 126
- "Ensuring that System REXX is active" on page 126
- "Starting the SYSREXX address space" on page 127

Ensuring that System REXX is set-up properly

Observe the following considerations regarding System REXX set-up:

- Ensure that you have an AXRnn JCL member in PROCLIB, similar to the AXRnn member in SYS1.IBM.PROCLIB.
- If you have an AXRnn member in SYS1.IBM.PROCLIB, ensure that SYS1.IBM.PROCLIB is in the MSTJCLxx IEFPDSI DD concatenation.
- Ensure that the user ID specified for AXRUSER in AXRnn has the correct permissions.

For more information about setting up System REXX, see the following documents:

- *z/OS MVS Programming: Authorized Assembler Services Guide*.
- *z/OS MVS Initialization and Tuning Reference*.

Ensuring that System REXX is active

SYSREXX is started automatically during IPL. If your installation has stopped SYSREXX, it is recommended that you restart it.

If you choose to defer this step, the Incident Log task runs with limited functionality.

How to check if this step is done

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

```
D A,AXR
```

Figure 40 on page 126 shows the expected result:

```
IEE115I 15.34.46 2010.132 ACTIVITY 111
  JOBS     M/S    TS USERS    SYSAS    INITS   ACTIVE/MAX VTAM     OAS
 00018    00040    00002      00043    00246    00002/03500       00043
  AXR      AXR      IEFPROC  NSWPR*   A=0019   PER=YES  SMC=000
                                      PGN=N/A  DMN=N/A  AFF=NONE
                                      CT=000.088S  ET=45.34.45
                                      WKL=STC_WLD  SCL=STCLOW   P=1
                                      RGP=N/A      SRVR=NO  QSC=NO
                                      ADDR SPACE ASTE=05A34640
                                      DSPNAME=AXRTRDSP ASTE=1002D880
                                      DSPNAME=AXRRXENV ASTE=06BED200
                                      DSPNAME=AXRREQCP ASTE=06029180
```

Figure 40. Expected result from the ***D A,AXR*** *command*

Starting the SYSREXX address space

To start the SYSREXX component, enter the following command from the operator console:

```
START AXRPSTRT
```

For information about configuring System REXX on your system, see *z/OS 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 41 on page 127 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 41. Sample JCL to rename SVC dumps in the sysplex dump directory

In the example:

- Modify the keyword DSN=SYS1.DDIR to specify the name of your sysplex dump directory (the default name is SYS1.DDIR)
- Modify the values *OldDump* and *NewDump* to use the correct dump data set names.

Updating z/OS for the ISPF plug-in

If you have selected to configure the ISPF plug-in, you must ensure that each user of the ISPF task is an existing TSO/E user with a valid password.

Specifically, for each user of the ISPF task, ensure that the corresponding user ID:

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

By default, the ISPF task uses the logon procedure IKJACCNT, which is supplied by IBM in your ServerPac order, and an asterisk ('*') for the account number. A user can select to use a different logon procedure or account number, as long as the user's logon procedure is properly configured for ISPF and the account number is valid.

Assigning the TRUSTED attribute to CEA

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

For more information about the RACF TRUSTED attribute, see the topic on associating started procedures and jobs with user IDs in *z/OS Security Server RACF System Programmer's Guide*, and the topic on using started procedures in *z/OS Security Server RACF Security Administrator's Guide*.

Customizing for reconnecting user sessions

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

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

Customizing for profile sharing

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

- Log on simultaneously through a z/OSMF ISPF session and a telnet 3270 session, or
- Log on through multiple z/OSMF ISPF sessions (this is different than having split screens, which is also allowed).

If you plan to allow the use of multiple ISPF sessions, the user's logon procedure must be configured to allow profile sharing. This option avoids enqueue lock outs and loss of profile updates when the same profile data set is used for concurrent ISPF sessions. With profile sharing enabled, the user's logon procedure is required to allocate ISPF profile data sets with the disposition SHARED, rather than NEW, OLD, or MOD, and the data sets must already exist. Or, these data sets must be temporary data sets. For more information about ISPF customization, see *z/OS ISPF Planning and Customizing*.

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

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

Updating z/OS for the Network Configuration Assistant plug-in

If your installation uses the Windows desktop version of Network Configuration Assistant, you can optionally transfer your existing configuration data into the z/OSMF environment.

About this task

If you have a backing store that was exported from another version or instance of the Network Configuration Assistant, select **Transfer Backing Store File to z/OSMF** and provide the fully qualified path and file name for the exported backing store, and the z/OSMF backing store name to transfer the file.

Updating z/OS for the Resource Monitoring Plug-in

If you selected to configure the Resource Monitoring plug-in, you might have system customization to perform, as described in this topic.

This topic contains the following information:

- "System customization for the Resource Monitoring and System Status tasks" on page 129
- "Enabling PassTicket creation for Resource Monitoring task users" on page 130
- "Establishing secure communications with the Distributed Data Server" on page 131
- "Browser consideration for the Resource Monitoring task" on page 134.

System customization for the Resource Monitoring and System Status tasks

Table 19 on page 129 describes the z/OS system changes that are required or recommended. Some of this work might already be done on your system, or might not be applicable. If so, you can skip the particular setup action.

Table 19. z/OS setup actions for the Resource Monitoring and System Status tasks

	z/OS setup action	Check when task is completed
1	Enable the optional priced feature, Resource Measurement Facility (RMF), on one of the systems in your enterprise. For information about enabling features, see z/OS Planning for Installation, GA22-7504.	
2	For data collection and monitoring of your systems, ensure that the RMF Distributed Data Server (DDS) is active on one of the systems in your sysplex. To monitor several sysplexes, ensure that a DDS is running on one system in each sysplex. You can use the following command to check for the existence of GPMSERVE address spaces in your sysplex: `ROUTE *ALL,D A,GPMSERVE` If your installation uses RMF Cross Platform Monitoring (RMF XP), the RACF profile name for the RMF XP DDS is GPM4CIM, rather than GPMSERVE. For information about setting up the DDS and RMF XP, see z/OS RMF User's Guide, SC33-7990.	

Table 19. z/OS setup actions for the Resource Monitoring and System Status tasks (continued)

	z/OS setup action	Check when task is completed
3	Determine whether the DDS on the target system is currently configured to require authentication. To check, use the following command to display the active DDS options: `MODIFY GPMSERVE,OPTIONS` If your installation uses RMF XP, the RACF profile name for the RMF XP DDS is GPM4CIM, rather than GPMSERVE. In the command output, check for the HTTP_NOAUTH setting, which indicates the scope of authentication for the DDS, as follows: **HTTP_NOAUTH()** All hosts must authenticate **HTTP_NOAUTH(*)** No authentication is required **HTTP_NOAUTH(*specific_host_or_mask*)** All hosts except those matching the mask must authenticate. If DDS authentication is not required in your enterprise, you are done. Otherwise, proceed to Step 4.	
4	Determine whether your installation security procedures require that the DDS should require authentication from the z/OSMF system and its users, and perform one of the following actions: • If DDS authentication is required from the z/OSMF system, you must ensure that the PassTicket is set up properly, and that the z/OSMF started task user ID is authorized to generate the PassTicket. See "Enabling PassTicket creation for Resource Monitoring task users" on page 130. • If DDS authentication is not required from the z/OSMF system, you can disable DDS authentication for the system on which z/OSMF is running. Doing so allows the Resource Monitoring and System Status tasks to access the DDS on behalf of z/OSMF users without potentially encountering authentication errors. To disable DDS authentication for the system on which z/OSMF is running (the server host name or IP address), modify the HTTP_NOAUTH statement in the GPMSRVxx parmlib member on the DDS system. In the following example, the HTTP_NOAUTH statement is updated to bypass DDS authentication for the host system represented by *`host_system_IP_address`*: `HTTP_NOAUTH(host_system_IP_address)` For more information about DDS authentication, see z/OS RMF User's Guide, SC33-7990.	

Enabling PassTicket creation for Resource Monitoring task users

If the RMF Distributed Data Server (DDS) requires authentication from the z/OSMF system and its users, follow the steps in this procedure to set up the PassTicket support.

About this task

In this procedure, you ensure that the PassTicket is set up properly, and that the z/OSMF started task user ID is authorized to generate the PassTicket. The procedure shows how this setup can be done for a system that uses RACF as its security management product.

Note: If your installation uses RMF Cross Platform Monitoring (RMF XP), the RACF profile name for the RMF XP DDS is GPM4CIM. Use this profile name instead of GPMSERVE when you complete Steps 2 through 4 in the procedure.

Procedure

1. On the z/OSMF system, activate the security class PTKTDATA, if this class is not already active. If you plan to use generic profiles for the PTKTDATA class, include the GENERIC option on the **SETROPTS** command, for example:

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

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

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

   where *key* is a user-supplied 16-digit value used to generate the PassTicket.

   If a common cryptographic architecture (CCA) product is installed on the systems with the secured signon function, you can encrypt the secured signon key using a KEYENCRYPTED value. If not, you can mask the secured signon key by using the SSIGNON option and a 64-bit KEYMASKED value, as shown in the preceding example.

   If you plan to use a KEYENCRYPTED value, note that additional authorizations are required, such as access to security profiles in the CSFSERV class, and additional profiles for PassTicket creation and PassTicket validation. Be sure to review the RACF setup requirements for the CCA product.

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

   - Example (for all user IDs):

     ```
     RDEFINE PTKTDATA IRRPTAUTH.GPMSERVE.* UACC(NONE)
     ```

   - Example (for a specific user ID):

     ```
     RDEFINE PTKTDATA IRRPTAUTH.GPMSERVE.specific_dds_login_userid UACC(NONE)
     ```

4. Grant the z/OSMF started task user ID permission to generate PassTickets for users.

   - Example (for all user IDs):

     ```
     PERMIT IRRPTAUTH.GPMSERVE.* CLASS(PTKTDATA) ID(passticket_creator_userid)
     ACCESS(UPDATE)
     ```

   - Example (for a specific user ID):

     ```
     PERMIT IRRPTAUTH.GPMSERVE.specific_dds_login_userid CLASS(PTKTDATA)
     ID(passticket_creator_userid) ACCESS(UPDATE)
     ```

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

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

Establishing secure communications with the Distributed Data Server

You must ensure that communication between the Resource Monitoring tasks and the RMF Distributed Data Server (DDS) is protected. For secure network communications, it is recommended that you use

Application Transparent Transport Layer Security (AT-TLS) and Transport Layer Security (TLS), as described in this topic.

Before you begin

- Ensure that the basic setup for the Policy Agent is done. For information about policy-based networking and data protection, in *z/OS Communications Server: IP Configuration Reference*.
- Ensure that the basic certificate setup is done. For information about handling certificates for secure communications with RACF, see the topic on digital certificates in *z/OS Security Server RACF Security Administrator's Guide*.
- To enable AT-TLS and encrypted communication with the DDS server, you require the following:
  - Valid server certificate and the associated server private key
  - Certificate from a trusted Certificate Authority (CA).

  The example in Figure 42 on page 133 uses a key ring that is named `DDSServerKeyring` to store these credentials. This key ring must be accessible by the DDS server user ID (for example, GPMSERVE), and the server certificate must be the default certificate.
- To enable secure communication for the Resource Monitoring tasks, you require a certificate from a trusted Certificate Authority (CA). The example in Figure 43 on page 134 uses a key ring that is named `DDSClientKeyring` to store the credentials. This key ring must be accessible to the z/OSMF server user ID, which is IZUSVR, by default.

For a sample setup that uses RACF, see "RACF and digital certificates" in *z/OS Security Server RACF Security Administrator's Guide*, specifically "Implementation Scenario 1" and "Implementation Scenario 2."

For other security management products, refer to your product documentation for information about handling certificates and key rings.

About this task

Use this procedure to establish secure communications between the Resource Monitoring tasks and the RMF DDS server.

Procedure

1. **Configure the Policy Agent to allow secure communication with the RMF DDS server.**

   a) Enable the Policy Agent for AT-TLS.

   For information about AT-TLS data protection, see *z/OS Communications Server: IP Configuration Reference*.

   b) Configure the Policy Agent to specify secure communication for the DDS server.

For a sample policy, see Figure 42 on page 133.

```
#--------------------------------------------------#
#  TYQ: Created this file for the pagent           #
#  configuration for the GPMSERVE server.          #
#--------------------------------------------------#

 # RMF DDS SERVER RULE
 TTLSRule                          DDSServerRule
 {
   LocalPortRange                  8803
   Jobname                         GPMSERVE
   Direction                       Inbound
   TTLSGroupActionRef              DDSServerGRP
   TTLSEnvironmentActionRef        DDSServerENV
 }
 TTLSGroupAction                   DDSServerGRP
 {
   TTLSEnabled                     On
   Trace                           255
 }
 TTLSEnvironmentAction             DDSServerENV
 {
   HandshakeRole                   Server
   TTLSKeyringParms
   {
     Keyring                       DDSServerKeyring
   }
 }
```

Figure 42. Sample Policy Agent policy for simple SSL protection for the RMF DDS server

Where the AT-TLS policy properties are set, as follows:

`TTLSRule: Jobname`
Identifies the program for which this rule applies, which is the RMF DDS server in this example (GPMSERVE). If you set the property as shown, the policy affects GPMSERVE only; it does not affect other programs that are running on the system.

`TTLSRule: LocalPortRange`
Specifies the port of the RMF DDS server, which is 8803 in the example.

`TTLSRule: Direction`
Specifies the direction from which a connection must be initiated for this rule's action to be performed. In the example, `Inbound` is specified, which means that the rule applies to connection requests that arrive inbound to the local host. An application must issue an accept request to service this connection.

`TTLSKeyringParms: Keyring`
Specifies the key ring name of the RMF DDS server, which is `DDSServerKeyring` in the example. The key ring must contain the server certificate, the associated server private key, and the certificate of the trusted Certificate Authority (CA).

2. **Configure the Policy Agent to require secure communication for the Resource Monitoring tasks.**

For an example of a Policy Agent policy for setting up simple TLS protection for the Resource Monitoring tasks, see Figure 43 on page 134.

```
#------------------------------------------------#

  TTLSRule                          DDSClientRule
  {
    RemotePortRange                 8803
    RemoteAddr                      9.xxx.yyy.zzz
    Direction                       Outbound
    TTLSGroupActionRef              DDSClientGroup
    TTLSEnvironmentActionRef        DDSClientEnvironment
  }
  TTLSGroupAction                   DDSClientGroup
  {
    TTLSEnabled                     On
    Trace                           255
  }
  TTLSEnvironmentAction             DDSClientEnvironment
  {
    TTLSKeyRingParms
    {
      Keyring                       DDSClientKeyring
    }
    HandshakeRole                   Client
    Trace                           255
  }
```

Figure 43. Sample Policy Agent policy for simple TLS protection for the Resource Monitoring tasks

Where the AT-TLS policy properties are set, as follows:

TTLSRule: RemoteAddr
Specifies the remote IP address for which this rule's action is to be performed. In the example, it is the IP address of the remote RMF DDS server (9.xxx.yyy.zzz).

TTLSRule: RemotePortRange
Specifies the port of the remote RMF DDS server, which is 8803 in the example.

TTLSRule: Direction
Specifies the direction from which a connection must be initiated for this rule's action to be performed. In the example, Outbound is specified, which means that the rule applies to connection requests that are issued from the local host. An application must issue a connect request to initiate a connection.

TTLSKeyringParms: Keyring
Specifies the key ring name of the z/OSMF server, which is DDSClientKeyring in the example. The key ring must contain the certificate of the trusted Certificate Authority (CA) that issued the server certificate.

3. **Refresh the Policy Agent to have your changes take effect.**

   You can use the following command to refresh the Policy Agent:

   ```
   F PAGENT,REFRESH
   ```

Browser consideration for the Resource Monitoring task

Users who plan to use the Internet Explorer with Resource Monitoring task, and who plan to export the data collected in a dashboard to a CSV file, should ensure that the browser is enabled for automatic prompting for file downloads. This setting prevents the file download blocker from being invoked when the user downloads service definitions to the workstation.

Otherwise, if automatic prompting is disabled (the default setting), the download blocker prompts the user to accept these file downloads, causing the browser session to be reloaded and the active tabs to be closed. Users can avoid this disruption by enabling automatic prompting for file downloads.

For more information, see “Enabling automatic prompting for file downloads” on page 201.

Updating z/OS for the Software Deployment plug-in

If you selected to configure the Software Deployment plug-in, you might have system customization to perform, as described in this topic.

The Software Deployment plug-in contains the Software Management task, which becomes available to users in the navigation area when you configure the plug-in.

The Software Management task:

- Allows all users of the task to access deployment objects. Optionally, your installation can further restrict these authorizations, as described in the topic "Creating access controls for the Software Management task" on page 135.
- Works only with systems in the local sysplex. Optionally, your installation can allow the Software Management task to work with other sysplexes in your installation, as described in Chapter 9, "Configuring a primary z/OSMF for communicating with secondary instances," on page 163.

Creating access controls for the Software Management task

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

You can use a security manager, such as RACF, to control access to the task and to create more granular authorizations, such as restricting access to an object or an action. Access to the Software Management task and its objects are controlled through the following default resource profiles, which are defined in the ZMFAPLA class:

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

With the default access authorities in effect, z/OSMF users and administrators are allowed to perform all actions for all software instances, portable software instances, and deployments, and only z/OSMF administrators are allowed to retrieve information from product information files and add, modify, or remove categories.

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

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

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

Authorizing users to software instances

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

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.SWI.category.systemName.instanceName
```

Where:

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

  To perform an action, users must have the access authority that is required for that action for all the SAF resource names that are associated with the software instance.
- **systemName** is the name of the z/OSMF host system that has access to the volumes and data sets where the software instance resides. The system is inherited from the global zone that is associated with the software instance, and is defined in the Systems task.
- **instanceName** is the name of the software instance.

For example, if you have a software instance that is named z/OSV2R3_Test that can be accessed by system AQFT and is assigned to categories z/OS and Test, its SAF resource names would be:

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.SWI.z/OS.AQFT.z/OSV2R3_Test
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.SWI.Test.AQFT.z/OSV2R3_Test
```

Table 20 on page 136 lists the access authorities that you can assign to software instance resources and the actions that are permitted for each access authority. The Software Management task does not perform authorization checks to determine which software instances to display in a list or table; therefore, all software instances are displayed regardless of access authority.

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

Access Authority	Actions Allowed
READ	• View the properties of the software instance. • View information about the products, features, and FMIDs contained in a software instance. • View information about the data sets contained in a software instance. • Copy the properties of the software instance. • Deploy the software instance during a deployment. • Use the software instance as the model for priming a deployment configuration. • Generate reports for the software instance. • Export the software instance. • Perform workflows for the software instance.

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

Access Authority	Actions Allowed
UPDATE	In addition to the actions specified for READ access, users can perform the following actions: • Modify the software instance properties that are *not* used to create the SAF resource name for the software instance. This includes modifying the software instance explicitly using the **Modify** action or implicitly when completing a deployment where the objective is to replace the software instance. • Replace the software instance during a deployment. • Retrieve information from SMP/E about the products, features, and FMIDs contained in the software instance and make that information available to z/OSMF.
CONTROL	In addition to the actions specified for READ and UPDATE access, users can perform the following actions: • Create new software instances explicitly using the **Add** action or implicitly as part of the **Copy** action or when completing a deployment where the objective is to create a new software instance. • Modify the software instance properties that are used to create the SAF resource name for the software instance and control access to the software instance. This includes modifying the software instance explicitly using the **Modify** action or implicitly when completing a deployment where the objective is to replace the software instance. • Remove the software instance.

Authorizing users to portable software instances

Each software instance archive has a unique SAF resource name that can be used by your security manager to control access to the portable software instance. The SAF resource name for a portable software instance archive object has the following format:

```
<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.PSWI.category.systemName.portableSwiName
```

where:

PSWI
Indicates that the object that is associated with this SAF resource is a portable software instance.

category
Is the name of the category that is assigned to the portable software instance. If multiple categories are assigned, a separate SAF resource name is created for each category. If no category is assigned, the category value is NOCATEGORY. To perform an action, users must have the access authority that is required for that action for all the SAF resource names that are associated with the portable software instance.

systemName
Is the nickname of the z/OSMF host system that has access to the UNIX directory where the portable software instance resides. The system is defined in the z/OSMF Systems task.

portableSwiName
Is the name of the portable software instance.

The following describes the access authority levels that are used to control access to portable software instance objects and the actions that are permitted for each access authority. The Software Management task does not perform authorization checks to determine which portable software instances to display in a list or table; therefore, all portable software instances are displayed regardless of a user's allowed access authority.

Table 21. Actions users can take against portable software instances by access authority

Access Authority	Actions Allowed
READ	• View the properties of the portable software instance. • Deploy the portable software instance during a deployment.
UPDATE	In addition to the actions specified for READ access, users can perform the following action: • Modify the portable software instance properties that are not used to create the SAF resource name for the portable software instance.
CONTROL	In addition to the actions specified for READ and UPDATE access, users can perform the following actions: • Create new portable software instances explicitly by using the Add action. • Modify the portable software instance properties that are used to create the SAF resource name for the portable software instance and control access to the portable software instance. • Remove the portable software instance.

Authorizing users to deployments

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

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.DEP.category.deploymentName
```

where:

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

  To perform an action, users must have the access authority that is required for that action for all the SAF resource names that are associated with the deployment.
- **deploymentName** is the name of the deployment.

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

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.DEP.NOCATEGORY.z/OS_R21_Production
```

Table 22 on page 139 lists the access authorities that you can assign to deployment resources and the actions that are permitted for each access authority. The Software Management task does not perform authorization checks to determine which deployments to display in a list or table; therefore, all deployments are displayed regardless of access authority.

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

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

Authorizing users to categories

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

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

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.CAT.categoryName
```

Where:

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

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

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.CAT.z/OS
```

Table 23 on page 140 lists the access authorities that you can assign to category resources and the actions that are permitted for each access authority. Note that the Software Management task does not perform authorization checks to determine which categories to display in a list or table; therefore, all categories are displayed regardless of access authority.

Table 23. Actions users can take against categories by access authority

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

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

Because category names are part of the SAF resource name for software instances and deployments, you can use categories to control access to groups of software instances and deployments. For example, if you want to give Db2 system programmers CONTROL access to all software instances and deployments in the Db2 category and give other users READ access to these objects, define a SAF profile for the following resource:

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.*.DB2.**
```

If your installation is using RACF and your Db2 system programmers are defined in a group that is called DB2PROG, you can create a profile like the following:

```
RDEFINE ZMFAPLA +
(IZUDFLT.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.*.DB2.**) UACC(NONE)
PERMIT +
IZUDFLT.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.*.DB2.** +
CLASS(ZMFAPLA) ID(DB2PROG) ACCESS(CONTROL)
PERMIT +
IZUDFLT.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.*.DB2.** +
CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)
```

Controlling who can manage categories

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

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.CATEGORIES.MODIFY
```

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

```
RDEFINE ZMFAPLA +
(IZUDFLT.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.CATEGORIES.MODIFY) +
UACC(NONE)
PERMIT +
IZUDFLT.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.CATEGORIES.MODIFY +
CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)
```

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

Ensuring that all objects are assigned to a category

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

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.*.NOCATEGORY.**
```

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

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

Controlling who can retrieve product information files

A product information file is a file that contains information about one or more products, such as the product announce date and end of service date. Information that is extracted from these files are displayed in several views and reports in the Software Management task, such as in the *Products* view and in the End of Service report.

When you retrieve a product information file, z/OSMF reads the file and loads the extracted content into the database where data for the Software Management task is stored. The scope of this action is broad and spans all products in the database; therefore, this action should be carefully controlled.

To control who can retrieve product information files, permit users READ access to the following resource:

```
<SAF-prefix>.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.PRODUCT_INFO_FILE.RETRIEVE
```

By default, only z/OSMF administrators are permitted READ access to this resource. That is, by default, only z/OSMF administrators can retrieve product information files.

Creating product information files for the Software Management task

A *product information file* is a flat file, such as a text file, that contains information about one or more products. This information includes, for example, the product announce date, general availability date, and end of service date. You can create your own product information files or obtain them from a provider, such as IBM, another vendor, or a third party.

z/OSMF displays data from product information files in several views in the Software Management task. For example, this information is displayed in the Products page, the Products, Features, and FMIDs page, and the End of Service report.

Syntax for product information files

To be processed by z/OSMF, product information files must be formatted as JSON data and have the following syntax:

```
{
  "Version": "date-modified",
  "Products":
  [
    {
      "prodName": "product-name",
      "prodId": "product-identifier",
      "prodVRM": "version-release-modification",
      "GAAnnounceDate": "date-announced",
      "GADate": "general-availability-date",
      "URL": "URL",
      "EOSDate": "end-of-service-date",
      "country": "country"
    }
  ]
}
```

where,

date-modified
Date the file was created or last updated. The date must have the format YYYY-MM-DD. The date is required.

product-name
Name of the product. The name is optional, and is not used by z/OSMF. To omit the product name, exclude the field, type `null` as the value, or set the value equal to an empty string.

product-identifier
Identifier of the product. The product ID is required.

version-release-modification
Version, release, and modification level of the product. The value has the format *VV.RR.MM*, where *VV* is the two-digit version, *RR* is the two-digit release, and *MM* is the two-digit modification level. The version, release, and modification level are required.

date-announced
Date the vendor publicly announced the details of the product. The date must have the format YYYY-MM-DD. The date is optional. To omit the date, exclude the field or type `null` as the value.

general-availability-date
Date that a version or release of the product is available to all users. The date must have the format YYYY-MM-DD. The date is optional. To omit the date, exclude the field or type `null` as the value.

URL
URL that links to additional information about the product. This information can include, for example, product life cycle dates, product highlights, planning information, and technical descriptions. The URL is optional. To omit the URL, exclude the field, type `null` as the value, or set the value equal to an empty string.

end-of-service-date
Last date on which the vendor delivers standard support services for a particular version or release of the product. This date is the general end of service date. It does not account for lifecycle extensions. The date must have the format YYYY-MM-DD. The date is optional. To omit the date, exclude the field or type `null` as the value.

country
Country for which the end of service date is applicable. The country is optional. To omit the country, exclude the field, type `null` as the value, or set the value equal to an empty string.

The information for each product must be contained within separate braces ({ }) inside the brackets ([ ]), and each set of braces must be comma-separated. For a sample file that contains the information for two products, see Figure 44 on page 143.

Sample product information file

```
{
  "Version": "2011-06-30",
  "Products":
  [
    {
      "prodName": "z/OS",
      "prodId": "5694-A01",
      "prodVRM": "01.10.00",
      "GAAnnounceDate": "2008-08-05",
      "GADate": "2008-09-26",
      "URL": "http://www-03.ibm.com/systems/z/os/zos/",
      "EOSDate": "2011-09-30",
      "country": "US"
    },
    {
      "prodName": "z/OS",
      "prodId": "5694-A01",
      "prodVRM": "01.13.00",
      "GAAnnounceDate": "2011-07-12",
      "GADate": null,
      "URL": "",
      "country": "US"
    }
  ]
}
```

Figure 44. Sample product information file for the Software Management task

Working with the IBM product information file

The product information file that IBM supplies for System z® software is available for download from Product information file for IBM Z software products (public.dhe.ibm.com/services/zosmf/JSONs/IBMProductEOS.txt)

To load the contents of the file into z/OSMF, do one of the following:

- Load directly from the URL.
- Manually download the file at the URL to your local workstation.
- Manually download the file at the URL to a z/OS data set or UNIX file that the primary z/OSMF host system can access.

When you transfer the file from a workstation to a z/OS data set or UNIX file, transfer the file in binary format. To avoid errors, do not convert the file to the EBCDIC character set.

After you store the file in your desired location to retrieve its contents, complete the steps that are provided in the *Retrieving product information from product information files* topic in the z/OSMF online help.

Updating z/OS for the Sysplex Management plug-in

If you selected to configure the Sysplex Management plug-in, you have system customization to perform, as described in this topic.

To use the Sysplex Management task, your system requires the following updates:

- “BCPii installation and configuration” on page 144
- “Configure the CPC information in Systems task” on page 145
- “Authorize users to the z/OS console services REST API” on page 145
- “Create security structures for the Sysplex Management task” on page 145
- “Update the z/OSMF settings for managing a remote sysplex” on page 146

The examples in this topic use RACF commands. If your installation uses an external security manager other than RACF, your security administrator can refer to these examples when creating equivalent commands for your environment.

For a summary of the required profile authorizations for the Sysplex Management task, see “Resource authorizations for the z/OSMF optional plug-ins” on page 306 . IBM provides job IZUSPSEC in SYS1.SAMPLIB to assist you with performing these updates. The job contains RACF commands for creating the required security authorizations.

BCPii installation and configuration

In the z/OSMF Systems task, the Discover CPC function uses z/OS data set and file REST services and BCP internal interface (BCPii) services to query the topology of interconnected CPCs and LPARs in the sysplex. Therefore, you must ensure that both z/OS data set and file REST services and BCPii are configured in the sysplexes that are to be managed through the Systems task.

After BCPii is configured, have your security administrator ensure that the required authorizations are created for the BCPii services. In SYS1.SAMPLIB, the IZUSEC job includes sample RACF commands for enabling the z/OSMF core functions, including the BCPii services.

The following procedure describes the steps that are performed in the IZUSEC sample job. Some values are installation-specific and require modification for your environment.

1. **Define the profile for the BCPii services.**

   ```
   RDEFINE FACILITY HWI.APPLNAME.HWISERV UACC(NONE)
   ```

2. **Grant the administrator groups access to the BCPii services:**

   ```
   PERMIT HWI.APPLNAME.HWISERV CLASS(FACILITY) ID(IZUADMIN) ACCESS(READ)
   ```

3. **Define the profile for the BCPii request type of CPC.**

   ```
   RDEFINE FACILITY HWI.TARGET.<netid.nau> UACC(NONE) APPLDATA('<uppercasecommunityname>')
   ```

   Where:

   - *netid.nau* is the 3–17 character SNA name of the particular CPC.
   - *uppercasecommunityname* is the SNMP community name that is associated with the CPC. The same SNMP community name that was defined in the support element configuration for a particular CPC must also be defined in the security settings for each CPC to which communication is required.

4. **Define the profile for the BCPii request type of LPAR.**

   ```
   RDEFINE FACILITY HWI.TARGET.<netid.nau>.<imagename> UACC(NONE)
   ```

   Where:

   - *netid.nau* is the 3–17 character SNA name of the particular CPC
   - *imagename* is the 1–8 character LPAR name.

5. **Grant administrators READ access to the CPC and IMAGE profiles through BCPii functions.**

   ```

   PERMIT HWI.TARGET.<netid.nau> CLASS(FACILITY) ID(IZUADMIN) ACCESS(READ)
   PERMIT HWI.TARGET.<netid.nau>.<imagename> CLASS(FACILITY) ID(IZUADMIN) ACCESS(READ)
   ```

6. **Refresh the security database.** For example:

   ```
   SETROPTS RACLIST(FACILITY) REFRESH
   ```

For more information about BCPii, see *z/OS MVS Programming: Callable Services for High-Level Languages*.

Configure the CPC information in Systems task

Before you use the Sysplex Management task, it is recommended that you configure the CPC information in the z/OSMF Systems task. You can use either of the following methods to do so:

- Add CPC information manually
- Use the Discovery CPC function in Systems task to discover the CPC topology of the currently interconnected CPCs and LPARs in the sysplex.

The Discovery CPC function is a long running action; it might take several minutes to complete.

Authorize users to the z/OS console services REST API

Users of the Sysplex Management task require authorization to the z/OS console services REST API. For a system that uses RACF as the security manager, IBM provides job IZUGCSEC in SYS1.SAMPLIB to assist you with creating the authorizations. Ask your security administrator to edit the job for your environment and submit it.

In the IZUGCSEC job, a unique console name must be specified for each user of the Sysplex Management task. In z/OS, a valid console name is 2 to 8 characters and does not begin with a digit. Characters are alphanumeric and can also include the special characters #, $, and @.

Use the following convention to specify console names in the IZUGCSEC job:

```
<username>SP
```

Where *<username>* is the z/OSMF user name, followed by the letters SP. If the user name is more than six characters, specify the last six characters of the user name, followed by SP. For example, if the user name is IBMUSER, specify the console name BMUSERSP.

Note: If a z/OSMF user name must be shortened to six characters (followed by SP) and the resulting name would not be a valid console name, use the following convention instead: SP*<username>*, where *<username>* is the last six characters of the z/OSMF user name. Consider, for example, the z/OSMF user name `ID123456`. Using the last six characters of this name followed by SP would result in 123456SP, which is an invalid name because it begins with a digit. To avoid this problem, specify SP123456 for the console name.

Create security structures for the Sysplex Management task

To enable users to work with the Sysplex Management task, your external security manager, such as RACF, requires that a number of security structures are defined, as described in this topic, and that users are authorized to the appropriate system resources. If RACF or another security manager is installed, the security administrator can define profiles that control the use of these resources.

Before using the Sysplex Management task, have your security administrator verify that the following conditions exist:

- The security database, such as the RACF database, is shared across the sysplex.
- The SAFDFLT profile is defined in the REALM class. The SAFDFLT profile in the REALM class allows the security environment to be recognized.
- Each security database REALM has its own unique APPLDATA profile, which is associated with the SAFDFLT profile. The same SAFDFLT APPLDATA value is used across all systems in the sysplex. Define the name by using the SAFDFLT profile in the REALM class. Substitute an appropriate string for the *plexname*, such as the name of the sysplex or another unique string.

  Example:

  ```
  SETROPTS GENERIC(REALM)
  RDEFINE REALM SAFDFLT APPLDATA('<plexname OR other unique string>')
  ```

```
SETROPTS RACLIST(REALM) CLASSACT(REALM)
SETROPTS RACLIST(REALM) REFRESH
```

- TRUSTED attribute must be assigned to the CEA started task.
- CEA address space is started in full function mode.
- Users are authorized to the appropriate resources, as described in Table 45 on page 306 .

To make the preceding updates effective, you must:

1. Refresh your security database. Example:

   ```
   SETROPTS RACLIST(SERVAUTH) REFRESH
   ```

   ```
   SETROPTS RACLIST(ZMFAPLA) REFRESH
   ```

2. Restart CEA.

The Sysplex Management plug-in requires access to local resources on your z/OS system. Table 45 on page 306 describes the security requirements for the Sysplex Management plug-in.

Update the z/OSMF settings for managing a remote sysplex

If you plan to manage a remote sysplex in addition to the local sysplex in the primary z/OSMF instance, ask your z/OSMF administrator to perform the following updates:

1. The remote sysplex to be managed must have a z/OSMF instance running in one of its systems. Open **z/OSMF Settings** > **Systems table** > **Add system** on the primary z/OSMF instance and define the system on which the z/OSMF instance is running in the remote sysplex. Specify the URL of the z/OSMF instance when you update the Systems table.
2. Ensure that single sign-on is configured for the system that is running the primary z/OSMF instance and for the secondary z/OSMF instances in other sysplexes.
3. Open **z/OSMF Settings** > **Systems table** on the primary z/OSMF instance and define the CPC objects on the primary z/OSMF instance, either manually or by running the discovery function, which retrieves CPC information by calling BCPii services.

z/OSMF does not verify the accuracy of your input. Ensure that the information you provide is correct and complete. Incorrect or missing information can cause the major views of the Sysplex Management task to be unavailable:

- **Physical View**
- **Connectivity View**
- **Connectivity Details View**

Updating z/OS for the Workload Management plug-in

If you selected to configure the Workload Management plug-in, you might have system customization to perform, as described in this topic.

This topic contains the following sections:

- "Authorizing the z/OSMF started task user ID to the MVSADMIN.WLM.POLICY profile" on page 147
- Table 24 on page 148
- "Using authorization levels for the Workload Management task" on page 148
- "Using a browser with WLM service definitions" on page 149.

IBM provides job IZUWMSEC in SYS1.SAMPLIB to assist you with performing these updates. The job contains RACF commands for creating the required security authorizations.

The Workload Management task is used for managing WLM resources in the IBM Cloud Provisioning and Management for z/OS provisioning tasks. For more setup considerations, see Chapter 4, "Preparing to use Cloud Provisioning," on page 51.

Authorizing users to the MVSADMIN.WLM.POLICY profile

Users of the Workload Management task require UPDATE access to resources that are protected by the profile MVSADMIN.WLM.POLICY in class FACILITY. If you run the CFZSEC job when you are setting up the Common Information Model (CIM) server for z/OSMF, all users who are authorized for the CIM server are automatically authorized for this profile. If this set of authorizations is acceptable in your environment, no further steps are needed.

However, if not all CIM server users should have access to the MVSADMIN.WLM.POLICY profile, you must perform additional steps to avoid creating unwanted authorizations. To do so, complete the following steps:

- Edit the CFZSEC job before you run it to remove any unneeded authorization commands from the job step ENWLM.
- Have your security administrator create a separate group for WLM users. Give the group UPDATE access to profile MVSADMIN.WLM.POLICY. If such a group exists in your environment, you can use the existing group instead of creating a new group.

  As an example, the following steps show sample RACF commands for creating a separate WLM group and authorizing it to the MVSADMIN.WLM.POLICY profile:

  1. Create the WLM group:

     ```
     ADDGROUP "WLMGroupName" OMVS(GID("WLMGroupGID"))
     ```

  2. Authorize the WLM group:

     ```
     PERMIT MVSADMIN.WLM.POLICY CLASS(FACILITY) ID("WLMGroupName") ACCESS(UPDATE)
     ```

  3. Have your changes take effect:

     ```
     SETROPTS RACLIST(FACILITY) REFRESH
     ```

- During the z/OSMF configuration process, edit the IZUWMSEC job before you run it and add the name of the WLM security group that your installation uses for authorizing users to the z/OS Workload Management component on your system. The IZUAUTH contains commands for connecting users to the group.

Authorizing the z/OSMF started task user ID to the MVSADMIN.WLM.POLICY profile

The Workload Management task performs periodic queries of WLM on the z/OS host system. To perform the queries, the Workload Management task uses the z/OSMF started task user ID. Therefore, you must ensure that the z/OSMF started task user ID has READ access to the profile MVSADMIN.WLM.POLICY and authorization to the CIM server.

To manually authorize the z/OSMF started task user ID for the MVSADMIN.WLM.POLICY profile and the CIM server, complete the following steps:

1. Grant the z/OSMF started task user ID read access to the profile MVSADMIN.WLM.POLICY. By default, this user ID is IZUSVR.

   In RACF, you can use the following command:

   ```
   PERMIT MVSADMIN.WLM.POLICY
   CLASS(FACILITY) ID(IZUSVR) ACCESS(READ)
   ```

2. Connect the z/OSMF started task user ID to the CIM user group. By default, the CIM user group is CFZUSRGP.

   In RACF, you can use the following command:

   ```
   CONNECT IZUSVR GROUP(CFZUSRGP)
   ```

Ensure that the user ID under which the CIM server is running has SURROGAT access for the z/OSMF started task user ID. If a generic BPX.SRV.** profile is already authorized in the SURROGAT class (for example, because you ran the CFZSEC job when setting up the CIM server), no additional action is required. Otherwise, define a discrete profile for the z/OSMF started task user ID and authorize it. If necessary, refresh the SURROGAT class.

Required security group for Workload Management

With the IZUWMSEC job, your security administrator can supply the name of the WLM security group that your installation uses for authorizing users to the z/OS Workload Management component on your system. The IZUAUTH job contains commands for connecting users to the group. As supplied by IBM, the IZUAUTH job contains a RACF CONNECT command for a group called WLMGRP. You can substitute a different group name. See Table 24 on page 148.

Table 24. Security group required for the Workload Management plug-in

Group	Purpose	Created by
WLMGRP	Security group for users of the Workload Management task.	ADDGROUP command or an equivalent security command for creating user groups.

Using authorization levels for the Workload Management task

Using predefined authorization levels, your installation can authorize users to specific functions within the Workload Management task.

The Workload Management task supports the following authorization levels:

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

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

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

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

Your installation can manage user authorizations through your security management product, such as RACF. Grant access authority to the users and groups, as described in Table 25 on page 149.

Table 25. Workload Management task authorizations for z/OSMF

Required authorization level of user or group	Required SAF access authority
View	READ access for profile *<SAF-prefix>*.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.VIEW
Install	READ access for profile *<SAF-prefix>*.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.INSTALL
Modify	READ access for profile *<SAF-prefix>*.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.MODIFY

If these default settings do not meet your needs, you can change the SAF authority of these respective groups for the profiles that are shown in Table 25 on page 149.

Alternatively, you can define new custom groups for the Workload Management task. For example, the following RACF commands can be used to define a custom group WLMPOLOP, which is authorized for the View and Install functions. This set of authorizations is equivalent to a WLM policy operator.

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

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

```
CONNECT "userid" GROUP(WLMPOLOP)
```

Using a browser with WLM service definitions

Users who plan to use the Internet Explorer browser to work with WLM service definitions should ensure that the browser is enabled for automatic prompting for file downloads. This setting prevents the file download blocker from being invoked when the user downloads service definitions to the workstation. Otherwise, if automatic prompting is unavailable (the default setting), the download blocker prompts the user to accept these file downloads, causing the browser session to be reloaded and the active tabs to be closed. Users can avoid this disruption by enabling automatic prompting for file downloads. For more information, see "Enabling automatic prompting for file downloads" on page 201.

Avoiding a potential synchronization error

After you begin using the Workload Management task, avoid using other applications, such as the z/OS WLM Administrative Application, to modify and install WLM service definitions. During a modify operation, the Workload Management task automatically extracts the installed service definition from the WLM couple data set and imports it into the service definition repository. This import fails if the Workload Management task finds that a service definition exists in both the repository and the couple data set with the same name and description, but different content. If this error occurs, you can resolve it by either changing the name or description of the service definition in the repository, or deleting it from the repository.

Updating z/OS for the z/OS Operator Consoles task

Some setup is required before you can use a z/OS console with the z/OS Operator Consoles task, as described in this topic.

See the following topics:

- "Authorizing users to the z/OS Operator Consoles task" on page 150
- "Host system customization for the z/OS Operator Consoles task" on page 150
- "Security setup for the z/OS Operator Consoles task" on page 150

Authorizing users to the z/OS Operator Consoles task

To view and access the z/OS Operator Consoles task in the z/OSMF navigation area, users require READ access to resource `<SAF-prefix>.ZOSMF.CONSOLES.ZOSOPER` in the ZMFAPLA class. By default, *<SAF-prefix>* is IZUDFLT.

Host system customization for the z/OS Operator Consoles task

To use a z/OS console with the z/OS Operator Consoles task, do the following:

- Ensure that the system is defined to z/OSMF. The systems that are displayed in the table on the Overview tab are retrieved from the Systems task of the z/OSMF Settings category. By default, z/OSMF provides a system definition for the z/OS® system that hosts the z/OSMF instance to which your web browser is connected, and it provides a system definition for the systems that belong to the same JES2 multi-access spool (MAS) or JES3 complex as the z/OSMF host system. If you want z/OSMF to interact with other systems, you must create the corresponding system definitions.
- Establish an extended MCS console for the system, then grant permission to a user to use that console. This work is performed outside of z/OSMF, typically by a security administrator. For instructions, see "Security setup for the z/OS Operator Consoles task" on page 150.

The attributes of the EMCS console that is started by z/OSMF are controlled by the OPERPARM settings of the user profile *<consolename>*. Thus, for example, if a user wants the z/OS Operator Consoles task to create a console named `console1`, a user profile named `console1` must exist and contain an OPERPARM segment with the appropriate settings.

Security setup for the z/OS Operator Consoles task

IBM provides job IZUGCSEC in SYS1.SAMPLIB to assist you with performing these updates. The job contains RACF commands for creating the required security authorizations. For more information, see "Resource authorizations for the z/OS console REST interface" on page 302.

Updating z/OS for the IBM zERT Network Analyzer Plug-in

If you selected to configure the IBM zERT Network Analyzer plug-in, you might have system customization to perform, as described in this topic.

This topic contains the following information:

- Authorize users to the IBM zERT Network Analyzer task
- Db2 for z/OS customization for the IBM zERT Network Analyzer task
- Install Java Database Connectivity.
- Connect IBM zERT Network Analyzer task with the Db2 for z/OS database.

The examples in this topic use RACF commands. If your installation uses an external security manager other than RACF, your security administrator can refer to these examples when creating equivalent commands for your environment.

For a summary of the required profile authorizations for the IBM zERT Network Analyzer plug-in, see "Resource authorizations for the z/OSMF optional plug-ins" on page 306. IBM provides job IZUNASEC in SYS1.SAMPLIB to assist you with performing these updates. The job contains RACF commands for creating the required security authorizations.

Authorize users to the IBM zERT Network Analyzer task

About this task

Users of the IBM zERT Network Analyzer task require access to resources that are protected by the profile <*SAF-prefix*>.ZOSMF.ZERT_NETWORK_ANALYZER in class ZMAFPLA. Your z/OS security administrator must perform additional steps to create the necessary authorizations.

Procedure

1. During the z/OSMF configuration process, edit the IZUNASEC job before you run it.
2. Add the names of the users who should be authorized to access the IBM zERT Network Analyzer task.

```
/*  Connect the users of the zERT Network Analyzer to the         */
/*  zERT Network Analyzer group                                   */
CONNECT USER1 GROUP(IZUZNA)
CONNECT USER2 GROUP(IZUZNA)
/*  End connect the users to zERT Network Analyzer group          */
```

3. Save your changes and run the updated IZUNASEC job.

Db2 for z/OS customization for the IBM zERT Network Analyzer task

About this task

The IBM zERT Network Analyzer task stores and queries SMF data in a Db2 for z/OS database. Before you can use the task, this database must be created in a suitable Db2 for z/OS subsystem and the connectivity information for the database must be configured in the IBM zERT Network Analyzer.

IBM provides tooling and templates in the SYS1.SAMPLIB data set to help your local Db2 for z/OS database administrator (DBA) create the IBM zERT Network Analyzer database.

Procedure

1. Determine the local parameters regarding where the IBM zERT Network Analyzer database is defined.

   Your local DBA decides which Db2 for z/OS subsystem contains the IBM zERT Network Analyzer database objects as well as the specific Db2 for z/OS resources (storage pools, buffer pools, and so forth) to be allocated to these objects.

   Tip: You can initially deploy the IBM zERT Network Analyzer database objects and the plug-in on a test system. The test system should be a place where you can easily get familiar with the operation of the plug-in and can better understand the Db2 and system resource requirements when running queries against your SMF record data. Depending on the number of imported SMF records and the complexity of your queries, you might consider initially limiting query execution to specific times of day or specific systems to minimize system impacts.

   Note: The amount of Db2 for z/OS table storage required by IBM zERT Network Analyzer varies, but you can use the following guidelines to estimate the table storage required in your environment:

   - Start with an allocation of 20 MB to hold the core security session data and operational data related to data management and user-built queries. If you are collecting zERT data from an unusually large number of unique security sessions across the z/OS systems, you might eventually need to add to this amount over time.

- Estimate the space that is required to store the maximum number of SMF Type 119 zERT Summary (subtype 12) records that is represented in the database at one time and add that amount to the initial 20 MB. To do so, see details in Table 26 on page 152.

Table 26. How to estimate the space for SMF Type 119 zERT Summary (subtype 12) records

Step	Task	Formula	Example
1	Estimate the number of unique security sessions that typically exist across the set of z/OS systems from which you are collecting zERT data.	Use local procedures to estimate this value.	Assume that 10,000 unique security sessions typically exist across all of the zERT-monitored systems. **UniqueSessions = 10,000**
2	Determine the maximum number of SMF intervals to be represented in the IBM zERT Network Analyzer database at a single time.	**MaxIntervals = ((1440 / SMFInterval) * Days)** where: **1440** = the number of minutes in a day; **SMFInterval** = the SMF interval in minutes as defined in your SMFPRMxx parmlib member. Note that if you use different SMF intervals across the zERT-monitored z/OS systems, use the average interval length across the different systems here; **Days** = the maximum number of days' worth of SMF data that is stored in the database at a single time.	Assume the average SMF interval is set to 20 minutes and you plan to store 30 days of SMF data in the zERT Network Analyzer database: MaxIntervals = (1440 / 20) * 30 = 72 * 30 **= 2160**
3	Determine how many SMF 119 subtype 12 records are collected over the Days value and imported into the database.	**MaxRecords = UniqueSessions * MaxIntervals**	MaxRecords = 10,000 * 2160 **= 21,600,000**
4	Determine how much DASD storage is required to store the data for the maximum number of records. Each SMF 119 subtype 12 record consumes about 500 bytes of DASD storage above and beyond the base space allocation of 20 MB.	**DASDSpaceMB = 20 + ((MaxRecords * 500) / 1,048,576)**	DASDSpaceMB = 20 + ((21,600,000 * 500) / 1,048,576) = 20 + 10,299 **= 10,319MB or 10GB**

According to the example shown in the table, you need to allocate a total of 10 GB of space in the storage group that is used for your IBM zERT Network Analyzer database's table spaces.

2. Create the IBM zERT Network Analyzer database.

   Your local DBA should use the following sample information to create the database for your environment:

   - The IZUZNADT member of the SYS1.SAMPLIB data set.

     IZUZNADT contains a Data Definition Language (DDL) template for creating the required database objects. The template contains all the required DDL commands but contains variables for many of the resource names and parameter settings. The DBA should set values for the variables that allow the IBM zERT Network Analyzer database to comply with the local Db2 for z/OS conventions and allocation strategies.

     Note: The IZUZNADT prolog commentary explains each of the variables.
   - The IZUZNADI member of the SYS1.SAMPLIB data set.

     IZUZNADI is a sample variable substitution data set in which the DBA can specify the desired values for each of the template variables defined in IZUZNADT. The IZUZNADI sample specifies the default values for each of the variables, but the DBA can override any of the variables as needed.
   - The IZUZNADG member of the SYS1.SAMPLIB data set.

     IZUZNADG is a REXX exec that reads the IZUZNADT template and the IZUZNADI variable substitution data sets and generates an executable set of DDL customized with the DBA's variable substitution values. Your DBA can use the resulting DDL data set in SPUFI or as input to a local JCL stream used to add new databases to a local Db2 for z/OS subsystem.

     Note: Instructions for using the IZUZNADG exec are available by running the exec with the --HELP parameter.
3. Collect the connectivity information that is required to link the IBM zERT Network Analyzer plug-in with the Db2 for z/OS database to be used by the plug-in.

   The DBA must provide database connectivity information to the person setting up the IBM zERT Network Analyzer plug-in. This information includes:

   - The hostname, or IP address, on which the Db2 for z/OS subsystem is running
   - The TCP port number of the subsystem
   - The database location name, which is the value of the LOCATION parameter of the DSNJU003 utility
   - The z/OS user ID that is permitted to connect to, store data into, and query data in the IBM zERT Network Analyzer database
   - The password for that z/OS user ID
   - The JDBC classpath for the Db2 for z/OS JDBC driver on the system where the IBM zERT Network Analyzer executes

   See Connect IBM zERT Network Analyzer task with the Db2 for z/OS database for how to use this connectivity information.
4. (**Optional**) Modify the setting of the DSN6SYSP URLGWTH parameter.

   Depending on the size of the SMF dump data sets that you plan to import into IBM zERT Network Analyzer and the setting of the DSN6SYSP URLGWTH parameter, you might see one or more DSNJ031I messages when importing the SMF dump data sets. You can modify the setting of the DSN6SYSP URLGWTH parameter to reduce the number of DSNJ031I messages. For more information, see *UR LOG WRITE CHECK field (URLGWTH subsystem parameter)* in *Installing and migrating Db2*.
5. **(Optional)** Define additional 4K and 32K work files to be used by IBM zERT Network Analyzer

   By default, small 4K and 32K work files are defined for use by the Db2 for z/OS subsystem. You might need to increase the size of the 4K and 32K work files to allow IBM zERT Network Analyzer to operate more efficiently. For more information, see *DSNTIP9: Work file database panel* in *Installing and migrating Db2*.

   Restriction: Db2 for z/OS packages associated with the NULLID collection will be used when IBM zERT Network Analyzer plug-in connects to the Db2 for z/OS subsystem. The collection-id is an optional parameter when binding Db2 for z/OS packages where NULLID is the default collection-id value for distributed applications such as IBM zERT Network Analyzer. For more information, review the DSNTIJLC and DSNTIJLR Db2 for z/OS jobs.

Install Java Database Connectivity

About this task

The IBM zERT Network Analyzer task uses the Java Persistence API (JPA) to access the contents of the Db2 database. JPA, in turn, uses Java Database Connectivity (JDBC). If you have not already installed JDBC, or you have not run the DB2Binder utility as part of that installation, you have additional customization steps to perform.

Procedure

Follow the instructions in *Installing the IBM Data Server Driver for JDBC and SQLJ as part of a Db2 installation* in *Programming for Db2 for z/OS*.

Connect the IBM zERT Network Analyzer task with the Db2 for z/OS database

About this task

You must provide the IBM zERT Network Analyzer task with Db2 for z/OS database connectivity information before using the task for any additional functions.

Procedure

1. Launch the IBM zERT Network Analyzer task. The first time you launch the task, you are directed immediately to the **Database Settings** panel.
    - To open the IBM zERT Network Analyzer task using the z/OSMF traditional view, expand the **Analysis** category in the navigation area, and select **IBM zERT Network Analyzer**.
    - To open the IBM zERT Network Analyzer task using the z/OSMF desktop view, click the **IBM zERT Network Analyzer** icon .
2. Enter the database connectivity information that is provided to you by the database administrator (DBA) as part of completing the Db2 for z/OS customization for the IBM zERT Network Analyzer task procedure.

    Note: After you save the connectivity information, the IBM zERT Network Analyzer task restarts using the configuration information. You must stop and restart your browser session when the task restarts.

Deployment guidelines for IBM zERT Network Analyzer

Here are some important guidelines to consider as you deploy the IBM zERT Network Analyzer.

You can initially deploy the IBM zERT Network Analyzer plug-in and database on a test system. Use a system where you can familiarize yourself with the plug-in operation and the Db2 for z/OS and system resource requirements. Depending on the number of imported SMF records and the complexity of your queries, you might also consider initially limiting query execution to specific times of day or specific systems to minimize system impacts.

The IBM zERT Network Analyzer import and query processing for large amounts of data might take a long time and consume significant CPU cycles. Because IBM zERT Network Analyzer is a Java application, and Db2 for z/OS is used as its data store, much of the IBM zERT Network Analyzer processing is eligible to run on IBM z Integrated Information Processor (zIIP) specialty engines. You can run IBM zERT Network Analyzer on a system that has sufficient zIIP capacity available to minimize the general-purpose processor CPU costs that are associated with import and query operations. You can also use WLM policies to properly prioritize the DDF workload initiated by IBM zERT Network Analyzer, so it does not impact more important workloads on the system.

If you plan to import SMF dump data sets with large numbers of SMF records (hundreds of thousands or millions), you can reduce the import time and processing costs by filtering out any of the SMF records that are not SMF type 119 subtype 12 before you run the import operation. These non-zERT records can be stripped out of your SMF dump data sets by using the IFASMFDP program. To do so, specify the SMF dump data set containing the SMF type 119 subtype 12 and other SMF records as the input data set (INDD) and specify `OUTDD(<outDDname>,TYPE(119(12)))`. For more information about using the IFASMFDP SMF data set dump program, see *z/OS MVS System Management Facilities (SMF)*.

You can use a Db2 for z/OS subsystem that is located with IBM zERT Network Analyzer to reduce latency and elapsed times when you run operations such as SMF imports and queries.

Chapter 8. Autostart concepts in z/OSMF

z/OSMF is started when you IPL your z/OS system. This behavior, which is referred to as *z/OSMF autostart*, means that z/OSMF is available for use as soon as the system is up.

To make the best use of the z/OSMF autostart capability, you must plan how to deploy one or more z/OSMF servers in your environment. Generally, having one z/OSMF server active in a sysplex or monoplex is sufficient, but you might choose to have more, based on your workload requirements. The goal is to ensure that at least one z/OSMF server is always active in your environment.

For a monoplex, little or no planning is needed. The z/OSMF server is started when you IPL the system.

For a sysplex, more planning is required. You can choose to have one z/OSMF server autostart on a particular system and be used by the other systems in the sysplex. Or, you can select a subset of systems, or several subsets, and associate each subset with a specific z/OSMF server within an autostart group.

If you do not want to use the autostart capability, some planning is needed to either remove it or to disable autostart, even in a monoplex. For more information, see "Scenario 4: The z/OSMF server is not autostarted on any system" on page 160.

The set of systems that is served by an autostarted server is known as the *autostart group*. z/OSMF includes one autostart group by default. To have more z/OSMF servers autostarted in a sysplex, you must associate each server—and the systems it serves—with a unique autostart group name.

In your planning, you must decide:

- What the autostart groups will be in your sysplex
- Which systems will autostart a z/OSMF server
- Which systems will share the use of the autostarted server; these systems must be defined to the same autostart group.

Only one z/OSMF server can be active per autostart group in the sysplex. An autostarted z/OSMF server holds an enqueue on the z/OSMF data directory file system, and handles the z/OSMF requests from other systems that are connected to the same autostart group. Based on your planning, you can enable the desired number of z/OSMF autostart groups for your sysplex.

To create one or more autostart groups in z/OSMF, use the following statements in parmlib member IZUPRMxx in combination:

AUTOSTART(<u>LOCAL</u>|CONNECT)

Specifies the capability for autostarting the z/OSMF server on this system.

- AUTOSTART(LOCAL) indicates that the system is capable of autostarting a z/OSMF server.
- AUTOSTART(CONNECT) indicates that the system cannot autostart a z/OSMF server. The system will, instead, use the z/OSMF server on another system in the same autostart group.

By default, AUTOSTART is set to LOCAL.

AUTOSTART_GROUP(<u>IZUDFLT</u>|'*nnnnnnnn*')

Assigns a name to the autostart group. z/OSMF includes one AUTOSTART_GROUP name by default (called IZUDFLT). To associate a group of systems with a different autostart group, ensure that each system specifies the same value for AUTOSTART_GROUP.

By default, AUTOSTART_GROUP is set to IZUDFLT.

If one autostart group is sufficient for your sysplex, it is recommended that you allow each system to use the IZUDFLT autostart group.

The following scenarios are valid in a multi-system environment:

- "Scenario 1: One z/OSMF server is autostarted for the entire sysplex" on page 158
- "Scenario 2: Multiple z/OSMF servers and autostart groups per sysplex" on page 158

- “Scenario 3: Some systems belong to an autostart group, and other systems do not” on page 159
- “Scenario 4: The z/OSMF server is not autostarted on any system” on page 160.

Scenario 1: One z/OSMF server is autostarted for the entire sysplex

In this scenario, the z/OSMF server is autostarted on one system in the sysplex. All systems are associated with the default autostart group, which is named IZUDFLT.

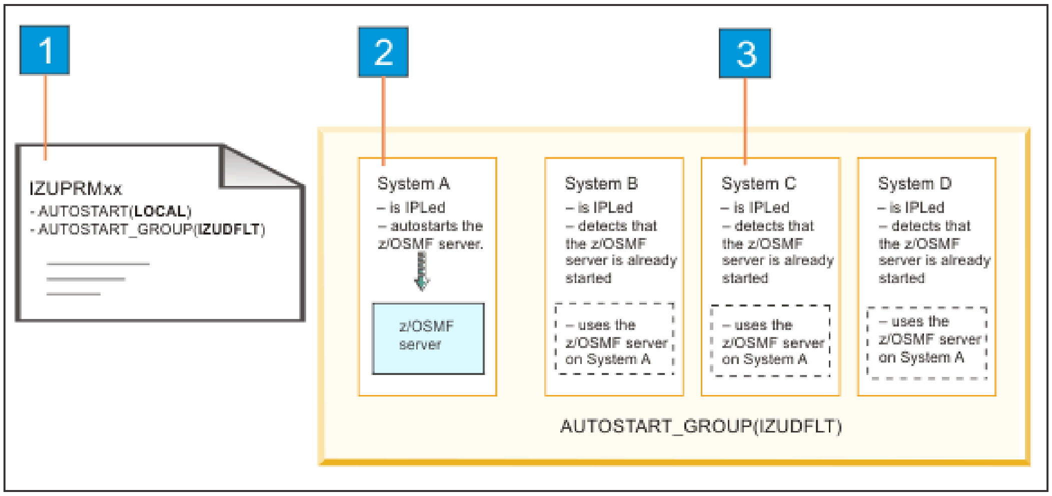

1
2
3
IZUPRMxx
- AUTOSTART(LOCAL)
- AUTOSTART_GROUP(IZUDFLT)
System A
– is IPLed
– autostarts the z/OSMF server.
z/OSMF server
System B
– is IPLed
– detects that the z/OSMF server is already started
– uses the z/OSMF server on System A
System C
– is IPLed
– detects that the z/OSMF server is already started
– uses the z/OSMF server on System A
System D
– is IPLed
– detects that the z/OSMF server is already started
– uses the z/OSMF server on System A
AUTOSTART_GROUP(IZUDFLT)

Figure 45. Scenario 1: One z/OSMF server is autostarted for the entire sysplex

In Figure 45 on page 158:

1. Each system uses the following default values for autostart:

   ```
   AUTOSTART(LOCAL)
   AUTOSTART_GROUP(IZUDFLT)
   ```

   With these values set for all systems, the first one to complete IPL is the system on which the z/OSMF server is started.
2. System A is the first system to complete IPL in the sysplex. Its attempt to autostart the z/OSMF server is successful.
3. System B, C, and D complete IPL. These systems detect that an autostarted server is active on System A, so they do not attempt a server. Instead, they use the server on System A.

In a sysplex of z/OS V2R3 systems, this scenario is enabled by default. If it is sufficient for your requirements, you can use the z/OSMF defaults. If you care *which* system in the sysplex autostarts the z/OSMF server, keep the default values for that system and change the AUTOSTART value to CONNECT for all other systems in the same autostart group.

Scenario 2: Multiple z/OSMF servers and autostart groups per sysplex

In this scenario, more than one z/OSMF server is to be autostarted in a sysplex. Suppose, for example, that you have a sysplex of four systems: A, B, C, and D. You plan to have System A autostart a server and share it with System B. Similarly, System C will autostart a server and share it with System D.

In this scenario, each server and the systems it serves are associated with an autostart group, as follows:

- System A and System B are associated with the autostart group IZUDFLT
- System C and System D are associated with the autostart group ALTERNATE.

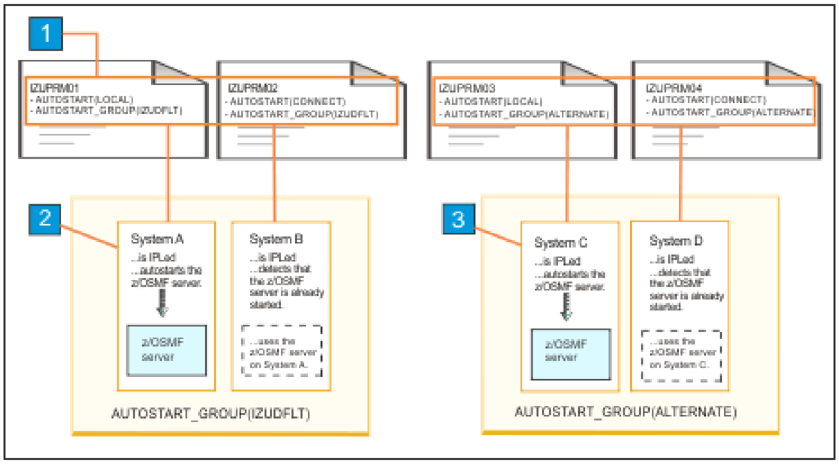

1
IZUPRM01
- AUTOSTART(LOCAL)
- AUTOSTART_GROUP(IZUDFLT)
IZUPRM02
- AUTOSTART(CONNECT)
- AUTOSTART_GROUP(IZUDFLT)
IZUPRM03
- AUTOSTART(LOCAL)
- AUTOSTART_GROUP(ALTERNATE)
IZUPRM04
- AUTOSTART(CONNECT)
- AUTOSTART_GROUP(ALTERNATE)
2
System A
...is IPLed
...autostarts the z/OSMF server.
z/OSMF server
System B
...is IPLed
...detects that the z/OSMF server is already started.
...uses the z/OSMF server on System A.
AUTOSTART_GROUP(IZUDFLT)
3
System C
...is IPLed
...autostarts the z/OSMF server.
z/OSMF server
System D
...is IPLed
...detects that the z/OSMF server is already started.
...uses the z/OSMF server on System C.
AUTOSTART_GROUP(ALTERNATE)

Figure 46. Scenario 2: Multiple z/OSMF servers and autostart groups per sysplex.

In Figure 46 on page 159:

1. Each system uses a different IZUPRMxx member with different settings for AUTOSTART and AUTOSTART_GROUP.
2. System A autostarts a z/OSMF server. System B uses the autostarted server on System A.
3. System C autostarts a z/OSMF server. System D uses the autostarted server on System C.

Scenario 3: Some systems belong to an autostart group, and other systems do not

In this scenario, some systems belong to an autostart group, and other systems do not. Suppose, for example, that you have a sysplex of four systems: System A, B, C, and D. In this sysplex, you plan to have System A autostart the z/OSMF server and share it with System B. System C and System D will not use an autostarted z/OSMF server. The z/OSMF server can be started on these systems manually, by using the **START** operator command with the name of the z/OSMF started procedure (IZUSVR1).

In this scenario:

- System A and System B are defined to autostart group IZUDFLT
- System C and System D are not defined to an autostart group.

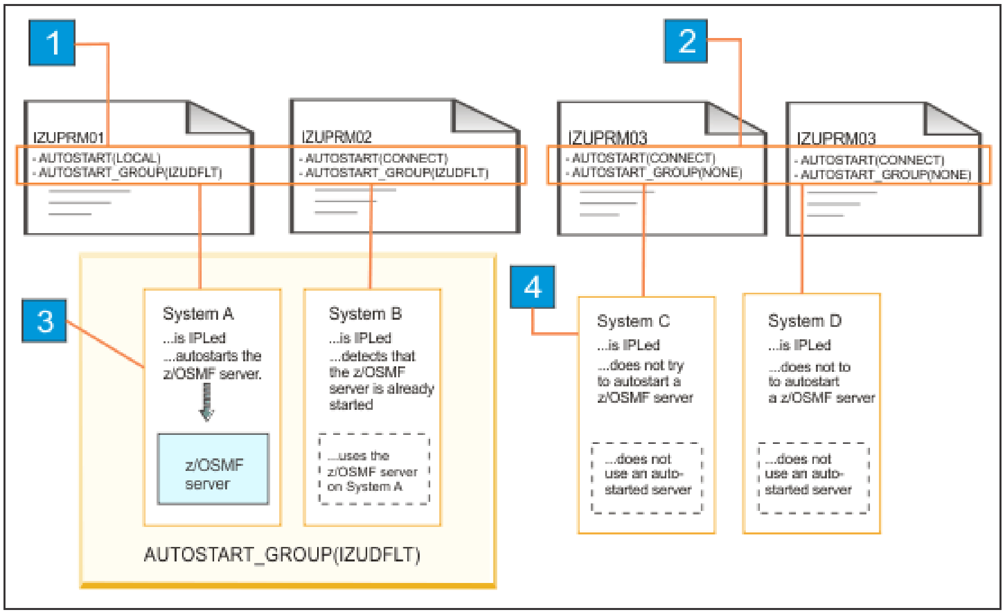

1
2
IZUPRM01
- AUTOSTART(LOCAL)
- AUTOSTART_GROUP(IZUDFLT)
IZUPRM02
- AUTOSTART(CONNECT)
- AUTOSTART_GROUP(IZUDFLT)
IZUPRM03
- AUTOSTART(CONNECT)
- AUTOSTART_GROUP(NONE)
IZUPRM03
- AUTOSTART(CONNECT)
- AUTOSTART_GROUP(NONE)
3
System A
...is IPLed
...autostarts the z/OSMF server.
z/OSMF server
System B
...is IPLed
...detects that the z/OSMF server is already started
...uses the z/OSMF server on System A
AUTOSTART_GROUP(IZUDFLT)
4
System C
...is IPLed
...does not try to autostart a z/OSMF server
...does not use an auto-started server
System D
...is IPLed
...does not to to autostart a z/OSMF server
...does not use an auto-started server

Figure 47. Scenario 3: One z/OSMF server is autostarted for a subset of systems in a sysplex.

In Figure 47 on page 160:

1. Systems A and B specify AUTOSTART_GROUP(IZUDFLT).
2. Systems C and D specify a non-functioning autostart group name, NONE.
3. System A autostarts a z/OSMF server. System B uses the autostarted server on System A.
4. Systems C and D do not use an autostarted z/OSMF.

Scenario 4: The z/OSMF server is not autostarted on any system

In this scenario, no z/OSMF servers are started automatically during system IPL. That is, the autostart capability is disabled. Perhaps, you prefer to start the server manually, with the **START** operator command, as done in previous releases.

To disable the autostarting of z/OSMF servers in a sysplex, do the following for each system in the sysplex:

- To prevent a z/OS system from autostarting the z/OSMF server, ensure that the system uses a IZUPRMxx member that specifies `AUTOSTART(CONNECT)`. This setting causes the system to connect to the autostart group that is specified on the AUTOSTART_GROUP statement, rather than autostarting its own server.
- To prevent a z/OS system from connecting to an autostart group, specify the name of a group on the AUTOSTART_GROUP parameter that is not used by any autostart server in the sysplex. For example, `AUTOSTART_GROUP('NONE')`.
- Similarly, for each system for which you want to disable z/OSMF autostart, ensure that the `AUTOSTART(CONNECT)` and `AUTOSTART_GROUP('NONE')` settings are in effect.
- In your IZU= specifications, verify that the IZU= parameter identifies the suffixes of the IZUPRMxx members that contain the desired settings.

These actions must be taken if you want to disable the autostarting of z/OSMF servers. Otherwise, the default behavior for each system is to attempt to start the z/OSMF server automatically during IPL.

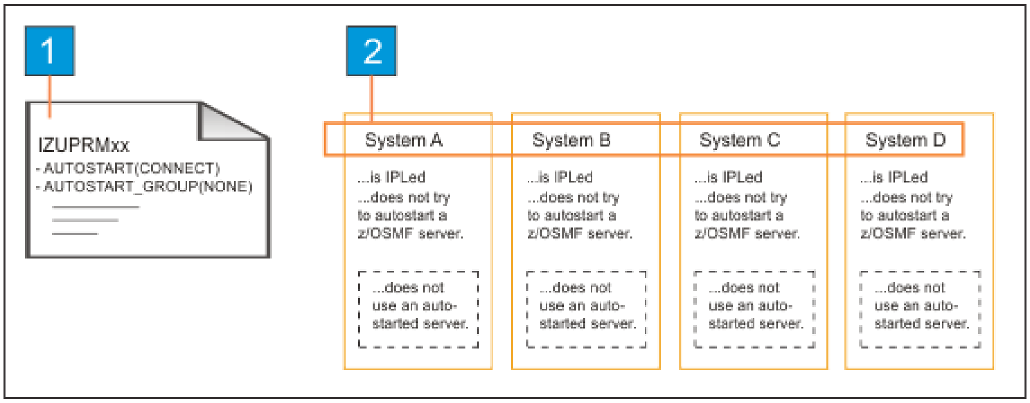


Figure 48. Scenario 4: No z/OSMF servers are started automatically.

In Figure 48 on page 161:

1. Each system uses the following values for autostart:

   ```
   AUTOSTART(CONNECT)
   AUTOSTART_GROUP(NONE)
   ```

   With these values set for all systems, no system attempts to autostart an z/OSMF server.
2. Systems A, B, C, and D complete the IPL process. No z/OSMF servers are autostarted in the sysplex.

- The JES2 Email Delivery Services (EDS) function in z/OS V2R3 requires a z/OSMF server to be active in an AUTOSTART group that JES2 can access. Specifically, the z/OSMF server must be started with SERVER='AUTOSTART' in the IZUSVR1 started procedure, and JES2 must be running on a system that is included in the AUTOSTART_GROUP specification. Otherwise, if this setup is not done, JES2 cannot send e-mail messages to users who submit jobs.

  The z/OSMF server does not necessarily have to be on the same system on which the JES2 EDS is used. However, you do need to ensure that the system from which you are using JES2 EDS is part of an z/OSMF AUTOSTART_GROUP in which there is an active server in that group. If so, JES2 automatically detects the presence of the z/OSMF server; you do not need to identify the location of the z/OSMF server to JES2.

  For information about configuring JES2 EDS, see the topic JES2 Email Delivery Services in *z/OS JES2 Initialization and Tuning Guide*.
- You can start the z/OSMF server manually on any system by using the **START** operator command with the name of the z/OSMF started procedure. By default, the procedure is IZUSVR1. For more information, see "Stopping and starting z/OSMF manually" on page 32.
- Changing an AUTOSTART_GROUP name requires an IPL. You cannot change this option with a stop and restart of the z/OSMF server.
- The z/OSMF autostart capability does not automatically restart a terminated server. If an autostarted server fails, you can resume z/OSMF operations by manually starting the server.
- Authorized programs can use the event notification facility (ENF) to determine whether the z/OSMF server is up or down. For more information, see "Detecting whether the z/OSMF server is available" on page 161.

Detecting whether the z/OSMF server is available

Your installation might choose to write a program that depends on the z/OSMF server being active.

A program can use one of the following methods to determine whether the z/OSMF server is up or down in the sysplex:

- An APF-authorized program can use the ENFREQ LISTEN service to specify a listen exit for ENF event code 83 that tells the program the z/OSMF server is up and running.

- An unauthorized program cannot use the ENFREQ LISTEN service. However, it can periodically check the global storage pointer, which is mapped by macro IZUGSP.

Using ENF event code 83 to listen for z/OSMF availability

An authorized program can use the ENFREQ LISTEN service to determine when the z/OSMF server is up and running. On the ENFREQ service, you specify the specific event for which you would like to listen (z/OSMF server availability) and the listener user exit routine that is to receive control after the specified event occurs. The listener user exit that is specified receives control when the z/OSMF server comes up and notifies your program.

To listen for ENF event code 83, you must specify the qualifying events on the QUAL parameter, which specifies a 4-byte field, a hexadecimal constant, or a register containing the address of a 4-byte field containing a bit-mapped qualifier that further defines the event. The qualifiers are mapped by mapping macro IZUENF83.

To use `QMASK=BYTE1` to listen for server up and down events, the QUAL values are:

X'80'
z/OSMF server is available.

X'00'
z/OSMF server has ended and is not available.

To use `QMASK=ALL`, to listen for server up and down events, the QUAL values are:

X'80000000'
z/OSMF server is available.

X'00000000'
z/OSMF server has ended and is not available.

When your program no longer needs to know whether the z/OSMF server is up, it can issue the ENFREQ REQUEST=DELETE request to delete the listen request.

For coded examples that show how to query the status of the z/OSMF server, see Appendix D, “ENF listener code examples ,” on page 319.

For more information about ENFREQ and listener exits, see:

- *z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG*
- Listening for system events in *z/OS MVS Programming: Authorized Assembler Services Guide*.

Chapter 9. Configuring a primary z/OSMF for communicating with secondary instances

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

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

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

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

These constructs are named, as follows:

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

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

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

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

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

Planning for secure communication between instances

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

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

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

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

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

Strategies for sharing CA certificates

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

If you have not yet created any secondary instances of z/OSMF, you might find it easier to create one CA certificate and use it to sign all of the server certificates in the primary and secondary instances. Using this approach, you export the CA certificate from the primary system and add it to each of the secondary system security databases. Then, you configure the additional instances of z/OSMF on each secondary system. Here, you should not run the IZUSEC job certificate commands on the secondary systems, as mentioned in "Each z/OSMF instance includes a server runtime and digital certificates" on page 163. Instead, use the certificate that you have from the primary system. As a result, the same CA certificate is used to sign the server certificate for each instance. This approach is shown in "Scenario 1: SSL connections using the same CA certificate" on page 165.

If you have already created one or more secondary instances of z/OSMF, and you want to enable them for communication with the primary, determine whether the secondary systems were configured to use identically-named CA certificates or uniquely-named CA certificates. If you created each of the secondary instances with unique SAF prefix values, each secondary instance uses a uniquely named CA certificate. To allow SSL connections in this case, you can make available the secondary system CA certificates on the primary system key ring (that is, export, add, and connect them). As a result, the primary system will trust the secondary system server certificates, and be able to establish SSL connections with those systems. This approach is shown in "Scenario 2: SSL connections using different CA certificates" on page 165.

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

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

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

Scenario 1: SSL connections using the same CA certificate

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

For example, in Figure 49 on page 165, both the primary z/OSMF and the secondary instances are identified by server certificates that were created using the same CA (Jupiter).

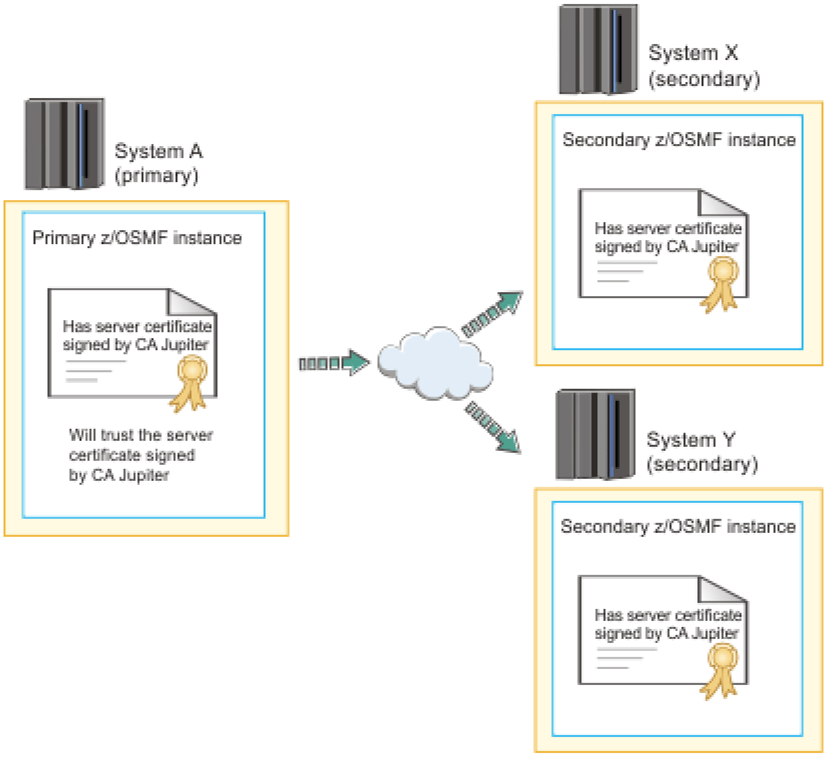


Figure 49. Trust relationship when server certificates are signed by the same CA certificate

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

Scenario 2: SSL connections using different CA certificates

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

For example, in Figure 50 on page 166, the primary z/OSMF:

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

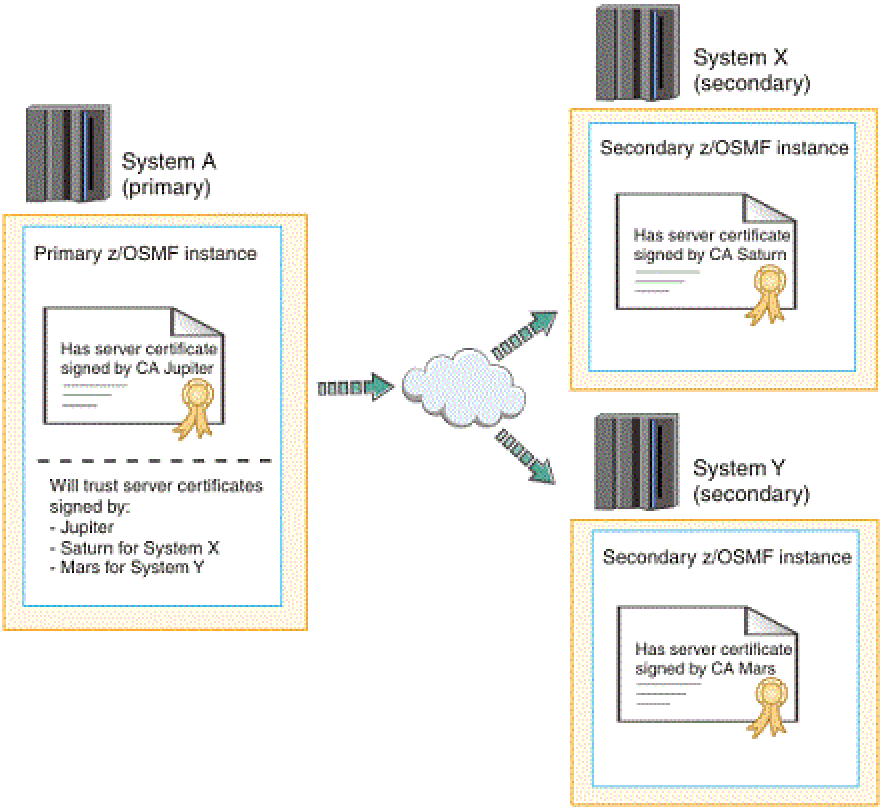

System X
(secondary)
Secondary z/OSMF instance
Has server certificate signed by CA Saturn
System A
(primary)
Primary z/OSMF instance
Has server certificate signed by CA Jupiter
Will trust server certificates signed by:
- Jupiter
- Saturn for System X
- Mars for System Y
System Y
(secondary)
Secondary z/OSMF instance
Has server certificate signed by CA Mars

Figure 50. Trust relationship when the server certificates are signed by different CA certificates

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

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

Enabling single sign-on between z/OSMF instances

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

The LTPA protocol uses an LTPA token to authenticate a user with the z/OSMF servers that are enabled for single sign-on. The LTPA token contains information about the user and is encrypted using a cryptographic key. The z/OSMF servers pass the LTPA token to other z/OSMF servers through cookies for web resources. If the receiving server uses the same key as the *primary z/OSMF server* -- the server that generated the key to be used for SSO, the receiving server decrypts the token to obtain the user information, verifies that the token has not expired, and confirms that the user ID exists in its user registry. After the receiving server validates the LTPA token, the server authenticates the user with that z/OSMF instance, and allows the user to access any resource to which the user is authorized.

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

- Before you enable the SSO, you must enable the z/OSMF Settings service on both the primary and secondary instances.
- Then, you must set up communications between the primary z/OSMF server and the secondary instances, as described in this chapter.
- The z/OSMF servers participating in the single sign-on environment must reside in the same LTPA domain as the primary z/OSMF server. The LTPA domain name is the parent portion of the fully qualified hostname of the z/OSMF servers. For example, if the fully-qualified hostname is *server.yourco.com*, the

LTPA domain is *yourco.com*. Due to browser restrictions, the hostname must be qualified with at least three levels (for example *server.yourco.com*). The domain name must have at least two levels (for example, *yourco.com*).

- The servers must share the same LTPA key. For z/OSMF, this is accomplished by invoking the **Enable Single Sign-on** action to synchronize the LTPA key on the primary and secondary z/OSMF servers. For instructions, see the z/OSMF online help.
- The user ID of the user must exist and be the same in all System Authorization Facility (SAF) user registries. It is recommended that you use the same user registry settings for all z/OSMF servers so that users and groups are the same, regardless of the server.
- The value specified for the SAF prefix during the z/OSMF configuration process must be the same for each z/OSMF server you want to enable for single sign-on. By default, the z/OSMF SAF prefix is IZUDFLT.

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

Chapter 10. Configuring z/OSMF for high availability

Normally, z/OSMF cannot be implemented in a high-availability cluster. However, for applications that use a critical subset of z/OSMF REST services, it is possible to configure a second z/OSMF server to ensure availability of those services. In this special configuration, one z/OSMF server is always available to provide the REST services to your applications.

The following z/OSMF REST services are supported for high availability:

- z/OS jobs REST interface services
- z/OS data set and file REST service "Retrieve the contents of a z/OS data set or member."

These services are described in IBM z/OS Management Facility Programming Guide.

To ensure that these services remain available to your applications, you can establish a pair of z/OSMF servers on different systems in your sysplex, and use a workload router to switch between them if an outage occurs. Figure 51 on page 169 shows how a z/OSMF workload can be distributed between multiple instances.

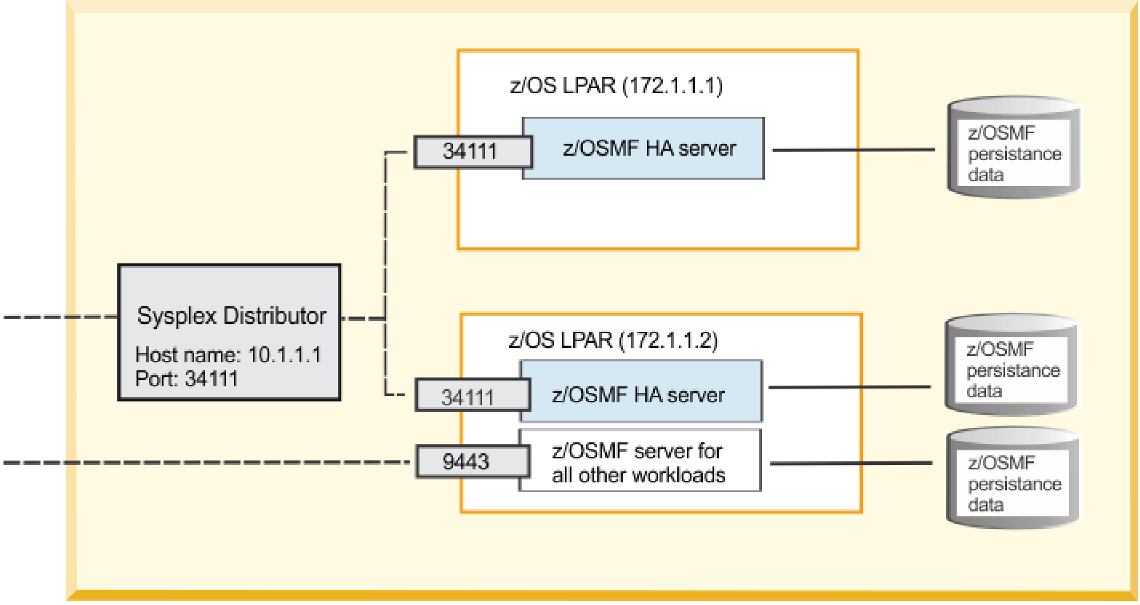


Figure 51. You can run multiple servers of z/OSMF, and use Sysplex Distributor to route requests to specific z/OSMF servers.

In this scenario, a Sysplex Distributor (or a similar workload router) is used to route application requests to a high availability (HA) server on a particular LPAR. If the HA server at system IP address 172.1.1.1 becomes unavailable, the Sysplex Distributor can redirect REST requests to the HA server at system IP address 172.1.1.2. Each HA server maintains its own copy of the z/OSMF data file system, which contains persistence data. No persistence data is shared between the HA instances.

How to set up z/OSMF for high availability

Assume that two z/OS systems in a sysplex, SYS1 and SYS2, are updated, as follows:

1. Define an IP address for both systems:

   a. Add the following statement to the TCPIP profile for the SYS1 system:

   ```
   IPCONFIG DYNAMICXCF 172.1.1.1 255.255.255.0 3
   ```

   b. Add the following statement to the TCPIP profile for the SYS2 system:

   ```
   IPCONFIG DYNAMICXCF 172.1.1.2 255.255.255.0 3
   ```

2. Define a dynamic VIPA (DVIPA) for both SYS1 and SYS2:

   ```
   VIPADYNAMIC
   ...
   :
   :------------------------------------------------------------
   : Test HA for zOSMF
   :
    VIPADEFINE 255.255.255.0 10.1.1.1
    VIPADISTRIBUTE DEFINE DISTM HOTSTANDBY 10.1.1.1 PORT 34111
      DESTIP 172.1.1.1 PREFERRED
             172.1.1.2 BACKUP
   ENDVIPADYNAMIC
   ```

   In this example, the VIPADEFINE statement is used to define the DVIPA 10.1.1.1. The VIPADISTRIBUTE statement with PREFERRED and BACKUP settings is used to enable automatic dynamic VIPA takeover to occur, if needed. The system SYS1 is defined as the preferred system and the system SYS2 is defined as the backup system.

   These statements are added to the TCP profiles for both SYS1 and SYS2.

3. Register the DVIPA with one host name so that z/OSMF can be bound to that host name. Define the z/OSMF host name in your name server, for example 10.1.1.1.
4. In the active IZUPRMxx parmlib member for SYS1 and SYS2, define the z/OSMF host name and port, for example:

   ```
   HOSTNAME('zosmfha.yourcompany.com')
      HTTP_SSL_PORT(34111)
   ```

Now assume that both SYS1 and SYS2 are active. Each system has an active z/OSMF server with its own data directory (sometimes called the user directory). Both z/OSMF servers are bound to the DVIPA 10.1.1.1. With both z/OS systems active in the sysplex, the preferred z/OSMF server receives all new incoming requests. If the SYS1 system fails, new work requests for z/OSMF are routed to the server on SYS2. When SYS1 resumes normal operations, new work requests for z/OSMF are routed to SYS1 again. This behavior occurs because the IP parameter AUTOSWITCHBACK is in effect by default.

For more information about network configuration, see the following documents:

- z/OS Communications Server: IP Configuration Guide
- z/OS Communications Server: IP Configuration Reference.

Part 3. Post-configuration

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

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

- Chapter 11, “Linking z/OSMF tasks and external applications,” on page 173
- Chapter 12, “Configuring your system for asynchronous job notifications,” on page 175
- Chapter 13, “Adding links to z/OSMF,” on page 185
- Chapter 14, “Deleting incidents and diagnostic data,” on page 189
- Chapter 15, “Troubleshooting problems,” on page 193
- Chapter 16, “Configuration messages,” on page 225.

Chapter 11. Linking z/OSMF tasks and external applications

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

Key components

The key components of the Application Linking Manager task include the:

- **Event requestor.** z/OSMF task or external application that requests the launch of a specific function within another task or external application
- **Event.** Action requested by the event requestor. It includes the type of event and the event parameters.
- **Event type.** Object that connects an event requestor to an event handler. It identifies the handlers that can process an event and the possible parameters that can be supplied with an event.
- **Event handler.** z/OSMF task or external application that can process the event parameters and display the requested information.

Figure 52 on page 173 depicts the relationship of these components in the application linking process.

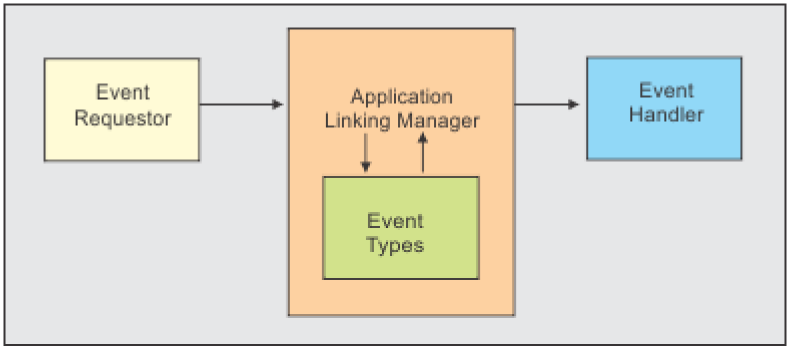


Figure 52. Key components in the application linking process

The process begins with a user action, such as clicking a link. In response to this action, the event requestor creates an event and sends it to the Application Linking Manager. The Application Linking Manager searches the set of known event types for the type identified by the event. If a match is found, the Application Linking Manager searches for event handlers that are registered for this event type. If only one handler is found, it is launched. Otherwise, the user is prompted to select the handler to launch. The Application Linking Manager provides the handler with the parameters that were supplied with the event. The event handler processes the parameters and displays the requested information.

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

Key features

To open the Application Linking Manager task, in the navigation area, expand the z/OSMF Administration category and select **Application Linking Manager**. The task provides a web-based, user interface that you can use to:

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

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

Programming interface

The Application Linking Manager task also provides an application programming interface (API) that you can use to complete the aforementioned actions. For more details about the API, see IBM z/OS Management Facility Programming Guide.

Chapter 12. Configuring your system for asynchronous job notifications

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

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

- Obtain the status of a job
- List the jobs for an owner, prefix, or job ID
- List the spool files for a job
- Retrieve the contents of a job spool file
- Submit a job to run on z/OS
- Cancel a job
- Change the job class
- Delete a job (cancel a job and purge its output).

The z/OS jobs REST interface services can be invoked by any HTTP client application, running on the z/OS local system or a remote system, either z/OS or non-z/OS. The z/OS jobs REST interface services are described in the document *IBM z/OS Management Facility Programming Guide* .

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

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

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

This topic is organized as follows:

- "Creating the CIM indication provider subscription" on page 175
- "Enabling secure job completion notifications for your programs" on page 181.

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

Creating the CIM indication provider subscription

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

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

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

Summary of the steps for creating a subscription:

- Select a user ID with sufficient access to CIM resources, such as the z/OSMF installer user ID; see "Selecting the appropriate user ID" on page 176
- Ensure that the user profile has the correct environment variable settings for entering CIM line commands; see "Customizing the administrator profile for running CIM commands" on page 177
- From this user ID, create the subscription to the CIM Jobs Indication Provider through a series of CIM line commands; see "Procedure for creating a subscription" on page 177.

Selecting the appropriate user ID

Choose an appropriate user ID for creating the subscription, one with sufficient access to CIM server resources to create CIM instances. Consider using the same user ID that you used earlier to install z/OSMF, as described in Chapter 3, "Setting up z/OSMF for the first time," on page 15. This user ID is likely to have the correct authorizations already, which it received during the configuration process. In effect, this user ID can serve as a CIM administrator, too. For more information, see "Ensure that the administrator role is authorized to the CIM server" on page 106.

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

To perform these authorizations manually, do the following:

- Grant the user CONTROL access to the CIMSERV profile in the WBEM class. This access can be granted through an explicit PERMIT command, or, if the CIM administrator group is already permitted with CONTROL access, you can connect the user to the group. If necessary, refresh the WBEM class.
- Ensure that the user ID under which the CIM server is running has SURROGAT access for the new user ID. If a generic BPX.SRV.** profile is already authorized in the SURROGAT class, no additional action is required. Otherwise, define a discrete profile for the user and authorize it. If necessary, refresh the SURROGAT class.
- Ensure that the user ID under which the CIM server is running has READ access to the following profiles in the SERVAUTH class:
  - CEA.*
  - CEA.CONNECT
  - CEA.SUBSCRIBE.*
  - CEA.SUBSCRIBE.ENF_078*

  Figure 53 on page 176 shows sample RACF commands that a security administrator can use to provide these CEA profile authorizations for the default CIM server user ID:

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

Figure 53. Sample RACF commands for creating CIM authorizations

If necessary, refresh the SERVAUTH class.

Customizing the administrator profile for running CIM commands

The CIM server commands are UNIX style programs running in a UNIX shell. To ensure that the z/OSMF administrator can use the CIM commands, verify that the administrator profile is properly set up, as described in “Customizing the administrator role for running CIM commands” on page 106.

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

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

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

Procedure for creating a subscription

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

Before you begin

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

```
D A,CFZCIM
```

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

Check the command output for the CIM server started task. If the CIM server is not already started, follow the steps described in *z/OS Common Information Model User's Guide* to start it. It is recommended that you ensure that the CIM server is started automatically at IPL time. For information about customizing the CIM server startup, see *z/OS Common Information Model User's Guide* .

Determine whether the CIM jobs indication provider subscription already exists. To view the existing subscriptions for your system, enter the following command from the z/OS UNIX shell command line: **cimsub -ls -v -n root/PG_InterOp**

If the command output includes an entry like the one shown in Figure 54 on page 177, the subscription for asynchronous job notification is already in place.

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

Figure 54. Subscription values for asynchronous job notification

In Figure 54 on page 177, <Name> is the name that was specified when the handler instance was created. If the subscription was created using the examples in this topic, for example, <NAME> would be `IZU_Job_Completed_Handler`.

If the command output is only a partial match with Figure 54 on page 177, observe the following considerations:

- If the handler value is correct, but the query value is not, a subscription was created using a filter other than the value that should be used with the listener destination. You can proceed with creating another subscription with the correct filter, but be aware that multiple notifications for the same completed job might result.

- If both the handler and query values are correct, but the SubscriptionState value is set to disabled, you can enter the following command to enable the subscription: **`cimsub -e`**

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

About this task

A subscription requires the creation of three CIM instances:

- Filter instance
- Handler instance
- Subscription instance.

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

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

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

Procedure

1. **Obtain the system name.**

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

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

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

   ```
   Command:

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

   echo $SYSTEMNAME

   Result:

   MY.TEST.SYSTEM.COM
   ```

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

2. **Create a filter instance.**

   To create the filter instance, enter the following command from the z/OS UNIX shell command line:

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

   where the value for *$SYSTEMNAME* is the value that was returned in Step "1" on page 178.

The results should look like the following example:

```
Command:

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

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

echo $FILTER_REFERENCE

Result:

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

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

3. **Create a handler instance.**

   To create the handler instance, enter the following command from the z/OS UNIX shell command line:

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

   where the value for *$SYSTEMNAME* is the value that was returned in Step "1" on page 178.

   The results should look like the following example:

```
Command:

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

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

echo $HANDLER_REFERENCE

Result:

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

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

4. **Create the subscription instance.**

   This step uses the filter and handler references that you collected in the previous steps.

   To create and enable a subscription instance, enter the following command from the z/OS UNIX shell command line:

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

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

   The results should look like the following example:

```
Command:

<filter and handler commands omitted for this example>

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

echo $SUBSCRIPTION

Result:

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

What to do next

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

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

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

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

- To remove the subscription only:

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

- To remove the handler only:

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

- To remove the filter only:

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

Enabling secure job completion notifications for your programs

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

Configuring the CIM server for SSL connections

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

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

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

Consider the following:

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

The remainder of this topic describes the steps needed to set up secure SSL connections for your job completion notifications. The instructions that follow cover both BASIC AUTH and CLIENT-CERT forms of SSL security setup. In the latter case, the key requirement is to export certificates and to enable the sharing of the certificates between the CIM server and the user-supplied servlet to which the notifications are being sent.

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

Enabling BASIC AUTH connections for your servlet

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

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

Follow these steps:

1. Create a SAF keyring to be used by TCP/IP for the CIM server outbound SSL connections.
2. Add the signer certificate that is used by the servlet for receiving secure job completion notifications. That is, add the signer certificate of the target server's SSL digital certificate to the SAF keyring that is identified for use by CIM in the Policy Agent TLS policy definition. For example, the default configuration for z/OSMF uses a signer certificate labelled zOSMFCA. Thus, you must add the

zOSMFCA certificate (or an alternative, if you used a non-default certificate) to the CIM server keyring that is identified in the Policy Agent TLS policy.

3. Configure the Communication Server Policy Agent. Consider using the z/OSMF Network Configuration Assistant task to perform this step. For the TLS policy, do the following:
   a. Create the `/etc/pagent.conf` file, as described in *z/OS Common Information Model User's Guide* . For more information, see the Communication Server Configuration Guide and Reference publications.
   b. Create the `/etc/tlsPolicy` file, following the instructions in *z/OS Common Information Model User's Guide* for securing CIM indications. Use the name of the SAF keyring created in Step 1.
   c. Create the `/etc/stackPagent` file, specifying the job name that is used by TCP/IP.
   d. Add the `TCPCONFIG TTLS` statement to the TCPIP PROFILE.
4. Restart TCP/IP and wait for the following message to be displayed on the system console:

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

5. Start the policy agent (PAGENT). On successful start-up, messages similar to the following are written to the console. If you are not using hardware cryptography, you can ignore the last message regarding ICSF:

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

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

Enabling CLIENT CERT connections for your servlet

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

Follow these steps:

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

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

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

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

2. Configure the Communication Server Policy Agent to send CIM indications over SSL per the instructions in the CIM Users Guide. This includes the step of adding TCPCONFIG TTLS to the TCPIP PROFILE to enable AT-TLS in the TCP/IP stack. Doing so causes TCP/IP to pause initialization until the Policy Agent has been started.

3. Add the signer certificate used by the servlet for receiving secure job completion notifications.
4. Configure the Communication Server Policy Agent. Consider using the Network Configuration Assistant task to perform this step. In the policy, specify the following:

   a. Create the /etc/pagent.conf file, as described in the CIM User's Guide. You will probably also need to refer to the Communication Server Configuration Guide and Reference manuals.

   b. Create the /etc/tlsPolicy file, following the instructions in the CIM User's Guide for securing CIM indications. Use the name of the SAF keyring created in Step 1.

   c. Create the /etc/stackPagent file, specifying the jobname used by TCP/IP

   d. Add the following statement to the TCPIP PROFILE: `TCPCONFIG TTLS`
5. Restart TCP/IP and wait for the following message to be displayed on the system console:

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

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

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

Coding considerations for your servlet

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

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

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

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

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

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

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

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

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

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

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

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

Considerations for receiving job notifications

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

Do the following:

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

Chapter 13. Adding links to z/OSMF

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

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

Steps for adding a link to z/OSMF

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

```
<product_dir>/samples/sampleLink.properties
```

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

To add a link to the z/OSMF navigation area, follow these steps:

1. **Make a copy of the sample link properties file.** Copy the sample link properties file to a read/write directory.
2. **Edit the new link properties file with your text.** As shown in Figure 55 on page 185, the link properties file contains the following input fields for a link:

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

Figure 55. Content of the link properties file

In your link properties file, define the link using these input fields:

LinkName

Specify a name for the link, as it should be displayed in the z/OSMF navigation area. Specify a value of up to 30 characters, including alphanumeric characters (A-Z a-z 0-9), blanks, mathematical symbols (+ - = | ~ ( ) { } \), punctuation marks (? , . ! ; : ' " / [ ]), and the following special characters: %, $, #, @, ^, *, and _. Any leading or trailing white space is ignored.

Specify your input in the form of the ASCII, EBCDIC or Unicode character sets. To use Japanese language characters, enter the characters in Unicode. Each Unicode character (\u*xxxx*) is treated as one character.

The name you select must be unique among the existing links defined in z/OSMF. It is recommended that you choose a name that will be easily understood by users. Avoid names that might be confused with other links or tasks in z/OSMF.

LinkURL

Specify the location for the link (a URL), which is a valid Internet or intranet address, for example:

```
http://www.ibm.com
```

The URL can be up to 4000 characters, including alphanumeric characters (A-Z a-z 0-9), blanks, mathematical symbols (+ - = | ~ ( ) { } \), punctuation marks (? , . ! ; : ' " / [ ]), and the following special characters: %, $, #, @, ^, *, and _. Any leading or trailing white space is ignored.

z/OSMF performs limited syntax checking of the specified URL. Ensure that the link location is a syntactically correct URL. Generally, a URL includes a protocol (such as `http://`), a host name (www.*hostname*.com), and, often, a resource such as a directory path and file.

To link to a file on the host system, ensure that the host name is included in the URL, for example:

```
file://localhost/C:/tmp/test.html
```

Note that the ability to connect to a particular location can depend on the user's browser settings.

LinkNavigationCategory

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

To indicate the placement of the link, specify one of the following values:

1

z/OSMF Administration.

2

Problem Determination.

3

Links.

4

Configuration.

5

Software.

7

z/OS Classic Interfaces.

9

Performance.

10

z/OSMF Settings.

11

No category. The link is placed outside of the categories, after the Welcome task.

Specify one value only. Any leading or trailing white space is ignored.

LinkAuthorizedRoles

Specify the z/OSMF roles for which users are authorized to use the link. You can limit access to users with one or more of the following roles:

- z/OSMF Guest
- z/OSMF Authenticated Guest
- z/OSMF User
- z/OS Security Administrator
- z/OSMF Administrator

Enter the role name exactly as depicted here. To specify multiple roles names, separate each name with a comma. Any leading or trailing white space is ignored.

If you specify a role incorrectly, the role is ignored. If you specify no roles at all, or omit this property, the link is added to the table displayed in the Links task with no roles assigned to it.

LinkSafSuffix

Specify the system authorization facility (SAF) resource name suffix to be used for managing user authorizations to the link. To create a unique resource name for the link, z/OSMF appends this value to the z/OSMF SAF profile prefix (by default, IZUDFLT), followed by ZOSMF.LINK. Specify a unique resource name suffix, for example: `IZUDFLT.ZOSMF.LINK.`**`mylink`**

You can specify a suffix of up to 220 alphanumeric characters (A-Z a-z 0-9) and the following special characters: underscore (_), dash (-), period (.). The use of a period in a resource name is treated as a qualifier. As such, the first character after a period must be A-Z or a-z.

You must provide a unique SAF resource name suffix for each link. z/OSMF uses the resource name for locating and identifying links.

LinkLaunchWorkArea

Specify how the link is to open in the user's z/OSMF session, as follows:

- To have the link open in the user's session as a separate window or tab, set this value to FALSE. The link will open in the user's browser as a new window or tab, based on the user's browser settings.
- To have the link open as a tab in the z/OSMF work area, like a z/OSMF task, set this value to TRUE.

Any other value is ignored and FALSE is used by default.

If you choose to have the link open as z/OSMF tab, verify that the link will work as intended in the z/OSMF work area. You might find that some links display better in a separate browser window or tab. Also, some external web sites might cause the user's browser window to be re-sized or even redirect the browser to a new destination, rather than opening in the z/OSMF work area. Therefore, it is strongly recommended that you verify the general usage of the link in the z/OSMF work area before directing users to use the link.

Figure 56 on page 187 shows an example of a completed link definition.

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

Figure 56. Example of a link definition

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

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

Managing security for links in z/OSMF

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

Managing a link in z/OSMF involves the following steps:

- Defining the link to z/OSMF through the Links task
- Controlling access to the link through the ZMFAPLA resource class profile.

The z/OSMF configuration process defines a generic resource profile for links and permits groups to it. Specifically, links in z/OSMF are protected under the generic resource profile: `<SAF-prefix>.ZOSMF.LINK.**` where *<SAF-prefix>* is the SAF profile prefix that was defined for your configuration (IZUDFLT by default). z/OSMF permits the groups for z/OSMF users (IZUUSER) and z/OSMF administrators (IZUADMIN) to this profile. As a result, these users will be able to see all of the links in the navigation tree. z/OSMF does not, by default, permit the z/OS security administrator role to the ZOSMF.LINK** profile.

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

Defining a link as a protected resource

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

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

As an example, Figure 57 on page 188 shows the RACF commands that a security administrator can use to define a discrete profile for a new link (the z/OS Basics Information Center web site) and permit a group (IZUUSER) to that link.

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

Figure 57. Example: Defining a link resource name and permitting a group to it

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

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

Chapter 14. Deleting incidents and diagnostic data

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

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

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

Overview

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

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

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

Before invoking the utility

Before invoking the utility, complete the following steps:

1. Ensure that the common event adapter (CEA) component and the System REXX (SYSREXX) component are active on your z/OS system. For instructions, see "Ensure that common event adapter (CEA) is configured and active" on page 124 and "Ensuring that System REXX is set up and active" on page 126.
2. Ensure that the user ID you are using to invoke the utility is authorized to access SAF resource CEA.CEAPDWB.CEADELETEINCIDENT, which is defined in the SERVAUTH class.
3. Ensure that the PATH environment variable is set to the directory in which the utility is installed. By default, the utility is installed in the `/bin` directory.
4. Ensure that the NLSPATH environment variable contains `/usr/lib/nls/msg/%L/%N`, which is, by default, the directory in which the CEA message catalog, called *ceamsg.cat*, is installed.

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

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

Invoking the utility

The **ceatool** command-line interface must be invoked from the z/OS UNIX System Services shell or a BPXBATCH environment. Figure 58 on page 190 shows the format of the **ceatool** command, which invokes the utility.

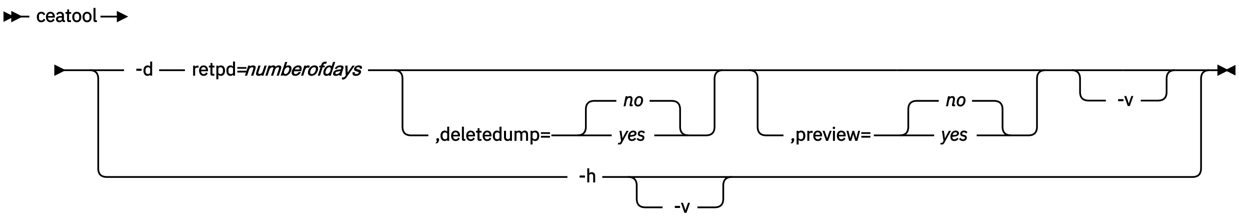


Figure 58. Format of the ***ceatool*** *command*

Where:

-d

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

retpd=*numberofdays*

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

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

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

deletedump

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

yes

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

no

All diagnostic data associated with an incident, except the SVC dumps, will be deleted when the incident is deleted. This is the default.

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

preview

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

yes

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

no

Preview mode is disabled. In this case, the incidents that match the filter criteria will be deleted. This is the default.

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

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

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

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

Examples

Table 27 on page 191 provides sample commands to invoke the **`ceatool`** utility and describes the expected result for each command.

Table 27. Sample ***`ceatool`*** *commands*

Sample Command	Results
	Deletes inactive incidents and. the corresponding diagnostic data, excluding SVC dumps, that are older than seven days
	Deletes inactive incidents and. the corresponding diagnostic data, including SVC dumps, that are older than seven days
	Deletes inactive incidents and. Because verbose mode is the corresponding diagnosticrequested, additional data, including SVC dumps,diagnostic messages are that are older than seven daysdisplayed during processing.
	Deletes all inactive incidents. and the corresponding diagnostic data, excluding SVC dumps
	Displays the number of. The incidents that satisfy the inactive incidents that arefilter criteria are not deleted. older than seven days

Verifying that the incidents were deleted

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

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

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

Chapter 15. Troubleshooting problems

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

This chapter is organized into topics, as follows:

- "Resources for troubleshooting" on page 193
- "Tools and techniques for troubleshooting" on page 194
- "Common problems and scenarios" on page 206.

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 28 on page 193 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 28. 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 194.	N/A
z/OSMF core functions and system management tasks	• The About page • z/OSMF log files and tracing.	• "Finding information about z/OSMF" on page 201 • "z/OSMF log files" on page 202. • "Problems when using Network Configuration Assistant" on page 218.	Messages encountered while configuring z/OSMF; see Chapter 16, "Configuration messages," on page 225. z/OSMF messages. For assistance, click on the message help link. For Network Configuration Assistant, messages and pop-ups are supplied with the task.
z/OSMF server	z/OSMF log files and tracing.	"IZUPRMxx reference information" on page 36.	• Chapter 16, "Configuration messages," on page 225 • z/OSMF messages. For assistance, click on the message help link.
WebSphere Liberty profile	Troubleshooting information is provided in the WebSphere Application Server for z/OS information center.	See the topics at: http://www.ibm.com/software/webservers/appserv/was/library/v85/was-zos/index.html.	Messages prefixed by `CW`.
CIM server and CIM providers	• CIM server logging • CIM server trace • CIM provider trace.	These options are defined in the CIM server configuration properties and set through the **`cimconfig`** command; see *z/OS Common Information Model User's Guide* .	*z/OS Common Information Model User's Guide* .

Table 28. Summary of tools and information for troubleshooting problems with z/OSMF (continued)

Component or task	Tools to assist with troubleshooting	Where described	Associated messages
Common event adapter (CEA)	System commands: • MODIFY CEA • MODIFY AXR • TRACE CT.	*z/OS MVS System Commands*	*z/OS MVS System Messages* for information about: • WTO messages • CTRACE • Reason codes.

Tools and techniques for troubleshooting

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

Verifying your workstation with the environment checker

To work with z/OSMF, your web browser and workstation require a number of settings for proper functioning. z/OSMF includes an environment checker tool to help you verify these settings. The environment checker tool inspects your web browser and workstation operating system for compliance with z/OSMF requirements and recommended settings.

Before you run the tool

Check to ensure that your workstation is set up correctly for z/OSMF. See "Preparing your workstation for z/OSMF" on page 16.

Your workstation requires a compatible operating system and web browser. For more information, see "Software prerequisites for z/OSMF" on page 6.

Ensure that your browser is enabled for JavaScript. For instructions, see Table 30 on page 196 or Table 31 on page 198.

Running the tool

To run the tool, do the following:

1. Open a web browser to the environment checker tool:

   ```
   https://hostname:port/zosmf/IzuUICommon/environment.jsp
   ```

   Where:

   - *hostname* is the hostname or IP address of the system on which z/OSMF is installed
   - *port* is the secure application port.

   To find the hostname and port, see the link for z/OSMF in message IZUG349I. This message was written to the z/OSMF server job log, as described in "Step 4: Verify server initialization" on page 29.
2. Follow the instructions for your particular browser in the online help for the tool.

Understanding the results of the tool

Table 29 on page 194 describes the layout of the environment checker report.

Table 29. Columns in the environment checker tool results page

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

Table 29. Columns in the environment checker tool results page (continued)

Column	Description
Settings as of *date-time*	Findings from the most recent invocation of the tool. This column indicates potential problems with your browser. In the column heading, the date and time (*date-time*) is represented in ISO 8601 format, a standard provided by the International Organization for Standardization (ISO). In this format: • Calendar date is represented in year-month-day format (*yyyy-mm-dd*). • Time of day (*T*) is based on the 24-hour clock: *hh:mm:ss:mmm*. • *Z* indicates zero offset from coordinated universal time (UTC). In the report, the status of each setting is indicated, as follows: **Items that are marked with a critical icon X** Setting is not correct for z/OSMF. You must fix this problem before you continue with z/OSMF. **Items that are marked with a warning symbol !** Setting is not optimal for z/OSMF. It is recommended that you update the setting before you continue 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 you update a setting, use the browser reload button to run the environment checker again. Repeat this process until you resolve all of the errors and warnings.

If you are using the Internet Explorer browser:

- When you are working with WLM service definitions, ensure that automatic prompting for file downloads is enabled for the web link (a URL) to the active z/OSMF instance. See "Enabling automatic prompting for file downloads" on page 201.
- When you are working with Resource Monitoring task, users who plan to export the data that is collected in a dashboard to a CSV file should ensure that automatic prompting for file downloads is enabled. See "Enabling automatic prompting for file downloads" on page 201.
- Do not use the browser with the Compatibility View feature enabled, which allows web sites to appear as they do when viewed with Internet Explorer Version 7. Some z/OSMF functions might not work correctly because Internet Explorer 7 is not supported.

If you are using the Microsoft Edge browser on a Windows 10 system:

- When you are working with the Sysplex Management task or the System Status task, you might experience problems with the zoom function on graphical views. If so, upgrade the browser to a later version and try again. If the problem persists, use another tested browser.

For a list of the supported web browsers, see "Software prerequisites for z/OSMF" on page 6.

Recommended settings for the Mozilla Firefox browser

Table 30 on page 196 shows the recommended settings for the Mozilla Firefox browser.

Table 30. Recommended settings for Firefox

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

Table 30. 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 30. 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 31 on page 198 shows the recommended settings for the Microsoft Windows Internet Explorer browser. If you are using the Workload Management task, see also "Enabling automatic prompting for file downloads" on page 201.

Table 31. 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 31. 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 31. 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 31. Recommended settings for Internet Explorer (continued)

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

Enabling automatic prompting for file downloads

If you are using Microsoft Internet Explorer to work with WLM service definitions or RMF exported data, ensure that automatic prompting for file downloads is enabled for the web link (a URL) to the active z/OSMF instance. If the feature is disabled, when you attempt to display the *File Download* dialog box, the browser window refreshes and all of your selections and unsaved changes are discarded. To enable automatic prompting for file downloads, use one of the procedures described in this section, depending on the version of the Internet Explorer browser.

Microsoft Internet Explorer Version 11

Procedure

1. From the *Tools* menu, click **Internet Options** > **Security** tab.
2. Under *Select a zone*, click **Local intranet**.
3. Click **Sites**.
4. Click **Advanced**.
5. If the URL to the active z/OSMF instance is listed in the Add this web site to the zone field, click **Add**. Otherwise, enter the URL, and then click **Add**.
6. Click **Close**.
7. Click **OK**.
8. Click **OK**.

Finding information about z/OSMF

z/OSMF includes an **About** page to display the product version details that can be useful to IBM Support for diagnosing a problem.

About this task

To access the About page for z/OSMF, do the following:

Procedure

1. Select the Welcome task in the navigation area. The **Welcome** page opens.
2. Click the **About** link in the **Welcome** page.
   Details about the product build level, and the SMP/E-installed plug-ins and their versions (FMIDs), are displayed in a new browser window. If no plug-ins are installed, this area is empty.

Types of messages in z/OSMF

z/OSMF records messages from the user interface, from tasks performed by z/OSMF users, and from programs that are running on the z/OS host system. Because of the various layers of functions involved in typical z/OSMF operations, locating a particular message might require you to check more than one location.

z/OSMF collects the following types of messages:

Operator console messages
z/OSMF writes some messages to the operator console with time stamps that are assigned by the console. These messages are also recorded in the z/OSMF server job log, with time stamps that are assigned by the JES subsystem. For example:

```
16.52.31 STC00049  IZUG400I: The z/OSMF Web application services are initialized.
```

Runtime data messages
z/OSMF collects its runtime data (log and trace messages) in the server logs directory. This directory contains one or more log files that are named IZUG*n*.log, where *n* is a numeral 0 - 9.

In a runtime log file, a message might appear like this:

```
[tx000000000000008:*izubootstrap*]
   2013-09-06T20:52:31.937Z|0000001F|com.ibm.zoszmf.navigation.listener.Boo
   tstrap|contextInitialized(ServletContextEvent)
   INFO:IZUG400I: The z/OSMF Web application services are initialized.
```

For more information about how runtime log files are processed, see "z/OSMF log files" on page 202.

Messages from z/OSMF tasks
These messages are written to SYSOUT and the job log. In addition, some z/OSMF tasks might write messages to the standard UNIX streams (STDOUT and STDERR) or to z/OS data sets. Typically, messages that are written to the UNIX streams do not have time stamps, for example:

```
.AUDIT   . CWWKZ0001I: Application IzuManagementFacilityWorkload....
```

Regardless of the message origin, z/OSMF records all of its messages and traces in the z/OSMF server logs directory. By default, the server logs directory is located in

```
<USER_DIR>/data/logs/zosmfServer/logs
```

where the default for *<USER_DIR>* is `/global/zosmf` (with APAR PI92211) or `/var/zosmf` (without APAR PI92211).

z/OSMF log files

During normal operations, z/OSMF runtime data is created on the server (*server side*) or sent to the server by the client (*client side*). Both types of data are written to the z/OSMF log files.

Viewing the z/OSMF logs

The z/OSMF and WebSphere Liberty logs are available in the z/OSMF `logs` directory:

```
<USER_DIR>/data/logs/zosmfServer/logs
```

where the default for *<USER_DIR>* is `/global/zosmf` (with APAR PI92211) or `/var/zosmf` (without APAR PI92211).

The z/OSMF runtime log files are written in English only, and are tagged as ASCII, using the ISO8859-1 code page. You can view the log files in ASCII format through ISPF option 3.17, using the VA action (View an ASCII file). Other viewing options, such as OBROWSE, or tools such as vi, emacs, or grep, might require that you first convert the files to EBCDIC. To have ASCII files converted to EBCDIC automatically before browsing, set the z/OS UNIX System Services environment variable _BPXK_AUTOCVT to "ON".

To access the logs, you require a user ID with z/OSMF administrator authority (that is, a user ID defined to the z/OSMF administrator group). Changing the level of logging and activating trace are performed through the IZUPRMxx parmlib member. For information, see "IZUPRMxx reference information" on page 36.

z/OSMF diagnostic data is stored in the following log files. By checking these log files, you can locate any of the messages that are written by z/OSMF.

IZUGx.log

Contains the runtime messages, including the standard output and standard error streams from the JVM process.

The IZUGx.log files are contained in the following directory:

```
<USER_DIR>/data/logs/zosmfServer/logs
```

z/OSMF names the log files IZUG*n*.log, where *n* is a numeral in the range 0 - 9. z/OSMF creates log files in a "cascading" manner. The most current log file is always named `IZUG0.log`. When this log file reaches its predefined limit, z/OSMF saves it as `IZUG1.log` and begins writing to a new `IZUG0.log` file. When the `IZUG0.log` file is again full, z/OSMF saves it as `IZUG1.log` after it renames the existing `IZUG1.log` file to `IZUG2.log`. z/OSMF continues this process, saving each log file under the next available name, up to a maximum of ten log files. Thereafter, z/OSMF discards the oldest log file (`IZUG9.log`) whenever a new log file is to be created.

If the current IZUG0.log file becomes unavailable, z/OSMF writes its runtime data to the z/OSMF server logs directory (trace.log and messages.log) until the problem is resolved.

For examples of z/OSMF runtime log data, and a description of the log file format, see "Examples of working with z/OSMF runtime logs" on page 204.

FFDC log files

Contains the WebSphere Liberty first failure data capture (FFDC) log files. FFDC log files include the exception stack and optional additional data that is recorded when an unexpected exception occurs.

The FFDC log files are contained in the following directory:

```
<USER_DIR>/data/logs/zosmfServer/logs/ffdc
```

messages.log

Contains the WebSphere Liberty startup and runtime messages. Messages that are written to this file begin with `CWW` and include information such as the message time stamp and the ID of the thread that wrote the message. The messages.log does not contain messages that are written by the JVM process.

For example:

```
[9/6/13 20:52:21:569 GMT] 0000001f
   com.ibm.ws.app.manager.internal.statemachine.StartAction A CWWKZ0001I:
   Application IzuManagementFacilityWorkloadManagement started in 4.121
   seconds.
```

The messages log is written to the following location:

```
<USER_DIR>/data/logs/zosmfServer/logs/messages.log
```

trace.log

Contains the same entries as found in messages.log. In addition, this file contains trace entries when additional tracing is enabled. This file does not contain messages that are written by the JVM process.

WebSphere Liberty defines this file as stderr. For example, JSSE tracing enabled with the z/OSMF advanced setting `–Djavax.net.debug=all`.

The trace log is written to the following location:

```
<USER_DIR>/data/logs/zosmfServer/logs/trace.log
```

Periodic maintenance of log files is recommended

z/OSMF does not perform any housecleaning of its directories. It is recommended that you periodically review the following directories and remove files that are no longer needed:

***<USER_DIR>*/data/logs/zosmfServer**
: Contains the JVM-generated diagnostic files for Java exceptions, such as Java core, heap dump, snap.trc, and jit dump files

***<USER_DIR>*/configuration**
: Contains the `backup_configuration` files.

***<USER_DIR>*/data/logs/zosmfServer/logs/ffdc**
: Might contain many log entries due to log rotation; additional file names with time stamps might be generated. The file names in this directory are created with a date and time stamp. For example: `exception_summary_18.07.06_19.33.00.0.log`

Managing log lock files

When z/OSMF initializes, the log file handler creates a file that is named IZUG0.log.lck. This file represents a "lock" on the log data. Usually, lock files are cleaned up automatically as part of application shutdown. If the z/OSMF server ends abnormally, however, the lock files might remain. If so, the log file handler appends numbers to the normal lock file name to find a file that is free.

If the server ends abnormally, inspect the log directory and delete the lock files. If more locks and log files were created, you can sort the files in the directory by time stamp to determine which files are the most recent. Back up these files if you want to preserve them, then clear the logs directory to conserve space.

If client data cannot be written to the server

If a communication problem prevents the client's critical error log data from being written to the z/OSMF logs directory, the unlogged client data is displayed to the user in a separate browser window. This failover action allows for the client data to be retained until the communication with the z/OS system can be restored. In some situations, IBM Support might request this data for diagnostic purposes. If the browser window is closed, the client data is not retained.

Other log files in z/OSMF

Do not confuse the z/OSMF runtime log file with the job log files that are created during the configuration process. In contrast to runtime data, configuration log data is written to a file in the z/OSMF user file system. If a problem occurs with the configuration log file, the log data is written instead to the directory specified by the `/tmp` parmlib statement.

Examples of working with z/OSMF runtime logs

For your reference, this topic describes the attributes of the z/OSMF log files that are created at runtime.

Examining log data that originates from the server

Figure 59 on page 205 shows portions of an example of z/OSMF server side log data.

```
2009-04-29T18:38:51.285Z|00000012|com.ibm.zoszmf.util.eis.cim.ccp.CimClientPool|getWBEMClient(Endpoint,
String,
Set<Locale>) INFO:IZUG911I: Connection to "http://null:5988" cannot be established, or was lost and
cannot be
re-established using protocol "CIM" .
com.ibm.zoszmf.util.eis.EisConnectionException: IZUG911I: Connection to "http://null:5988" cannot be
established,
or was lost and cannot be re-established using protocol "CIM" .
   com.ibm.zoszmf.util.eis.EisException.getEisException(EisException.java:145)
   com.ibm.zoszmf.util.eis.EisException.diagnoseAndThrow(EisException.java:221)
   com.ibm.zoszmf.util.eis.cim.ccp.CimClientPool.getWBEMClient(CimClientPool.java:279)

                                        o
                                        o
                                        o

+-> javax.wbem.WBEMException: JNI Exception type CannotConnectException:
   Cannot connect to local CIM server. Connection failed.
   org.sblim.cimclient.internal.jni.pegasus.CimReturnBuffer.getWBEMException(CimReturnBuffer.java:1244)
   org.sblim.cimclient.internal.jni.pegasus.NativeCimClient.verifyResult(NativeCimClient.java:1834)

                      o
                                        o
                                        o

[tx0000000000000017:pegadm@IBM-FF0E8EC4FCB.xxx.yyy.com (GET) /zosmf/pdw/PdwServiceServlet/
Incidents?filters=IncidentTime(FROM1240704000000)&dojo.preventCache=1241030163470]
```

Figure 59. Portion of z/OSMF server side log data

As shown in Figure 59 on page 205, each log record begins with a line divided by 'pipe' (|) characters into the following components:

- Timestamp in ISO8601 format, set to UTC timezone. Example: `2009-03-10T18:04:08.051Z`
- Thread ID as an 8 digit hex number. Example: `00000010`
- Class name. Example: `com.ibm.zoszmf.util.eis.cim.ccp.CimClientPool`
- Method name. Example: `getClient(Endpoint, String)`.

The next line of a log record contains the logging level, followed by a colon, followed by the message text. Messages logged at level INFO, WARNING, or SEVERE begin with an eight character message ID at the start of the message text. Message IDs that begin with "IZU" are part of the z/OSMF product.

If the log record includes an exception, the exception is logged next. The exception class is logged, followed by a colon, followed by the message text of the exception. The lines following this make up the traceback information embedded in the exception, which is useful first-failure data capture. If the exception has attached causes, each cause is also logged with "+->" indicating the start of an attached cause.

The final line in every log record is contained in brackets. If the log record is written during a specific user's context, information about that context is logged, as follows:

- "Transaction ID". An internal counter value that applies to all actions between a specific set and clear of a context. This identifier begins with `"tx"`, followed by a sixteen digit hex ID, and ends with a colon ':'.
- Remote user name (null for a guest user). This value is followed by an 'at' symbol (@).
- Remote host name. This value is followed by a space.
- Servlet "verb" is next, contained in parenthesis. Examples include GET and POST.
- URL of the request and query string, ending with the closing bracket ']'.

If the log record is created during an initialization sequence, the transaction ID is printed and the user name is listed as `"*bootstrap*"`. No other data are provided.

If the log record is created with no known context, only "[tx:]" appears on the final line.

Viewing client side log data

Included with the server statistics in the z/OSMF logs are client side data, which are used to monitor the JavaScript activity of each user login session. Client side log data differs in format from server side log data, as shown in Figure 60 on page 206.

```
[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 60. Example of z/OSMF client side log data

Log records that originate from the client side are formatted using the same data as those that originate within the server. However, the "message text" itself is specially formatted to represent the state of the client when the message occurred. This is done to compensate for the fact that client side messages might not be immediately sent to the server.

The following fields are recorded on the client when the message occurs, and are formatted within the message text of a log record as such:

- Client timestamp in brackets [ ]
- Browser name and level
- ENTRY or RETURN, to indicate the beginning or the end of a routine
- Package name, such as AuthorizationServices
- Module name, such as util.ui.messages.Message.js
- Method name, such as _getMessageType()
- Detailed message.

Common problems and scenarios

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

Troubleshooting topics are included for the following problems and scenarios:

- “Problems during configuration” on page 207
- “Problems when accessing the user interface” on page 209
- “Problems when using Network Configuration Assistant” on page 218
- “Problems when using IBM zERT Network Analyzer” on page 219
- “Problems when using the Incident Log task” on page 221
- “Problems when using the ISPF task” on page 220
- “Problems when attempting to send data” on page 223.

Problems during configuration

This topic provides troubleshooting tips for resolving problems that are related to the configuration and setup of z/OSMF.

Troubleshooting topics are included for the following problems and scenarios:

- “z/OSMF server does not initialize or appears to hang” on page 207
- “IZUSEC job fails with an authorization failure for the issuer” on page 207
- “A z/OSMF script fails because no z/OS UNIX processes are available” on page 208
- “Initialization fails with messages IZUG401E and IZUG620E” on page 208
- “You receive message EDC5134I: Function not implemented” on page 209
- “RACDCERT or another RACF command abends during configuration” on page 209.

A problem in the configuration of z/OSMF might be indicated by error messages from the common event adapter (CEA) component of z/OS. For a description of configuration-related CEA reason codes, which might be useful in diagnosing problems in your z/OSMF setup, see Appendix C, “Common event adapter (CEA) reason codes,” on page 315.

z/OSMF server does not initialize or appears to hang

Symptom: On start-up, the z/OSMF server (IZUSVR1) does not fully initialize. The following message or a similar message is written to the server job log:

```
ERROR  CWWKZ0002E: An exception occurred while starting the application
IzuManagementFacilitySoftwareDeployment. The exception message was:
com.ibm.ws.container.service.state.StateChangeException: java.lang.IllegalStateException:
Unable to acquire TCCL store lock
```

Possible Cause: The thread context classloader (TCCL) store lock timeout threshold was exceeded. By default, this time limit is 5 seconds. In a resource constrained environment, this time limit can be exceeded.

Corrective Action: Increase the timeout threshold by specifying a larger value in an override file.

Follow these steps:

1. Create an override file in the z/OSMF data directory. By default, the data directory is `/global/zosmf`. For example:

   ```
   /global/zosmf/configuration/local_override.cfg
   ```

2. In the override file, add the following statement on one line:

   ```
   JVM_OPTIONS=-Dcom.ibm.ws.classloading.tcclLockWaitTimeMillis=300000
   ```

   This statement sets the timeout to 300,000 milliseconds (5 minutes).

3. To have this change take effect, restart the z/OSMF server.

You can experiment with this value by reducing it to find the minimum possible timeout for your environment. The z/OSMF server is not negatively affected if the value is set higher than necessary.

IZUSEC job fails with an authorization failure for the issuer

Symptom: The job IZUSEC fails with an authorization failure message for the z/OSMF issuer’s user ID.

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

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

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

A z/OSMF script fails because no z/OS UNIX processes are available

Symptom: A script fails with a message that indicates that no z/OS UNIX processes are available for the user ID that was used to run the script.

Possible Cause: The user ID exceeds the MAXPROCUSER setting for your system. MAXPROCUSER specifies the maximum number of z/OS UNIX processes that a single user can have active concurrently. Typically, an installation sets a system-wide limit through the MAXPROCUSER setting in the BPXPRMxx member of parmlib, and then sets higher limits for individual users and processes through PROCUSERMAX, a value in the OMVS segment. Though z/OSMF by itself does not add significantly to the number of z/OS UNIX processes for the user, the MAXPROCUSER setting can be reached when the user is also running a number of other processes on the system besides z/OSMF.

Corrective Action: Use the RACF ADDUSER or ALTUSER command (or an equivalent command for your external security manager) to specify a PROCUSERMAX value for the user ID that is higher than the MAXPROCUSER setting. Try adding 20 to the value that is specified through the MAXPROCUSER setting.

Suppose, for example, that your installation specified a MAXPROCUSER value of 80 in the BPXPRMxx member. Here, you would set the PROCUSERMAX value for this user ID to 100 to allow a greater number of processes for the user ID. For example:

```
ALTUSER USER-ID OMVS(PROCUSERMAX(100))
```

If the problem persists, repeat this process by increasing the PROCUSERMAX value by an extra 20, taking care not to exceed any limits that are appropriate for your installation; check with your security administrator.

Initialization fails with messages IZUG401E and IZUG620E

Symptom: During initialization, the z/OSMF server fails with the following error messages:

```
IZUG401E: Initialization has failed for the z/OSMF web application services.
IZUG620E: The required environment variable "IZU_DATA_DIR" is missing or blank.
```

Possible Cause: The TCP/IP resolver trace function is active on the system. This trace is used for debugging problems that are related to TCP/IP. The trace is enabled by including the TRACE RESOLVER statement in data set TCPIP.DATA.

When active, the resolver trace causes the z/OS UNIX command **hostname** to return diagnostic data with the host name. During z/OSMF initialization, the diagnostic data is erroneously supplied as input to the z/OSMF configuration file. The incorrect input data is indicated in message IZUG620E.

Corrective Action: Disable the TCP/IP resolver trace function on the z/OSMF system. If the trace is required, you can resume the trace after the z/OSMF server is initialized.

You can use the **MODIFY RESOLVER,REFRESH** command to change the TCPIP.DATA statements that are being used by the z/OSMF server. For more information about modifying statements in TCPIP.DATA, see z/OS Communications Server: IP System Administrator's Commands.

You receive message EDC5134I: Function not implemented

Symptom: You receive the following message and error code:

```
atoe_getcwd error: EDC5134I Function not implemented. (errno2=0x052C04DC)
```

Possible Cause: The error code indicates that the system root directory is not mounted. However, this message is also issued if the OMVS home settings for a user ID include a root directory (/) specification, but the user ID does not have access to the root directory.

Corrective Action: Verify that the system root directory is mounted and that the user ID OMVS home settings are correct.

RACDCERT or another RACF command abends during configuration

Symptom: A RACF command abends with code S684 or code 047 during the configuration process. On checking the script log, you find a message such as the following:

```
Script izutsoz.rexx returned with reason code -1668
```

Possible Cause: The RACF command is not defined in AUTHCMD section of your active IKJTSOxx parmlib member.

Corrective Action: Verify that the IKJTSOxx member defines the required RACF commands. See the list of IKJTSOxx parmlib updates in the *z/OS Program Directory*. The AUTHCMD section of member IKJTSOxx should list RACDCERT and a number of other RACF commands. You can update the IKJTSOxx member dynamically through the TSO command: `PARMLIB UPDATE(xx)` where *xx* is the correct suffix.

Problems when accessing the user interface

This topic provides troubleshooting tips for resolving problems related to the user interface of z/OSMF.

Troubleshooting topics are included for the following problems and scenarios:

- "Browser cannot connect to z/OSMF" on page 209
- "Missing initialization message or JSP processing error when attempting to use z/OSMF" on page 211
- "Certificate error in the Mozilla Firefox browser" on page 212
- "Cannot log into z/OSMF" on page 214
- "Re-authenticating in z/OSMF" on page 216
- "User receives message ICH408I for insufficient authority to an EZB.STACKACCESS resource" on page 216
- "Help link does not work" on page 217
- "Action or link that was previously provided is not available" on page 217
- "A script takes too long to run or is not responding" on page 218.

Browser cannot connect to z/OSMF

When you log in to z/OSMF for the first time, your browser either does not connect, or waits indefinitely. Verify that the browser has network connectivity to the host on which the z/OSMF instance is running. If your network connectivity is functioning properly, there might be an issue with the digital certificates that are used for SSL connections.

See the following topics:

- "Check your network connection" on page 210
- "Enable the client with a certificate signed by a certificate authority" on page 210
- "More information about certificates" on page 211

Check your network connection

Try the following network diagnostic techniques:

- Entering the command NSLOOKUP to verify that the host name is resolvable
- Pinging the host system for a response
- Running the TRACEROUTE command.

Enable the client with a certificate signed by a certificate authority

Follow these steps:

1. **Generate a client certificate and associate it with the user ID that is associated with the server.**. For example, assume that you want to create a client certificate with the label **Certificate for user DEBUG41**. This label is signed by the internal Certificate Authority (CA), which uses the label **zOSMFCA**. This certificate is created under the user ID DEBUG41.

   To create the client certificate signed by the internal CA, enter the following RACF command:

   ```
   RACDCERT ID(DEBUG41) GENCERT SUBJECTSDN(CN('User DEBUG41')
   O('Your Company') OU('Org A') C('US')) WITHLABEL('Certificate for DEBUG41')
   SIGNWITH(CERTAUTH LABEL('zOSMFCA'))
   ```

   Where the distinguished name consists of the following properties:

   Common name (Domain Name)

   `User DEBUG41`

   Organization name

   `Your Company`

   Optional organizational unit

   `Org A`

   Country code

   `US`

   User ID under which the client certificate is to be added

   `DEBUG41`

   Label of the client certificate

   `Certificate for DEBUG41`

   Label of the CA certificate that is used to sign the client certificate

   `zOSMFCA`

   The client certificate is created with status TRUST, which indicates that the client certificate can be used to authenticate the user ID DEBUG41.

2. **Add the signed client certificate to the client's browser.**

   a. Export the client certificate to an MVS data set. In this example, to export the client certificate to a z/OS data set, you can enter the following RACF command:

   ```
   RACDCERT ID(DEBUG41) EXPORT(LABEL('Certificate for DEBUG41'))
   DSN('TYQTYQ.CLIENTCR.DEBUG41.P12') FORMAT(PKCS12DER) PASSWORD('Test1234')
   ```

   Where:

   - DEBUG41 is the user ID associated with the client certificate to be exported.
   - `Certificate for DEBUG41` is the label of the client certificate.
   - `TYQTYQ.CLIENTCR.DEBUG41.P12` is the data set that will contain the client certificate.

- `PKCS12DER` indicates that the client certificate and private key are DER encoded when saved to the data set.
- `Test1234` is the password that is associated with the encrypted certificate. You are required to provide this password when you import the client certificate into the browser. The password is case-sensitive.

b. FTP the client certificate to the client's workstation. In this example, the FTP command is used to transfer the PKCS12 data set that contains the signed client certificate to the client's workstation. The following steps are performed on the workstation:

1) Enter the FTP command and the host name or IP address of the server, for example, `ftp hostname.com`.
2) When prompted, enter your user ID and password.
3) Enter **`bin`** to transfer the file in binary format.
4) Transfer the file to the workstation by entering **`get 'TYQTYQ.CLIENTCR.DEBUG41.P12' debug41.p12`**
5) Enter **`quit`** to exit.

c. Import the client certificate into the user's web browser. In this example, the PKCS12 file is imported into the Mozilla Firefox browser:

1) Start the Firefox browser.
2) Access the Certificate Manager by selecting **Tools** > **Options** > **Privacy & Security** > **View Certificates**.
3) Under **Certificate Manager**, click **Your Certificates**.
4) To import the certificate, click **Import**.
5) Locate your PKCS12 certificate file and select it.
6) Click **Open** and enter the case-sensitive password to be used for protecting the file.
7) Click **OK**. The following message is displayed: "`Successfully restored your security certificate(s) and private key(s).`"
8) Click **OK**. Verify that the certificate label is shown in the window **These are Your Certificates**.
9) To make these changes effective, restart the browser.

Tip: For the Microsoft Internet Explorer browser, you can double-click the PKCS12 certificate file to import it.

In an installation with many z/OSMF users, you must decide on an appropriate way to distribute the certificate to users. For example:

- Send the certificate to users in email.
- Allow users to download the certificate from the mainframe by FTP
- Implement a method for sending certificates to users automatically.

More information about certificates

For another example that uses certificates in z/OSMF connections, see Chapter 9, “Configuring a primary z/OSMF for communicating with secondary instances,” on page 163.

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

Symptoms: The following symptoms occur in this sequence:

1. You start z/OSMF, but see no message in the operator log about whether z/OSMF started successfully or failed.
2. You attempt to access the z/OSMF URL, but encounter a JSP processing error with HTTP code 500, along with text like the following with supporting messages:

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

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

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

Possible Cause: A failure of the JSP to compile typically means that one or more required classes could not be found. Most likely, this is a problem with a referenced shared library. Failures with the shared libraries typically mean either of the following:

- Shared libraries class path entries are incorrect.
- Class path entries point to missing JAR files.

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

Investigation: Use the following procedure to determine the cause of the error.

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

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

2. The directory does not exist, so determine which file systems are mounted.

Corrective Action: Mount the necessary file system in the correct location and restart z/OSMF.

Certificate error in the Mozilla Firefox browser

When logging into z/OSMF for the first time, you might notice that the Mozilla Firefox browser displays the error message: `Secure Connection Failed`.

If the error message indicates that the browser does not recognize the Certificate Authority (CA) certificate that is configured for z/OSMF, you can resolve the error by adding the certificate to the browser security exception list, or importing the certificate into the browser. For information, see the following sections:

- “Adding the CA certificate to the security exceptions list” on page 212
- “Importing the CA certificate into the browser” on page 213.

If the error message indicates that the certificate contains the same serial number as another certificate issued by the CA, it is possible that your browser contains a CA certificate from a previous installation of z/OSMF. If so, you can remove the older certificate from the browser, as described in “Removing the CA certificate from the browser” on page 214. Then, try again to access z/OSMF and allow the new certificate to be stored in the browser.

Adding the CA certificate to the security exceptions list

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

Do the following:

1. On the error page, click **Or you can add an exception**.
2. Click **Add Exception**. The *Add Security Exception* dialog is displayed.
3. Click **Get Certificate**.

4. Click **View** to display a window that describes the problem with your z/OSMF site.

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

   Examine the *Issued By* fields. Verify that the certificate was issued by the certificate authority (CA) that was used to generate the server certificate. By default, z/OSMF uses the certificate authority *zOSMFCA*.

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

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

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

Importing the CA certificate into the browser

You can import the CA certificate into your browser. Doing so involves exporting the z/OSMF certificate from RACF, transferring the CA certificate to your workstation, and importing the CA certificate into your browser.

The CA certificate is determined by your configuration setting for the variable IZU_DEFAULT_CERTAUTH. If this variable is set to Y, z/OSMF creates the CA during the configuration process. Otherwise, no CA is created, and z/OSMF uses CERTAUTH LABEL('zOSMFCA') to sign the certificate. z/OSMF uses the SAF key ring name `IZUKeyring.IZU_SAF_PROFILE_PREFIX`.

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

1. List the key rings for the z/OSMF server user ID, using the RACDCERT command, for example:

   ```
   RACDCERT ID(IZUSVR1) LISTRING(*)
   ```

   Figure 61 on page 213 shows an example of the output from the RACDCERT command.

   ```
   Digital ring information for user IZUSVR1:

     Ring:
          >IZUKeyring.IZUDFLT<
     Certificate Label Name            Cert Owner     USAGE      DEFAULT
     --------------------------------   ------------   --------   -------
     zOSMFCA                           CERTAUTH       CERTAUTH     NO
     Verisign Class 3 Primary CA       CERTAUTH       CERTAUTH     NO
     Verisign Class 1 Primary CA       CERTAUTH       CERTAUTH     NO
     Thawte Server CA                  CERTAUTH       CERTAUTH     NO
     Thawte Premium Server CA          CERTAUTH       CERTAUTH     NO
     Thawte Personal Basic CA          CERTAUTH       CERTAUTH     NO
     Thawte Personal Freemail CA       CERTAUTH       CERTAUTH     NO
     Thawte Personal Premium CA        CERTAUTH       CERTAUTH     NO
   ```

   Figure 61. Digital ring information for the z/OSMF server user ID

   Verify that the configured SAF key ring is shown for the z/OSMF server user ID. Note the key ring name and the certificate label (zOSMFCA, in this case).

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

   ```
   RACDCERT EXPORT(LABEL(' zOSMFCA')) CERTAUTH
   DSN('??????.CERT.AUTH.DER')FORMAT(CERTDER)
   ```

3. Transfer this file in binary format to your workstation. Keep the `.der` extension when you transfer the file.

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

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

Removing the CA certificate from the browser

You can remove an older CA certificate from the browser to allow the CA certificate for the new release of z/OSMF to be added.

Do the following:

1. From the *Tools* menu, click **Options** > **Advanced** tab.
2. Click the **Encryption** tab.
3. Click *View Certificates*.
4. Click the **Servers** tab.
5. In the *Certificate Name* column, locate the *z/OSMF CertAuth* section.
6. Select the certificate files under z/OSMF and click **Delete**.
7. Click **OK**.

Try to access z/OSMF with your web browser. If prompted, allow the CA certificate to be stored in the browser. Your browser will now open to the z/OSMF user interface.

Cannot log into z/OSMF
If a user receives an error when attempting to log into z/OSMF, try troubleshooting with the following steps.

Procedure

1. Verify that the user ID is correct and try logging in. If the user is still not able to log in, continue to the next step.
2. Ensure that the password that is associated with the user ID is correct. If the user is still not able to log in, continue to the next step.
3. It is possible that the password for the user ID is expired. To check, try logging in to TSO through an emulator.
4. Ensure that your installation defined the z/OSMF unauthenticated guest user in your external security manager. This authorization is required so that users can access the z/OSMF Welcome page prior to

login. In a system with RACF, for example, your security administrator can use the following commands to create the unauthenticated guest user:

```
/* Create the z/OSMF unauthenticated USERID */
ADDUSER IZUGUEST RESTRICTED DFLTGRP(IZUUNGRP) OMVS(UID(9011)) +
NAME('zOSMF Unauthenticated USERID') NOPASSWORD NOOIDCARD

/* Permit the z/OSMF unauthenticated USERID access */
PERMIT IZUDFLT CLASS(APPL) ID(IZUGUEST) ACCESS(READ)

/* Permit other users USERID access */
PERMIT IZUDFLT CLASS(APPL) ID(userid) ACCESS(READ)
```

5. If the user is attempting to log in with a password phrase (pass phrase), your installation's external security manager might need to be updated to allow mixed case passwords. In a system with RACF, for example, your security administrator can use the SETROPTS PASSWORD(MIXEDCASE) option to allow mixed-case passwords at your installation. After this change is made, you must restart the z/OSMF server.
6. Check the z/OSMF server job log for message BPXP014I with either of the following messages: ICH420I or BPXP015I. These message pairings indicate that the z/OSMF server did not connect to the z/OSMF angel process.

   - For example:

     ```
     ICH420I PROGRAM BPXBATSL FROM LIBRARY SYS1.LINKLIB CAUSED THE ENVIRONMENT TO BECOME
     UNCONTROLLED.
     BPXP014I ENVIRONMENT MUST BE CONTROLLED FOR DAEMON (BPX.DAEMON) PROCESSING.
     ```

   - Or:

     ```
     BPXP015I HFS PROGRAM /usr/lpp/zosmf/lib/libIzugJni64.so IS NOT MARKED PROGRAM CONTROLLED.
     BPXP014I ENVIRONMENT MUST BE CONTROLLED FOR DAEMON (BPX.DAEMON) PROCESSING.
     ```

   If these messages appear, check the Liberty log for message CWWKB0117W or CWWKB0118W:

   ```
   CWWKB0117W: The angel-name angel process is not available. No authorized services
   will be loaded. The reason code is 4.

   CWWKB0118W: This server is not authorized to connect to the angel-name angel process.
   No authorized services will be loaded.
   ```

   - For message CWWKB0117W, you must start the address space for the angel that is identified in the message. Then, restart the z/OSMF server address space.
   - For message CWWKB0118W, you must grant the z/OSMF server user ID read access to the profile BBG.ANGEL.*proc-name* in the SERVER resource class, where *angel-proc* is the name of the angel started procedure. Then, restart the z/OSMF server address space.

   By default, the Liberty log is located in the following path `/global/zosmf/data/logs/zosmfServer/logs/messages.log`.

What to do next

If none of these steps resolves the problem, contact your system programmer for assistance. The system programmer should check the z/OSMF log files for messages that indicate that the user ID is not authorized.

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

Re-authenticating in z/OSMF

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

About this task

Your z/OSMF session expires after a period of time has elapsed. By default, this period is 495 minutes from the time you log into z/OSMF. Your installation can choose to modify this setting (SESSION_EXPIRE) using the IZUPRMxx parmlib member. z/OSMF. For details, see "IZUPRMxx reference information" on page 36.

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

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

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

Procedure

1. Verify the user ID.

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

Results

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

User receives message ICH408I for insufficient authority to an EZB.STACKACCESS resource

When accessing z/OSMF as a guest user, the user receives message ICH408I for insufficient authority to an EZB.STACKACCESS resource.

About this task

In z/OSMF, a non-authenticated guest user is one who displays the Welcome page, but has not yet logged in. Here, z/OSMF applies the guest user classification (IZUGUEST) to the user. By default, a guest user can access the z/OSMF Welcome page and the default links.

A guest user might encounter an ICH408I message like the following:

```
ICH408I USER(IZUGUEST ) GROUP(GUESTGRP) NAME(ZOSMF UNAUTH USER)
  EZB.STACKACCESS.nnn.nnn CL(SERVAUTH)
```

```
   INSUFFICIENT ACCESS AUTHORITY
   FROM EZB.STACKACCESS.*.* (G)
   ACCESS INTENT(READ   )  ACCESS ALLOWED(NONE   )
```

This problem can occur if your installation created a NETACCESS or STACKACCESS rule to limit access to the TCP/IP stack. If so, a login attempt to the z/OSMF server is first performed under the IZUGUEST identity before the identity is switched to that of the user's TSO/E user ID. This behavior allows the z/OSMF Welcome page to be displayed to the user, prior to log-in.

Procedure

1. It is recommended that your installation define the IZUGUEST identity with the RESTRICTED attribute. Doing so means that the guest user cannot access any profiles unless explicitly granted. That is, the UACC specification is ignored for any NETACCESS or STACKACCESS rule.
2. If your installation uses a STACKACCESS or NETACCESS rule, grant the IZUGUEST identity READ access to the specific EZB.STACKACCESS.*nnn*.*nnn* or EZB.NETACCESS.*nnn*.*nnn* profile that is referenced in the ICH408I message. This authorization allows the user to access the TCP stack on which the z/OSMF server is running.

Help link does not work

The online help information for the z/OSMF user interface (UI) pages or messages is not available.

Symptom

The user clicks a help link to open a new window with help information for a UI page or message, but the help is not displayed. Instead, the error message `file not found` is displayed in the user’s web browser.

Possible cause

The help files are missing or are not readable. Or, new help files were installed and the z/OSMF server was not restarted. By default, the z/OSMF help files reside at the location `/global/zosmf/helps/eclipse/plugins`.

System programmer response

Use the following procedure to resolve this error:

1. Verify that symlinks exist in the `/global/zosmf/helps/eclipse/plugins` subdirectory. The symlinks must refer to the z/OSMF product directory, which, by default, is `/usr/lpp/zosmf`).
2. Verify that the EJBROLE resource class is defined properly; it is case-sensitive.
3. Restart the z/OSMF server, for example, through the MVS **START** command.

User response

No action is required.

Action or link that was previously provided is not available

Symptom: An action or link that was previously provided in the user interface is disabled, not listed, or no longer provided.

Possible Cause:

- No items have been selected against which to perform the action.
- Too many items have been selected.
- The action or link is not applicable for the selected items.
- The event type is not registered or no handlers are available to process the request.

Administrator Action:

1. Determine if the user-interface control invokes an event type. For IBM-supplied event requestors, see the topic about the in IBM z/OS Management Facility Programming Guide.
2. If the user-interface control invokes an event type, do the following:
   a. Verify that the event type is registered in the Application Linking Manager task.
   b. If the event type is not registered, ensure that the plug-in that registers the event type is configured in z/OSMF.
   c. If the plug-in is configured, you can use the Application Linking Manager task or the API to register the event type, or you can recycle the z/OSMF server to register it automatically. For IBM-supplied event types, to register them manually, specify the information included in the topic about the in IBM z/OS Management Facility Programming Guide.
   d. Verify that a handler is registered for the event type and that the user is authorized to access the handler.

User Action: Ensure that items are selected and that the correct number and type of items are selected.

A script takes too long to run or is not responding

When using z/OSMF, you might encounter the long-running script dialog, which means that a script is taking a long time to run or that a script has stopped responding. From the dialog, you can decide either to stop executing the script or to continue executing it. If you stop executing the script, the function on that web page that is dependent upon the script might not function properly. If you continue executing the script, the dialog will re-display each time the number of statements executed or the amount of time executing a script exceeds the browser's threshold.

To decrease the number of times the long-running script dialog is displayed, you can increase the maximum amount of time a script is allowed to execute or you can increase the maximum number of statements that can be executed. Whether you are modifying the amount of time or the number of statements is dependent upon the browser. For example, the Firefox threshold is based on time; while the Internet Explorer threshold is based on the number of statements.

For more information about unresponsive or long-running scripts, see the appropriate support web site for your browser:

Firefox

- See the following Mozilla web site for information you might find useful: http://support.mozilla.com/en-US/kb/Warning+Unresponsive+script.

Internet Explorer

- See the following Microsoft web site for information you might find useful: http://support.microsoft.com/kb/175500.

Problems when using Network Configuration Assistant

This section provides a procedure you can use to send troubleshooting documentation to IBM Support.

Steps for sending information to IBM Support

For a failure in the Network Configuration Assistant task, use the following procedure to gather troubleshooting documentation. This information can be used by IBM Support to diagnose the problem.

Procedure

1. Transfer the z/OSMF runtime log files that contain Network Configuration Assistant logging data.

   During normal operations, z/OSMF collects its runtime data (log messages and trace messages) in log files. z/OSMF runtime data is created on the server (server side) or sent to the server by the client (client side). Both types of messages are written to the z/OSMF runtime log files.

z/OSMF creates the log files in the product logs directory, which is, by default, `/global/zosmf/data/logs`. z/OSMF names the log files IZUGn.log, where n is a numeral in the range 0 - 9.

z/OSMF creates log files in a "cascading" manner. The most current log file is always named IZUG0.log. When this log file reaches its predefined limit, z/OSMF saves it as IZUG1.log and begins writing to a new IZUG0.log file. When the IZUG0.log file is again full, z/OSMF saves it as IZUG1.log after it renames the existing IZUG1.log file to IZUG2.log. z/OSMF continues this process, saving each log file under the next available name, up to a maximum of ten log files. Thereafter, z/OSMF discards the oldest log file (IZUG9.log) whenever a new log file must be created.

2. Transfer the currently active backing store file. From the **Tools** option, select **Manage Backing Stores** > **Actions** > **Transfer**.
3. For issues that are related to Cloud Provisioning, create a compressed copy (.zip) of the directory `/global/zosmf/data/datastore/NetworkResourceManager`.
4. Package the files and send them to IBM Support.

Problems when using IBM zERT Network Analyzer

This section provides a procedure you can use to send troubleshooting documentation to IBM Support.

Steps for sending information to IBM Support

For a failure in the IBM zERT Network Analyzer task, use the following procedure to gather troubleshooting documentation. This information can be used by IBM Support to diagnose the problem.

Procedure

1. Use the **Applications Settings** sub-panel on the IBM zERT Network Analyzer task to ensure that the proper level of logging is being used. By default, IBM zERT Network Analyzer writes Info level messages to the z/OSMF runtime logs, but writes no logging information to the IBM zERT Network Analyzer logs.

   After the necessary level of logging is in place, re-create the problem that was reported, if needed.
2. Transfer the z/OSMF runtime log files that contain IBM zERT Network Analyzer logging data.

   During normal operations, z/OSMF collects its runtime data (log messages and trace messages) in log files. z/OSMF runtime data is created on the server or sent to the server by the client. Both types of messages are written to the z/OSMF runtime log files.

   In addition, if IBM zERT Network Analyzer logging is enabled, the IBM zERT Network Analyzer task writes some runtime data (log messages and trace messages) to the z/OSMF runtime log files.

   z/OSMF creates the log files in the product logs directory, which is, by default, `/global/zosmf/data/logs`. z/OSMF names the log files IZUG*n*.log, where *n* is a numeral in the range 0 - 9.

   z/OSMF creates log files in a "cascading" manner. The most current log file is always named IZUG0.log. When this log file reaches its predefined limit, z/OSMF saves it as IZUG1.log and begins writing to a new IZUG0.log file. When the IZUG0.log file is again full, z/OSMF saves it as IZUG1.log after it renames the existing IZUG1.log file to IZUG2.log. z/OSMF continues this process, saving each log file under the next available name, up to a maximum of ten log files. Thereafter, z/OSMF discards the oldest log file (IZUG9.log) whenever a new log file must be created.
3. Transfer the IBM zERT Network Analyzer log files that contain IBM zERT Network Analyzer logging data.

   During normal operations, when logging is enabled, IBM zERT Network Analyzer collects runtime data (log messages and trace messages) specific to IBM zERT Network Analyzer processing in its own separate log files. Only server-side information is written to the IBM zERT Network Analyzer runtime log files.

   By default, IBM zERT Network Analyzer creates its log files in the `/global/zosmf/data/app/<release>/debug` folder, where `<release>` is the current level of IBM zERT Network Analyzer. The format of `<release>` is ZNA*xxxx*, where *xxxx* represents the z/OSMF release level. For example, IBM zERT Network Analyzer running on z/OSMF V2R3 would use ZNAV2R3 for `<release>`. The full name of the default folder would be `/global/zosmf/data/app/ZNAV2R3/debug`. IBM zERT Network Analyzer names the files ZnaDbgn.log, where n is a numeric value in the range 0 - 24.

IBM zERT Network Analyzer creates log files in a "cascading" manner. The most current log file is always named ZnaDbg0.log. When this log file reaches its predefined limit, IBM zERT Network Analyzer saves it as ZnaDbg1.log and begins writing to a new ZnaDbg0.log file. When the ZnaDbg0.txt file is again full, IBM zERT Network Analyzer saves it as ZnaDbg1.log after it renames the existing ZnaDbg1.log file to ZnaDbg2.log. IBM zERT Network Analyzer continues this process, saving each log file under the next available name, up to the current maximum of log files. Thereafter, IBM zERT Network Analyzer discards the oldest log file (ZnaDbgn.log) whenever a new log file must be created.

By default, the maximum number of log files maintained is 10. You can modify that setting on the IBM zERT Network Analyzer **Applications Settings** sub-panel, up to a maximum of 25 possible log files.

4. Package the files and send them to IBM Support.

Problems when using the ISPF task

This topic provides troubleshooting tips for common problems that might occur while using the ISPF task.

Troubleshooting topics are included for the following problems and scenarios:

- "Unexpected behavior occurs in the ISPF user session after the user logs on again" on page 220
- "Log-on or log-off through the ISPF task takes too long" on page 221
- "Log-on through the ISPF task takes too long, even though the system is enabled for reconnectable user sessions" on page 221.

Unexpected behavior occurs in the ISPF user session after the user logs on again

Symptom: User logs off from an ISPF session. On logging on again, the user encounters an unexpected behavior, such as one of the following:

- z/OSMF ISPF environment is not reset
- Logon proc is not run
- Region size is not restored
- Session behaves unexpectedly in some other manner.

Probable cause: The user required a new session, but the ISPF task reconnected the user to an existing session. To save time and system resources, the ISPF task can reconnect a user to an existing session, rather than creating a new session. This reconnect capability requires that some aspects of the user session be preserved after logoff (the session is not completely ended). In some cases, this processing can pose a problem for users who require that their sessions be completely ended and cleaned up during logoff.

Corrective Action: The user can force z/OSMF to create a new session, rather than reconnect to an existing session, by changing one of the logon settings. For example, changing the screen size or region size slightly would result in a new session being created. If this problem occurs frequently or for multiple z/OSMF users, consider deactivating the reconnect capability for the ISPF task. You can do so through parmlib member, CEAPRMxx, which is used to specify options for the common event adapter (CEA) component of z/OS. In CEAPRMxx, the following statements control the reconnect capability for the ISPF task:

- RECONTIME limits the number of reconnectable sessions
- RECONSESSION limits the time that sessions can remain in a reconnectable state.

To deactivate the reconnect capability for the ISPF task, set one or both of these values to zero, as indicated in the commented section of IBM-supplied member, CEAPRM00. For more information about CEAPRM00, see z/OS MVS Initialization and Tuning Reference.

Log-on or log-off through the ISPF task takes too long

Possible Cause: The extra time is used by the system during logon processing to perform a complete log-on for the user. Or, to log-off the user and clean-up the user address space.

Corrective Action: Enable the use of reconnectable sessions for ISPF task users. Doing so can allow for potentially faster logon processing when existing user sessions are eligible for re-use. Enabling reconnectable user sessions involves modifying the CEA component on your system through parmlib member CEAPRMxx. See the descriptions of statements TSOASMGR, RECONSESSIONS, and RECONTIME in z/OS MVS Initialization and Tuning Reference. If reconnectable user sessions are already enabled, consider increasing either the RECONSESSIONS or RECONTIME values.

Log-on through the ISPF task takes too long, even though the system is enabled for reconnectable user sessions

Symptom: User selects the ISPF task, but the resultant log-on takes too long, even though the z/OS system is enabled for reconnectable user sessions.

Possible Cause: On a system enabled for reconnectable user sessions, the ISPF task checks for a session to which the user can reconnect. No eligible session was found, however, possibly because the session has expired, based on one or more system limits. Without an available reconnectable session, the ISPF task creates a new session for the user. The additional processing increases the time for the log-on request to complete. Another possibility is that the ISPF task has discarded its reconnectable user sessions as part of normal clean-up. This processing occurs when the ISPF task is idle (has no active users) for at least 15 minutes. After the clean-up is completed, a subsequent user of the ISPF task will always receive a new session.

Corrective Action: You can increase the number of reconnectable sessions allowed on your system and the time that sessions can remain connectable. See the descriptions of the RECONTIME and RECONSESSION statements of parmlib member CEAPRMxx in z/OS MVS Initialization and Tuning Reference. Regardless of these settings, the ISPF task discards its reconnectable sessions when it is idle for 15 minutes.

Problems when using the Incident Log task

This topic provides troubleshooting tips for common problems that might occur while using the Incident Log task.

Troubleshooting topics are included for the following problems and scenarios:

- "User cannot access the Incident Log task" on page 221
- "User encounters message ICH408I" on page 222
- "CEA address space is blocking the use of the sysplex dump directory" on page 222
- "CEA cannot allocate a data set for dump prepare or snapshot" on page 222
- "Diagnostic log streams and other incident data for deleted incidents are not being deleted over time" on page 222
- "Problems when attempting to send data" on page 223.

User cannot access the Incident Log task

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

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

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

User encounters message ICH408I

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

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

Corrective Action: Determine whether the user should be allowed to update the master catalog. If so, you can authorize the user to create entries in the master catalog through the appropriate security commands.

To authorize a user to create entries in a user catalog, use the following command:

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

CEA address space is blocking the use of the sysplex dump directory

Possible Cause: CEA holds an exclusive ENQ to serialize on the sysplex dump directory data set while processing a z/OSMF request. Usually, the ENQ is released in microseconds. But sometimes an I/O error could result in holding the ENQ for longer time periods, therefore blocking DUMPSRV from updating the dump directory with information about a new dump, or your installation from doing maintenance on the sysplex dump directory data set.

Corrective Action: Use the system console command **`F CEA,DROPIPCS`** to disconnect CEA from the IPCS sysplex dump directory data set.

CEA cannot allocate a data set for dump prepare or snapshot

Possible Cause: CEA alias is not cataloged properly.

Corrective Action: If your installation has a user catalog setup instead of using the MASTER catalog, you might need to define the CEA alias to the user catalog. For example:

```
DEFINE ALIAS(NAME(CEA) RELATE(YOUR_CATALOG_NAME))
```

Diagnostic log streams and other incident data for deleted incidents are not being deleted over time

Possible Cause: If you modified the HLQ parameter value in the CEAPRMxx parmlib member, CEA no longer detects the previously-stored diagnostic data files stored under the old high level qualifier.

Corrective Action: Carefully remove the data manually. The data exists in both log stream and data set format. Use caution as to not remove any needed data. Remove data sets and log streams manually. To list the available log streams, enter the following system console command: **`D LOGGER,L`**.

Most log streams with the status of AVAILABLE are the result of diagnostic snapshots taken at the time of the dump. The old high level qualifier appears in the log streams that were created earlier by CEA. To delete log streams, enter the following command: **`SETLOGR FORCE,DELETE,LSN=logstreamname`**.

To remove data sets, do the following:

- List the data sets having the same HLQ as the available log streams.
- Delete the data sets.

Problems when attempting to send data

When you invoke the Send Diagnostic Data wizard from the Incident Log task, the information supplied in the page is used to produce one FTP job for each diagnostic data file being sent. Thus, if an incident has a dump data set and three log snapshot files, four FTP jobs are created (and the FTP Job Status table will have four entries). To debug the FTP jobs, you need access to the job output. Typically, this is done by using z/OS System Display and Search Facility (SDSF) to examine the spooled output from the job.

FTP job status codes and other information

The Incident Log task allows you to display the status of the FTP jobs. On the *FTP Job Status* page, you can display the status of all FTP jobs associated with a particular incident or the FTP jobs associated with diagnostic data.

For a description of each FTP job status condition and the actions you can take to resolve errors in the jobs, see the online help for the *FTP Job Status* page.

Chapter 16. Configuration messages

This chapter describes the z/OSMF messages that you might encounter during the configuration process. These messages have a message ID between IZUG000-IZUG399.

For each configuration message, this document provides a detailed explanation of the message; describes the reason codes (if any) listed in each message; and, suggests actions that you can take to resolve the issue. The messages are organized by message ID.

Information about other messages you might encounter while configuring z/OSMF is provided in the following documents:

- Messages for the common event adapter (CEA) component of z/OS are prefixed by CEA. See *z/OS MVS System Messages*, which is available online in the z/OS Internet Library (www.ibm.com/servers/resourcelink/svc00100.nsf/pages/zosInternetLibrary).
- 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* .
- Messages for the WebSphere Liberty profile are prefixed by CW. For descriptions of the WebSphere messages, see WebSphere Liberty message descriptions (www.ibm.com/support/knowledgecenter/SS7K4U_8.5.5/com.ibm.websphere.wlp.zseries.doc/ae/rwlp_messages.html).

All other messages for z/OSMF are documented in the z/OSMF node of the IBM Knowledge Center, which is available at https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zosmfmessages.help.doc/izuG00hpMessages.html.

Because of the various layers of function involved in typical z/OSMF operations, locating a particular message might require you to check more than one location. For more information, see “Types of messages in z/OSMF” on page 202.

IZUG000-IZUG399

This topic describes the z/OSMF messages that have a message ID between IZUG000-IZUG399.

IZUG001E **A system request for storage in the *storage-area* area ended in error. The return code is *return-code*.**

Explanation
While attempting to allocate storage for the z/OSMF global storage area control block (IZUGSP), the system encountered an error that prevented the storage request from completing. The return code from the STORAGE macro is included in the message for diagnostic purposes.

This message might indicate a storage constraint in your system.

In the message text:

storage-area
Storage area that was requested.

return-code
Return code from the STORAGE macro.

System programmer response
This problem can be caused by a shortage of common storage or private storage. Refer to the STORAGE macro return code for more information.

Most likely, the problem is that ECSA storage (subpool 241) is exhausted. When this happens, further storage requests are allocated from the much smaller CSA storage area. Determine whether ECSA is exhausted and, if so, why the shortage occurred. For example, it is possible that not enough common storage is currently allocated, or that an address space has allocated a large amount of ECSA storage.

For assistance with this problem, contact IBM Support.

User response:
Contact the system programmer for assistance.

IZUG002E **The address space *address-space-name* failed to start. The following error codes were returned: Return code *return-code*, reason code *reason-code*.**

Explanation
This message is issued when one of the following z/OSMF dependent address spaces cannot be started:

- IZUINSTP, which is used for detecting z/OS UNIX and TCP/IP.
- z/OSMF server, which is named IZUSVR1, by default.
- z/OSMF angel process, which is named IZUANG1, by default.

The return code from the ASCRE macro is included in the message for diagnostic purposes.

In the message text:

address-space-name
Address space that was not started.

return-code
Return code from the ASCRE macro.

reason-code
Reason code from the ASCRE macro.

System programmer response
Refer to the STORAGE macro return code for more information.

For assistance with this problem, contact IBM Support.

User response:
Contact the system programmer for assistance.

IZUG003E **The request to listen for ENF code 83 failed with return code *return-code*.**

Explanation
An error occurred that prevented the system from listening for events related to the z/OSMF server, such as server start-up or server shut down. The return code from the ENFREQ macro is included in the message for diagnostic purposes.

In the message text:

return-code
Return code from the ENFREQ macro.

System programmer response
Refer to the ENFREQ macro return code for more information.

For assistance with this problem, contact IBM Support.

User response:
Contact the system programmer for assistance.

IZUG004I **An autostarted z/OSMF server was detected on another system in the same AUTOSTART group. As a result, the local system will connect to the autostarted server, rather than attempting to start a server locally.**

Explanation
Only one z/OSMF server can be active per autostart group in the sysplex. An autostarted z/OSMF server holds an enqueue on the z/OSMF user directory file system, and handles the z/OSMF requests from other systems that are connected to the same AUTOSTART group.

This message can be issued during IPL for either of the following situations:

- The initializing system determines that an autostarted z/OSMF server is already active in the sysplex for the local AUTOSTART group. Because only one autostarted server can be active for a particular AUTOSTART group, the system does not attempt to autostart a z/OSMF server on the local system. In IZUPRMxx, the default setting of AUTOSTART(LOCAL) is treated as AUTOSTART(CONNECT).
- Multiple z/OSMF servers are attempting to autostart at the same time. The first system to complete IPL will autostart the z/OSMF server. The other systems will be treated as AUTOSTART(CONNECT) systems.

System programmer response:
No action is required.

User response:
No action is required.

IZUG005E **The attempt to cancel the z/OSMF server, which is identified by job *job-name*, ended with an error. The return code is *return-code*.**

Explanation
Only one z/OSMF server can be active per AUTOSTART group in the sysplex. Because a z/OSMF server is already active on another system in the same AUTOSTART group, the local system attempted to cancel the z/OSMF server that was attempting to start locally. However, an error occurred that prevented the cancel request from completing. The return code from the IEFSSREQ macro is included in the message for diagnostic purposes.

In the message text:

job-name
Job name for the local z/OSMF server.

return-code
Return code from the IEFSSREQ macro.

System programmer response:
Contact IBM Support for assistance.

User response:

Contact the system programmer for assistance.

IZUG006E **The z/OSMF service *service-number* failed after detecting one or more errors in the IZUPRMxx parmlib member. The return code is *return-code*.**

Explanation

During IPL, the indicated z/OSMF service attempted to read the contents of the currently active IZUPRMxx parmlib member. However, the service failed when it detected errors in one or more of the parmlib member statements. The return code from the z/OSMF service is included in the message for diagnostic purposes.

In the message text:

service-number
Number that identifies the failing z/OSMF service.

return-code
Return code from the failing service.

System programmer response:
Contact IBM Support for assistance.

User response:
Contact the system programmer for assistance.

IZUG007I **A z/OSMF server is already running in AUTOSTART group *autostart-group-name*. The extra server identified by address space *address-space-name* on system *system-name*is cancelled.**

Explanation

Only one z/OSMF server can be active per AUTOSTART group in the sysplex. Because a z/OSMF server is already active on another system in the same AUTOSTART group, the local system has cancelled the z/OSMF server that was attempting to start locally.

In the message text:

autostart-group-name
AUTOSTART group name.

address-space-name
Address space name.

system-name
System name.

System programmer response:
No action is required.

User response:
No action is required.

IZUG008I **Initialization of the z/OSMF server is suspended until TCP/IP is active.**

Explanation:
The z/OSMF server initialization does not complete until TCP/IP is initialized on the system.

System programmer response:
No action is required.

User response:
No action is required.

IZUG009I **the z/OSMF AUTOSTART server cannot be started due to the needed ENQ has been hold by another server**

Explanation:
the z/OSMF AUTOSTART server cannot be started due to the needed ENQ hold by another system

System programmer response:
No action is required.

User response:
No action is required.

IZUG010E **The ENQ failed to be released. RC= *return-code*, RSN= *reason-code*.**

Explanation

Only one z/OSMF server can be active per AUTOSTART group in the sysplex in IPL. When the actived z/OSMF server starts, a ENQ (qname:zosmf/ rname:AUTOSTART_GROUP plus FILE SYSTEM mounted on user directory) will be hold. When the z/OSMF server stops, the ENQ is intended to be released. The return code and reason code from the ISQENQ macro is included in the message for diagnostic purposes.

In the message text:

return-code
Return code from the ISQENQ macro.

reason-code
Reason code from the ISQENQ macro.

System programmer response:
Contact IBM Support for assistance.

User response:
Contact the system programmer for assistance.

IZUG011I ***action* z/OSMF *procedure-name* procedure on *timestamp*.**

Explanation

The specified action was taken on the specified procedure. The timestamp indicates the time the action was taken on the procedure.

In the message text:

action
The action being performed on the procedure. This can be the start or completion of the procedure.

procedure-name
Name of the procedure.

timestamp
The timestamp for the procedure being performed.

System programmer response:
No action is required.

User response:
No action is required.

IZUG012W **The user ID executing this procedure is *actual-userid*. The expected user ID *expected-userid*should be used instead.**

Explanation
An unexpected user ID was found to be executing the procedure. The specified expected user ID should be used instead.

In the message text:

actual-userid
User ID executing the procedure.

expected-userid
The user id expected to be executing the procedure.

System programmer response:
The expected user id should be used to execute the procedure.

User response:
No action is required.

IZUG013E **The *branch-country-name* code must be *branch-country-range*alphanumeric characters (A-Z, 0-9).**

Explanation
The value specified for the branch or country code does not conform to guidelines.

In the message text:

branch-country-name
Name of the branch or country

branch-country-range
Range for the branch or country attribute.

System programmer response:
Specify the correct value.

User response:
No action is required.

IZUG014E **No roles match the value *the-value*specified with the -role option.**

Explanation
There were no matches found for the specified value.

In the message text:

the-value
No roles were found matching the specified value.

System programmer response:
Ensure that the role file or alias exists and retry the operation.

User response:
No action is required.

IZUG015I **The following aliases (and role files) can be specified when authorizing users.**

Explanation:
Specifies that a list of role files will follow based on the request.

System programmer response:
No action is required.

User response:
No action is required.

IZUG016I **Specify *the-alias* or *the-role-file*to authorize the user id to this role.**

Explanation
The specified alias value is set in the specified role file.

In the message text:

the-alias
The alias value in the role file.

the-role-file
The role file.

System programmer response:
No action is required.

User response:
No action is required.

IZUG017W **Unable to access file *the-target-file*. The file *the-default-file*will be used.**

Explanation
The specified file is not accessible. The specified default file will be used.

In the message text:

the-target-file
The target file to be used.

the-default-file
The default file to be used.

System programmer response:
Check the specified target file to ensure that the file is accessible and retry the operation.

User response:
No action is required.

IZUG018W **The property *the-property* is set to *the-value*. The value is incorrect. The default value of *the-default*will be used.**

Explanation
The specified timeout value is incorrect. The specified default value will be used.

In the message text:

the-property
The property that is set.

the-timeout
The value for the property.

the-default
The default value for the property.

System programmer response:
No action is required.

User response:
No action is required.

IZUG019I **The *the-procedure* timeout value is set to *the-timeout*.**

Explanation
The specified timeout value will be used for the specified procedure.

In the message text:

the-procedure
The procedure being performed.

the-timeout
The timeout value for the procedure being performed.

System programmer response:
No action is required.

User response:
No action is required.

IZUG020W **The value *prop-value* was found for property *prop-name1* in file *file-name1*. The role file *file-name2*will not be processed.**

Explanation
The indicated property was found in the specified file containing the indicated value. At least one valid group name or user id is required in order to process the specified file.

In the message text:

prop-value
The value of the property.

prop-name1
The name of the property.

file-name1
The name of the file.

file-name2
The name of the file.

System programmer response:
Specify a valid group name or user id and retry the operation.

User response:
No action is required.

IZUG021E **The argument *the-argument*is required.**

Explanation
The specified argument is required and must be supplied.

In the message text:

the-argument
The name of the required argument.

System programmer response:
Retry the operation and provide the specified argument.

User response:
No action is required.

IZUG022W **Argument *the-argument*is ignored.**

Explanation
The specified argument will be ignored.

In the message text:

the-argument
Name of the argument that will be ignored.

System programmer response:
No action is required.

User response:
No action is required.

IZUG023W **An unexpected error has occurred while attempting to *the-procedure*.**

Explanation
An error was encountered while attempting to run the specified procedure.

In the message text:

the-procedure
The procedure where the error occured.

System programmer response:
Review the log file for additional information and retry the operation.

User response:
No action is required.

IZUG024W **Te value *prop-value* was found for properties *prop-name1* and *prop-name2* in file *file-name1*. The role file *file-name2*will not be processed.**

Explanation
The indicated properties was found in the specified file containing the indicated value. At least one valid group name or user id is required in order to process the specified file.

In the message text:

prop-value
The value of the property.

prop-name1
The name of the property.

prop-name2
The name of the property.

file-name1
The name of the file.

file-name2
The name of the file.

System programmer response:
Specify a valid group name or user id and retry the operation.

User response:
No action is required.

IZUG025I **The value *prop-value* for property *prop-name* was found in file *file-name*.**

Explanation
The indicated property was found in the specified file containing the indicated value.

In the message text:

prop-value
The value of the property.

prop-name
The name of the property.

file-name
The name of the file.

System programmer response:
No action is required.

User response:
No action is required.

IZUG026I **The *file-type* file *file-name*is being processed.**

Explanation
The specified file of the specfied type is being processed.

In the message text:

file-type
The type of file being processed.

file-name
The name of the file being processed.

System programmer response:
No action is required.

User response:
No action is required.

IZUG027E **Multiple selection of plug-ins in *value*are not allowed.**

Explanation
One or more duplicate entries were found in the value. The specified value is incorrect for the property.

In the message text:

value
The value containing duplicate entries

System programmer response:
Correct the error and retry. Ensure the value for the specified property is valid.

User response:
No action is required.

IZUG028I **Completed *procedure-name* for *plugin-name*.**

Explanation
The specified procedure has completed for the specified plug-in.

In the message text:

procedure-name
Name of the procedure.

plugin-name
Name of the plugin.

System programmer response:
No action is required.

User response:
No action is required.

IZUG029I **Starting *procedure-name* for *plugin-name*.**

Explanation
The specified procedure is being processed for the specified plug-in.

In the message text:

procedure-name
Name of the procedure.

plugin-name
Name of the plugin.

System programmer response:
No action is required.

User response:
No action is required.

IZUG030E **Script *script-name* requires the following input options: *input-options*.**

Explanation
The valid script options are displayed. For information about the script options, see IBM z/OS Management Facility Configuration Guide .

In the message text:

script-name
Name of the script

input-options
Options required by the script.

System programmer response:
Correct the error and retry the operation.

User response:
No action is required.

IZUG031I **The *file-name* file will be used from the following location: *file-name-location***

Explanation
The specified file will be used from the specified location.

In the message text:

file-name
Name of the file.

file-name-location
Name of the file location.

System programmer response:
No action is required.

User response:
No action is required.

IZUG032W **The property *var-name* could not be found in *file-name*. Defaulting value to: *value-name***

Explanation
The specified variable could not be found in the specified file. The variable will default to the specified value. The value is obtained from the shipped default file.

In the message text:

var-name
Name of the variable.

file-name
Name of the file.

value-name
Value for the variable.

System programmer response:
No action is required.

User response:
No action is required.

IZUG033I **Examine each of the output execs and determine which exec is appropriate for your environment. Run one exec only. The output execs are: *rexx-exec-name1*, *rexx-exec-name2***

Explanation
The z/OSMF configuration process creates sample security execs to assist your security administrator in creating security authorizations for z/OSMF. The execs are tailored, based on the selections you made when running the script izusetup.sh -config, or specified in your override file.

z/OSMF creates several execs to accommodate a number of possible configuration paths, however, your installation should run only one of the execs. Your choice of which exec to run depends on whether:

- You are creating a new z/OSMF configuration or migrating from an earlier release of z/OSMF.
- The configuration process detected a change in the authorization mode for your installation.
- One or more of your selected plug-ins require additional security authorizations on your z/OS system.

In the message text:

rexx-exec-name1
Name of the first generated RACF exec.

rexx-exec-name2
Name of the second generated RACF exec.

Have your security administrator review the execs, and run the exec that is appropriate for your environment. Most likely, one of the following descriptions fits your environment.

- The exec named *configfilename*.cfg.rexx is the appropriate choice for new or first-time z/OSMF configurations. This exec contains the superset of required RACF commands, tailored for the plug-in selections you specified when running the script izusetup.sh -config, or specified in your override file.
- The exec named *configfilename*.cfg.convertFromSAFtoREP.rexx is the appropriate choice if your installation is migrating from an earlier release of z/OSMF for the new configuration. This exec contains the subset of RACF commands that are needed to update an existing security setup to SAF based security.

z/OSMF creates the execs for any izusetup.sh invocation that updates your configuration file, even if you are just adding a plug-in to an existing configuration (izusetup.sh -add). If the plug-ins to be added require no additional security setup, the created execs are "empty" and need not be run. It is recommended that your security administrator review each of the output execs to determine whether they require changes and should be run for your installation.

System programmer response:
Have your security administrator review the execs and determine which exec to run, based on the guidance information in this message. For more information about the security execs, see IBM z/OS Management Facility Configuration Guide .

User response:
No action is required.

IZUG034I **The z/OSMF configuration process has created a set of sample security execs for your reference in directory *directory-name*.**

Explanation

The z/OSMF configuration process creates sample security execs to assist your security administrator in creating security authorizations for z/OSMF. The execs are tailored, based on the selections you made when running the script izusetup.sh -config, or specified in your override file. The execs are stored in the indicated directory.

In the message text:

directory-name
Directory in which the generated sample security execs reside.

System programmer response:
See the accompanying message for the names of the sample security execs.

User response:
No action is required.

IZUG035W **The default value *file-name*will be used because a fully-qualified path name was not provided for the file.**

Explanation

A fully-qualified path name was not provided for the file. The default value specified in the property IZU_CONFIG_DIR will be used.

In the message text:

file-name
Name of the file.

System programmer response:
No action is required.

User response:
No action is required.

IZUG036W **The variable *var-name* could not be found in the configuration file *file-name*. Defaulting value to: *value-name***

Explanation

The specified variable could not be found in the specified configuration file. The variable will default to the specified value.

In the message text:

var-name
Name of the variable.

file-name
Name of the configuration file.

value-name
Value for the variable.

System programmer response:
No action is required.

User response:
No action is required.

IZUG037E **The value *value* in file *file* is incorrect for property *property*.**

Explanation

The specified value is incorrect for the property.

In the message text:

value
The value for the property

file
File containing the value.

property
Property containing the value.

System programmer response:
Correct the error and retry. Ensure the value for the specified property is valid.

User response:
No action is required.

IZUG038E **The file *file-name* does not conform to the expected format: *release-level*. Migrate the file to the correct format and retry the operation.**

Explanation
The file is not at the correct release level.

In the message text:

file-name
Name of the file.

release-level
Level of the release.

System programmer response:
Migrate the file to the correct release level and retry the request.

User response:
No action is required.

IZUG039I **The override file *config-file* has been migrated to the format: *release-level*.**

Explanation
The specified configuration file has been migrated to the specified release level.

In the message text:

config-file
Name of the configuration file.

release-level
Level of the release.

System programmer response:
No action is required.

User response:
No action is required.

IZUG040W **The variable *var-name* could not be found in the override file *file-name*. Defaulting value to: *value-name***

Explanation
The specified variable could not be found in the specified override file. The variable will default to the specified value.

In the message text:

var-name
Name of the variable.

file-name
Name of the override file.

value-name
Value for the variable.

System programmer response:
No action is required.

User response:
No action is required.

IZUG041E **The variables specified in override file *file-name*could not be exported.**

Explanation
The variables included in the specified override file were not exported because an error occurred.

In the message text:

file-name
Name of the override file.

System programmer response:
For more information, review the log file that was created for the error.

User response:
No action is required.

IZUG042I **The override file *file-name* conforms to the expected format: *release-level*. No migration will be performed.**

Explanation
No migration is needed since the specified override file is at the correct version level.

In the message text:

file-name
Name of the override file.

release-level
Level of the release.

System programmer response:
No action is required.

User response:

No action is required.

IZUG043E **Unable to update override file *file-name*.**

Explanation
The specified override file could not be updated.

In the message text:

file-name
Name of the override file.

System programmer response:
Ensure that the caller is authorized to update the override file. For more information, review the log file that was created for the error.

User response:
No action is required.

IZUG044I **The input override file *over-file* was saved to a backup file *back-up-override-file*.**

Explanation
The data of the source override file has been saved to the specified override file.

In the message text:

over-file
Name of the override file.

back-up-override-file
Name of the backup override file.

System programmer response:
No action is required.

User response:
No action is required.

IZUG045E **Unable to back up override file data.**

Explanation:
The data of the source override file could not be saved. Ensure that the permission settings are correct for the file and directory.

System programmer response:
Ensure that the permission settings are correct for the file and directory.

User response:
No action is required.

IZUG046I **Enter the existing *group-name* group name that is used to authorize users to the *plug-in-name* resources. Enter *keyword-name*if no group exists.**

Explanation
The message prompts for the plug-in group name. These group are expected to already exist. If a group does not exist or if the group has not yet been created enter the specified keyword. The RACF exec generated will have the required commands commented out. Once the group has been created, update and uncomment the commands in the RACF exec.

In the message text:

group-name
Name of the group

plug-in-name
Name of the plug-in

keyword-name
Name of the keyword

System programmer response:
Enter the information or enter the specified keyword if no group exists.

User response:
No action is required.

IZUG047I **Enter the existing *group-name* group name that is used to authorize users to the *plug-in-name* resources. Press Enter to accept the default *default-value*, or enter *keyword-name*if no group exists.**

Explanation
The message prompts for the plug-in group name. These groups are expected to already exist. If a group does not exist or if the group has not yet been created enter the specified keyword. The RACF exec generated will have the required commands commented out. Once the group has been created, update and uncomment the commands in the RACF exec.

In the message text:

group-name
Name of the group

plug-in-name
Name of the plug-in

default-value
The default value

keyword-name
Name of the keyword

System programmer response:
Enter the information, press Enter to accept the default, or enter the keyword if no group exists.

User response:
No action is required.

IZUG048W **Group *group-name*does not exist.**

Explanation
The specified group does not exist.

In the message text:

group-name
Name of the group.

System programmer response:
Ensure that the specified group exists. If not create it and retry.

User response:
No action is required.

IZUG049I **z/OSMF configuration has detected a *current-auth-mode* to *new-auth-mode*authorization mode switch.**

Explanation
The current authorization mode will be changed to the new authorization mode specified.

In the message text:

current-auth-mode
The current authorization mode.

new-auth-mode
The new authorization mode.

System programmer response:
No action is required.

User response:
No action is required.

IZUG050I **z/OSMF configuration has detected a *current-auth-mode* to *new-auth-mode* authorization mode switch. The data file system *file-system*must be mounted.**

Explanation
The authorization mode switch indicated requires the data file system specified be mounted.

In the message text:

current-auth-mode
The current authorization mode.

new-auth-mode
The new authorization mode.

file-system
The data file system.

System programmer response:
No action is required.

User response:
No action is required.

IZUG051W **The permissions assigned to directory *directory-name* will be changed to *permissions*.**

Explanation
The current assigned permissions for the specified directory will be changed to the new permissions specified.

In the message text:

directory-name
The directory being checked.

permissions
The new permissions that will be assigned to the specified directory.

System programmer response:
No action is required.

User response:
No action is required.

IZUG052W **The group assigned to directory *directory-name* will be changed to *group-name*.**

Explanation
The current assigned group of the specified directory will be changed to the new group specified.

In the message text:

directory-name
The directory being checked.

group-name
The new group that will be assigned to the specified directory.

System programmer response:
No action is required.

User response:
No action is required.

IZUG053W **The owner assigned to directory *directory-name* will be changed to *new-owner*.**

Explanation
The current owner of the specified directory will be changed to the new owner specified.

In the message text:

directory-name
Directory being checked.

new-owner
User id of the new owner to be assigned to the specified directory.

System programmer response:

No action is required.

User response:
No action is required.

IZUG054I **To obtain the results of the *verification-type* verification, review report *report-name*.**

Explanation
Review the specified report file to obtain the results of the verification.

In the message text:

verification-type
The type of verification being performed.

report-name
Name of the verification report.

System programmer response:
Review the specified report.

User response:
No action is required.

IZUG055E **Group *group-name* not permitted to RACF class *class-name*.**

Explanation
The specified group name is not permitted to the specified RACF class.

In the message text:

group-name
Name of the group being evailuated.

class-name
Name of the RACF class.

System programmer response:
For more information, review the log file created for the error and the RACF report.

User response:
No action is required.

IZUG056I **The file *target-file* was saved to a backup file *back-up-file*.**

Explanation:
The data of the source file has been saved to the specified file.

System programmer response:
No action is required.

User response:
No action is required.

IZUG057E **File *file-name*does not exist or is not accessible.**

Explanation
The specified file does not exist or is not accessible.

In the message text:

file-name
Name of the file.

System programmer response:
Ensure that the specified file exists and is accessible. Retry your request.

User response:
No action is required.

IZUG058E **File *file-name* is incomplete. The property *configuration-property*is missing.**

Explanation
This message indicates that the specified configuration property was not found. The script exits in error.

In the message text:

file-name
The configuration file.

configuration-property
The configuration property.

System programmer response:
Ensure that the specified property exists in the specified configuration file.

User response:
No action is required.

IZUG059I **Specify the CEA high level qualifier (HLQ) to use for log snapshot data sets. The HLQ can be 1-4 characters.**

Explanation:
The message prompts for the high level qualifier to use.

System programmer response:
Enter the high level qualifier value to use.

User response:
No action is required.

IZUG060I **Specify the CEA high level qualifier (HLQ) to use for log snapshot data sets. The HLQ can be 1-4 characters. Or press Enter to accept the default *default-HLQ-mode*:**

Explanation:
The message prompts for the high level qualifier to use.

System programmer response:

Enter the high level qualifier value to use or press Enter to use the specified default value.

User response:
No action is required.

IZUG061I **What security mode do you want to use? To use SAF mode, enter S. To use Repository mode, enter R. Or press Enter to accept the current setting *current-mode*:**

Explanation
The message prompts for the security mode to use.

In the message text:

current-mode
Current security mode for the z/OSMF configuration.

System programmer response:
Enter S to use SAF security mode or R to use Repository mode or press Enter to use the current setting for security mode.

User response:
No action is required.

IZUG062I **What security mode do you want to use? To use SAF mode, enter S. To use Repository mode, enter R:**

Explanation:
The message prompts for the security mode to use.

System programmer response:
Enter S to use SAF security mode or R to use Repository mode.

User response:
No action is required.

IZUG063E **File *file-name* could not be found in *dataset-name*. This file is required for the configuration of Common Event Adapter (CEA) for Incident Log.**

Explanation
The specified file does not exist in specified data set. This file is used by the Incident Log verification to verify the Inicdent Log configuration. As part of the configuration of CEA for Incident Log, this file is copied to the specified target dataset where it will be used to create a test dump for the verification of Incident Log.

In the message text:

file-name
File name.

dataset-name
Data set name.

System programmer response:
Ensure that the specified file exists in the specified data set. Retry your request.

User response:
No action is required.

IZUG064I **Enter the name of the target data set to be used for saving the updated *member-name* parmlib member. Specify the fully qualified data set name, or press Enter to accept the default: *default-member-name*:**

Explanation
The message prompts you for the name of the data set to be used for saving the updated parmlib members, IEADMCnn and CEAPRMnn, which are used for Incident Log task processing. A fully qualified data set name is expected.

In the message text:

member-name
User-specified parmlib member

default-member-name
Default data set name.

System programmer response:
Specify the fully qualified data set name, or press Enter to accept the supplied default if it is correct for your environment. If you specify the data set name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response:
No action is required.

IZUG065I **Enter the name of the target data set to be used for saving the updated *member-name*parmlib member. Specify the fully qualified data set name, or press Enter to use SYS1.PARMLIB:**

Explanation
The message prompts you for the name of the data set to be used for saving the updated parmlib members, IEADMCnn and CEAPRMnn, which are used for Incident Log task processing. A fully qualified data set name is expected.

In the message text:

member-name
User-specified PARMLIB member.

System programmer response:
Specify the fully qualified data set name, or press Enter to save the updated member in SYS1.PARMLIB. If you specify the data set name in quotes, the quotes

are ignored. Your input is stored without quotes in the configuration file.

User response:
No action is required.

IZUG066I **Enter the name of the source data set for the IEADMCZM parmlib member. Specify the fully qualified data set name, or press Enter to accept the default *data-set-name*:**

Explanation
The message prompts you for the name of the data set that contains the IEADMCZM parmlib member. This is shipped by default in SYS1.SAMPLIB. A fully qualified data set name is expected.

In the message text:

data-set-name
Default data set name.

System programmer response:
Specify the fully qualified data set name, or press Enter to accept the supplied default if it is correct for your environment. If you specify the data set name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response:
No action is required.

IZUG067I **Enter the name of the source data set for the IEADMCZM parmlib member. Specify the fully qualified data set name, or press Enter to use SYS1.SAMPLIB:**

Explanation:
The message prompts you for the name of the data set that contains the IEADMCZM parmlib member. This is shipped by default in SYS1.SAMPLIB. A fully qualified data set name is expected.

System programmer response:
Specify the fully qualified data set name, or press Enter to use SYS1.SAMPLIB as the source for the IEADMCZM member. If you specify the data set name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response:
No action is required.

IZUG068W **The configuration property *cfg-prop* was found in file *cfg-ovr-file*. This property will be ignored.**

Explanation
The indicated configuration property was found in either the configuration or override file. The indicated property will be ignored since the property can only be set by manually exporting it or through the use of the environment file specified by environment variable IZU_ENV_FILE.

In the message text:

cfg-prop
Name of the property.

cfg-ovr-file
The configuration or override file.

System programmer response:
If the intent was to set the specified property, either update the file specified by IZU_ENV_FILE with the property and then export IZU_ENV_FILE OR manually export the property prior to calling the script. Otherwise, no action is required.

User response:
No action is required.

IZUG069I **The configuration property *cfg-prop* is set to the value *cfg-val*.**

Explanation
The indicated configuration property is set to the indicated value.

In the message text:

cfg-prop
Name of the property.

cfg-val
Value of the property.

System programmer response:
No action is required.

User response:
No action is required.

IZUG070I **If you have AUTOGID enabled, RACF can assign unused GIDs for your group ids. Do you want RACF to automatically assign GIDs to groups created by z/OSMF? For yes, enter Y. For no, enter N:**

Explanation:
RACF can automatically assign unused GIDs to your group ids if AUTOGID is enabled. If selected, all GID properties in the configuration file will be set to AUTOGID. This can also reduce the number of prompts for UIDs.

System programmer response:
Enter Y to have RACF automatically assign unused GIDs for your z/OSMF created group ids or enter N to assign your own.

User response:
No action is required.

IZUG071I If you have AUTOGID enabled, RACF can assign unused GIDs for your group ids. Do you want RACF to automatically assign GIDs to groups created by z/OSMF? For yes, enter Y. For no, enter N. Or press Enter to accept the default *default-value*:

Explanation

RACF can automatically assign unused GIDs to your group ids if AUTOGID is enabled. If selected, all GID properties in the configuration file will be set to AUTOGID. This can also reduce the number of prompts for UIDs.

In the message text:

default-value
The default value to use.

System programmer response:

Enter Y to have RACF automatically assign unused GIDs for your z/OSMF created group ids or enter N to assign your own.

User response:

No action is required.

IZUG072I If you have AUTOUID enabled, RACF can assign unused UIDs for your user ids. Do you want RACF to automatically assign UIDs to user ids created by z/OSMF? For yes, enter Y. For no, enter N:

Explanation:

RACF can automatically assign unused UIDs to your user ids if AUTOUID is enabled. If selected, all UID properties in the configuration file will be set to AUTOUID. This can also reduce the number of prompts for UIDs.

System programmer response:

Enter Y to have RACF automatically assign unused UIDs for your z/OSMF created user ids or enter N to assign your own.

User response:

No action is required.

IZUG073I If you have AUTOUID enabled, RACF can assign unused UIDs for your user ids. Do you want RACF to automatically assign UIDs to user ids created by z/OSMF? For yes, enter Y. For no, enter N. Or press Enter to accept the default *default-value*:

Explanation

RACF can automatically assign unused UIDs to your user ids if AUTOUID is enabled. If selected, all UID properties in the configuration file will be set to AUTOUID. This can also reduce the number of prompts for UIDs.

In the message text:

default-value
The default value to use.

System programmer response:

Enter Y to have RACF automatically assign unused UIDs for your z/OSMF created user ids or enter N to assign your own.

User response:

No action is required.

IZUG074I Clearing cached content for z/OSMF online help at location: *help-dir*.

Explanation

While processing your request, z/OSMF deployed or redeployed one or more plug-ins. This activity includes the deletion of the contents of the z/OSMF online help directory. This processing is normal.

In the message text:

help-dir
Name of the directory to be processed.

System programmer response:

No action is required.

User response:

No action is required.

IZUG075I Environment file *env-file*has been sourced.

Explanation

The indicated environment file has been sourced.

In the message text:

env-file
Name of the environment file.

System programmer response:

No action is required.

User response:

No action is required.

IZUG076E An unexpected error occurred.

Explanation:

An error occurred, but the cause could not be determined.

System programmer response:

Check the job log for any other messages that might indicate a reason for this error. If the log messages do not explain the cause of the problem, contact IBM Support for assistance.

User response:
No action is required.

IZUG077E **The value specified for *attribute* is not valid. The value must start with an alpha character (A-Z, a-z) or a special character (# $ @) and must contain *number*characters.**

Explanation
The value specified for the variable is not valid.

In the message text:

attribute
Attribute for the prompt.

number
Minimum and maximum number of characters the variable can contain.

System programmer response:
Enter a value that starts with an alpha character (A-Z, a-z) or a special character (# $ @) and contains between the minimum and maximum number of characters specified.

User response:
No action is required.

IZUG078E **File *file-name*does not exist. This file is required for the configuration of Common Event Adapter (CEA) for Incident Log.**

Explanation
The specified file does not exist. This file is required for the configuration of the Incident Log plug-in.

In the message text:

file-name
File name.

System programmer response:
Ensure that the specified file exists. Retry your request.

User response:
No action is required.

IZUG079E **File *file-name*could not be found in SYS1.SAMPLIB. This file is required for the configuration of Common Event Adapter (CEA) for Incident Log.**

Explanation
The specified file does not exist in SYS1.SAMPLIB. This file is used by the Incident Log verification to verify the Inicdent Log configuration. As part of the configuration of CEA for Incident Log, this file is copied to the specified target dataset where it will be used to create a test dump for the verification of Incident Log.

In the message text:

file-name
File name.

System programmer response:
Ensure that the specified file exists in SYS1.SAMPLIB. Retry your request.

User response:
No action is required.

IZUG080I **All of the available z/OSMF plug-ins have been configured already.**

Explanation:
All of the plug-ins that were shipped with z/OSMF have been configured with the product already. No other plug-ins remain to be configured.

System programmer response:
No action is required.

User response:
No action is required.

IZUG081E **The plug-in -add request cannot be performed because the specified configuration file *file-name*was not found. This file is required for adding plug-ins.**

Explanation
The request to add one or more plug-ins could not be completed because the specified input configuration file was not found. This file is required for configuring plug-ins on your system.

In the message text:

file-name
Name of the configuration file.

System programmer response:
Ensure that the specified configuration file exists. If not, recreate the configuration file with the values for your existing z/OSMF configuration. Retry your request.

User response:
No action is required.

IZUG082E **File system *file-system-name* at mount point *file-system-mount-point*must be a ZFS or HFS file**

system and must be mounted in read-write mode.

Explanation

The specified file system at the specified mount point must be of type ZFS or HFS and must be mounted in read-write mode. This can be done by specifying rdwr for the mode when mounting the filesystem.

In the message text:

file-system-name
Name of the file system.

file-system-mount-point
The mount point of the file system.

System programmer response:
Ensure the file system is a ZFS or HFS. Also, ensure that the file system is mounted in read-write mode.

User response:
No action is required.

IZUG083I **The verification of *verify-type*has completed successfully.**

Explanation

The verification request completed.

In the message text:

verify-type
Type of verification that was requested.

System programmer response:
No action is required.

User response:
No action is required.

IZUG084W **The IZU_DATA_DIR variable, which identifies the mount point of the z/OSMF data file system, has been reset to the default value *mount-point*.**

Explanation

The z/OSMF configuration process has updated the IZU_DATA_DIR variable in your configuration file to the default value of /global/zosmf. In old releases of z/OSMF, the z/OSMF data file system was mounted at /var/zosmf by default.

In the message text:

mount-point
Default mount point for the z/OSMF data file system.

System programmer response:
Determine whether the z/OSMF data file system on your system is currently mounted at the old default location /var/zosmf. If so, unmount it. You can remount the data file system manually at the new location /global/zosmf or you can allow z/OSMF processing to mount it at this location during the processing of the izusetup.sh -config script.

User response:
No action is required.

IZUG085I **The IZU_IL_CONFIGURE variable must be set to Y before completing action *action*.**

Explanation

The IZU_IL_CONFIGURE variable in the configuration file must be set to Y before the specified action can be completed.

In the message text:

action
The Incident Log action to be completed.

System programmer response:
Enter the `izusetup.sh -config [ filename.cfg ]` command, specifying as input the configuration file that you used previously for setting up z/OSMF. If you omit this file name, the IBM-supplied configuration file (izudflt.cfg) is used. Then, when prompted to configure the Incident Log, enter Y.

User response:
No action is required.

IZUG086E **The Incident Log configuration request failed. The IZU_IL_CEA_CONFIGURE variable in the configuration file must be set to Y before the request can be processed.**

Explanation:

The Incident Log configuration request failed because the IZU_IL_CEA_CONFIGURE variable is not set to Y.

System programmer response:
Enter the `izusetup.sh -config [ filename.cfg ]` command. The configuration file name is optional. If you omit this file name, the IBM-supplied configuration file (izudflt.cfg) is used. Then, when prompted to configure the Incident Log, enter Y.

User response:
No action is required.

IZUG087I **The IZU_IL_CEA_CONFIGURE variable must be set to Y before completing action *action*.**

Explanation

The IZU_IL_CEA_CONFIGURE environment variable in the configuration file must be set to Y before the specified action can be completed.

In the message text:

action
The Incident Log action to be completed.

System programmer response:
Enter the `izusetup.sh -config [ filename.cfg ]` command. Use the configuration file that you used previously for setting up z/OSMF. If you omit this file name, the IBM-supplied configuration file (izudflt.cfg) is used. Then, when prompted to configure the Incident Log, enter Y.

User response:
No action is required.

IZUG088E **The required environment variable *env-var*is not set.**

Explanation
For script processing, z/OSMF requires that the indicated environment variable be set to a valid value. However, no value was found for the variable.

In the message text:

env-var
Name of the variable that was not set.

System programmer response:
A serious error has occured. Contact IBM Support.

User response:
No action is required.

IZUG089E **Directory *directory-name*must be writable.**

Explanation
Processing of the script has stopped. For processing to continue, the indicated directory must be writable.

In the message text:

directory-name
Name of the directory.

System programmer response:
Ensure that the user running the script has permission to write to the directory. After correcting the error, have the user run the script again.

User response:
No action is required.

IZUG090I **Environment variable *env-var* has been set to the default value *env-value*.**

Explanation
The indicated environment variable has been set to the specified default value.

In the message text:

env-var
Name of the variable.

env-value
Value of the variable.

System programmer response:
No action is required.

User response:
No action is required.

IZUG091I **Environment variable *env-var* is set to the value *env-value*.**

Explanation
The indicated environment variable is set to the indicated value.

In the message text:

env-var
Name of the variable.

env-value
Value of the variable.

System programmer response:
No action is required.

User response:
No action is required.

IZUG092E **Path /usr/lib was not found in LIBPATH variable in file *file-name*.**

Explanation
The path /usr/lib was not found in the LIBPATH variable in the specified file.

In the message text:

file-name
Name of the file that was processed.

System programmer response:
Ensure that the path /usr/lib in LIBPATH environment variable is set in the specified file.

User response:
No action is required.

IZUG093I **The directory *tmpdir-value*will be used for storing temporary files.**

Explanation
z/OSMF processing will use the indicated directory for storing temporary files.

In the message text:

tmpdir-value
Temporary directory value.

System programmer response:
No action is required.

User response:
No action is required.

IZUG094I In the previous configuration of z/OSMF, you allowed z/OSMF to configure the Common Information Model (CIM) server. In the current release of z/OSMF, the CIM configuration procedure is modified.

Explanation:
The procedure for configuring the CIM server has been modified in the current release of z/OSMF.

System programmer response:
No action is required.

User response:
No action is required.

IZUG095I The Common Information Model (CIM) server must be configured and started before proceeding with configuration.

Explanation:
After reviewing the RACF instructions for the CIM server, and running the exec, your installation must configure and start the CIM server before proceeding with the configuration of z/OSMF.

System programmer response:
Review the contents of the RACF exec that was created by the z/OSMF configuration process and run the exec, if appropriate. Then, configure and start the CIM server. For information about configuring the CIM server, see *z/OS Common Information Model User's Guide* , SC33-7998, which is available on-line in the IBM z/OS Internet Library.

User response:
No action is required.

IZUG096I Do you need assistance in setting up security for the Common Information Model (CIM) server? To have z/OSMF create an exec with sample RACF commands, enter Y. Otherwise, enter N.

Explanation:
The z/OSMF configuration process includes the option of creating a REXX exec with sample RACF commands. Your security administrator can use these commands for authorizing z/OSMF users to the CIM server.

System programmer response:
To allow z/OSMF to create this exec, enter Y in response to this prompt. Otherwise, enter N.

User response:
No action is required.

IZUG097I Do you need assistance in setting up security for the Common Information Model (CIM) server? To have z/OSMF create an exec with sample RACF commands, enter Y. For no, enter N. Press Enter to accept the default *value*:

Explanation
The z/OSMF configuration process includes the option of creating a REXX exec with sample RACF commands. Your security administrator can use these commands for authorizing z/OSMF users to the CIM server.

In the message text:

value
Default for whether to set up RACF security for the CIM server.

System programmer response:
Enter Y or N, or accept the default value.

User response:
No action is required.

IZUG098E Unable to remove file *file-name*.

Explanation
z/OSMF processing of the izusetup.sh -finish request was unable to remove the indicated file. Possibly, the file is marked read-only or has permissions that do not allow for write access.

In the message text:

file-name
File that could not be removed.

System programmer response:
Ensure that the specified file exists. Ensure that the file and the file directory have permissions that allow for write access. Also, verify that the user ID for the request has update access to the file and its directory. Then, retry your request.

User response:
No action is required.

IZUG099W File *file-name*does not exist.

Explanation
In processing a izusetup.sh -config request, z/OSMF did not find the indicated file. If the file is needed, z/OSMF processing will create it using IBM defaults.

In the message text:

file-name
File that does not exist.

System programmer response:
No action is required.

User response:
If you are running the izusetup.sh script in interactive mode, the script will prompt you for a number of installation-specific values needed for configuration. In response to each prompt, you must either press Enter to use the default value, or type your installation specific value. Ensure that these values are appropriate for your setup. If you are running the script in fastpath mode, check the override file to ensure that the appropriate values have been specified for your installation.

IZUG100E Unable to register provider *name*.

Explanation
The specified provider could not be registered. Typically, this error occurs when the user is not authorized to write to the Common Information Model (CIM) server repository or when the providers are missing.

In the message text:

name
Name of the provider.

System programmer response:
Verify that the user is authorized to write to the Common Information Model (CIM) server repository. Ensure that the providers are available.

User response:
No action is required.

IZUG101W The file or parmlib member was not overwritten.

Explanation:
The specified file or parmlib member was not overwritten.

System programmer response:
No action is required.

User response:
No action is required.

IZUG102E The request to start the Common Information Model (CIM) server failed because the server is already running.

Explanation:
The Common Information Model (CIM) server could not be started because it is already running.

System programmer response:
Shutdown the CIM server by entering the `cimserver -s` command. Then, re-run the script.

User response:
No action is required.

IZUG104I Provider *name*module has already been registered with the Common Information Model (CIM) server.

Explanation
The specified provider module is already registered with the Common Information Model (CIM) server.

In the message text:

name
Name of the provider.

System programmer response:
No action is required.

User response:
No action is required.

IZUG105W Provider *name*module is not registered with the Common Information Model (CIM) server.

Explanation
The specified provider module is not registered with the Common Information Model (CIM) server. The script will register it.

In the message text:

name
Name of the provider.

System programmer response:
No action is required.

User response:
No action is required.

IZUG106I The provider *name*module is being registered with the Common Information Model (CIM) server.

Explanation
The provider module is not registered with the Common Information Model (CIM) server; therefore, the script is registering it.

In the message text:

name
Name of the provider.

System programmer response:
No action is required.

User response:
No action is required.

IZUG107E Unable to register provider *name*module.

Explanation
The specified provider module could not be registered. Typically, this error occurs when the user is not authorized to write to the Common Information Model (CIM) server repository or when the providers are missing.

In the message text:

name
Name of the provider.

System programmer response:
Verify that the z/OSMF administrator is authorized to write to the Common Information Model (CIM) server repository. Ensure that the providers are available.

User response:
No action is required.

IZUG108W **The temporary directory *directory-name*specified for environment variable TMPDIR does not exist or cannot be accessed. The directory /tmp will be used.**

Explanation
The specified temporary directory either could not be found or is not writable. Thus, the directory /tmp will be used.

In the message text:

directory-name
Name of the directory specified for the TMPDIR environment variable.

System programmer response:
Verify that the directory exists. Ensure that the user running the script has permission to write to the directory.

User response:
No action is required.

IZUG109E **Temporary directory *directory-name*must exist and be writable: exiting script.**

Explanation
For script processing, the named temporary directory must exist and be writable. If these requirements are not satisfied, processing of the script stops.

In the message text:

directory-name
Name of the temporary directory.

System programmer response:
Verify that the directory exists. Ensure that the user running the script has permission to write to the directory. After correcting the error, run the script again.

User response:
No action is required.

IZUG110I **The IZU_INCIDENT_LOG environment variable must be set to Y before completing action *action*.**

Explanation
The IZU_INCIDENT_LOG environment variable in the configuration file must be set to Y before the specified action can be completed.

In the message text:

action
The Incident Log action to be completed.

System programmer response:
Enter the `izusetup.sh -config [ filename.cfg ]` command. Use the configuration file that you used for setup. If the file name is omitted, the default configuration file is used. When prompted to configure the Incident Log, enter Y.

User response:
No action is required.

IZUG111E **The value specified for variable *variable-name* is not valid. The variable must start with an alphanumeric character (A-Z, a-z, and 0-9) or a special character (# $ @) and must contain *number*characters.**

Explanation
The value specified for the variable is not valid.

In the message text:

variable-name
Name of the input variable.

number
Minimum and maximum number of characters the variable can contain.

System programmer response:
Enter a value that starts with an alphanumeric character (A-Z, a-z, and 0-9) or a special character (# $ @) and contains between the minimum and maximum number of characters specified.

User response:
No action is required.

IZUG112I **Script *script-name* returned with reason code *code*.**

Explanation
The specified script returned with the specified reason code.

In the message text:

script-name
Name of the script.

code
Reason code.

System programmer response:
If the reason code is not 0, check the log for errors.

User response:
No action is required.

IZUG113I **The output of the command that was passed to script *script-name* is *output*.**

Explanation
The output of the command that was passed to the specified script is displayed.

In the message text:

script-name
Name of the script.

output
The output of the command.

System programmer response:
No action is required.

User response:
No action is required.

IZUG114I **Command *command-name* was passed to script *script-name*.**

Explanation
The specified command was passed to the specified script.

In the message text:

command-name
The command to execute.

script-name
Name of the script.

System programmer response:
No action is required.

User response:
No action is required.

IZUG115I **The RACF REXX executable was generated and saved in file *file-name*. Review and execute the script before proceeding.**

Explanation
The RACF REXX executable has been created and saved in the specified file. The script sets up the RACF security for z/OSMF.

In the message text:

file-name
Name of the file in which the RACF REXX executable is stored.

System programmer response:
Review and execute the script. If you do not set up the security, you cannot proceed.

User response:
No action is required.

IZUG116E **User *user-name*does not exist.**

Explanation
The specified user does not exist.

In the message text:

user-name
User ID of the user.

System programmer response:
Provide a valid user name and try your request again.

User response:
No action is required.

IZUG117I **A *action*of the test incident for the Incident Log has occurred.**

Explanation
To verify that the Incident Log is configured properly, a test incident is created. Then, a series of tests are run against the incident. After verification is complete, the test incident is deleted. This message indicates that the test incident is either being created or that it is being deleted.

In the message text:

action
The action being performed as part of Incident Log verification.

System programmer response:
No action is required.

User response:
No action is required.

IZUG118I **Checking Incident Log dependencies.**

Explanation:
The PDW_IVP is being called to determine the status of Incident Log dependencies on the system.

System programmer response:
No action is required.

User response:
No action is required.

IZUG119I Obtaining data for dependency *dependency-name*.

Explanation

Dependency data is being collected for either the SysplexDumpDirectory provider or PDWLogstream provider.

In the message text:

dependency-name
Name of the Incident Log dependency.

System programmer response:
No action is required.

User response:
No action is required.

IZUG120I Creating Incident Log report *report-name*.

Explanation

The specified Incident Log report is being created.

In the message text:

report-name
Name of the Incident Log report.

System programmer response:
No action is required.

User response:
No action is required.

IZUG121I To obtain the results of the Incident Log verification, review report *report-name*.

Explanation

Review the Incident Log report to obtain the results of the verification.

In the message text:

report-name
Name of the Incident Log report.

System programmer response:
Review the specified report.

User response:
No action is required.

IZUG122E Verification failed for *item-name*.

Explanation

Verification failed because an error occurred while the specified item was being verified.

In the message text:

item-name
The item being verified.

System programmer response:
For more information, review the log file created for the error.

User response:
No action is required.

IZUG123E An error occurred. The Common Event Adapter (CEA) parmlib member was not activated.

Explanation:
The CEA parmlib member was not activated because an error occurred.

System programmer response:
For more information, review the log file created for the error.

User response:
No action is required.

IZUG124I The Common Event Adapter (CEA) parmlib member *member-name*is being activated.

Explanation

The specified CEA parmlib member is being activated on the system.

In the message text:

member-name
Name of the CEA parmlib member.

System programmer response:
No action is required.

User response:
No action is required.

IZUG126E An error occurred. Variable *variable-name* is set to value *actual-value*. The expected value is *expected value*.

Explanation

The specified variable is set to the specified value. The variable must be set to the expected value.

In the message text:

variable-name
Name of the variable.

actual-value
Actual value specified for the variable.

expected value
Value to which z/OSMF expects the variable to be set.

System programmer response:
For more information, review the log file created for the error and the RACF report.

User response:
No action is required.

IZUG127E **User *user-name* not connected to group *group-name*.**

Explanation
The specified user is not connected to the specified group.

In the message text:

user-name
User ID of the user.

group-name
Name of the group.

System programmer response:
For more information, review the log file created for the error and the RACF report.

User response:
No action is required.

IZUG128E **User *user-name* not permitted to RACF class *class-name*.**

Explanation
The specified user or group name is not permitted to the specified RACF class.

In the message text:

user-name
User ID of the user.

class-name
Name of the RACF class.

System programmer response:
For more information, review the log file created for the error and the RACF report.

User response:
No action is required.

IZUG129E **Unable to allocate the sysplex dump directory.**

Explanation:
The sysplex dump directory could not be allocated.

System programmer response:
For more information, review the log file created for the error.

User response:
No action is required.

IZUG130I **Allocating sysplex dump directory on volume *volume-name*.**

Explanation
The sysplex dump directory is being allocated on the specified volume.

In the message text:

volume-name
Name of the volume.

System programmer response:
No action is required.

User response:
No action is required.

IZUG131I **Activating sysplex dump directory.**

Explanation:
The sysplex dump directory is being activated.

System programmer response:
No action is required.

User response:
No action is required.

IZUG132E **Unable to activate sysplex dump directory.**

Explanation:
The sysplex dump directory could not be activated.

System programmer response:
For more information, review the log file created for the error.

User response:
No action is required.

IZUG133I **Enter the cluster transition name (case sensitive) for the server:**

Explanation:
Indicate the cluster transition name to be used. The name is case sensitive.

System programmer response:
Enter the cluster transition name.

User response:
No action is required.

IZUG134I **Enter the cluster transition name (case sensitive) for the server, or press Enter to accept the default *cluster-name*:**

Explanation
Indicate the cluster transition name to be used.

In the message text:

cluster-name
The default cluster transition name.

System programmer response:
To use the default cluster transition name, press Enter without entering a value. Otherwise, enter the name of the cluster transition.

User response:

No action is required.

IZUG135W **File *file-name*already exists. Ensure that the environment variables specified in the file have the same value as the corresponding variables in the configuration file.**

Explanation
The specified file already exists.

In the message text:

file-name
Name of the file.

System programmer response:
Ensure that the environment variables specified in the file have the same values as the corresponding variables in the configuration file. After you compare the variables and make any corrections, you can continue.

User response:
No action is required.

IZUG136I **The *item-type file-name*was created.**

Explanation
The specified file or directory has been created.

In the message text:

item-type
Type of item being created: file or directory.

file-name
Name of the file or directory.

System programmer response:
No action is required.

User response:
No action is required.

IZUG137E **File *file-name*already exists. The value specified in the file for the PEGASUS_HOME environment variable does not match the value specified in the configuration file for the IZU_WBEM_ROOT variable.**

Explanation
The specified file already exists. An error occurred because the PEGASUS_HOME variable specified in the file does not have the same value as the IZU_WBEM_ROOT variable specified in the configuration file. The values for these two variables must be the same.

In the message text:

file-name
Name of the file.

System programmer response:
Update the specified file so that the PEGASUS_HOME variable has the same value as the IZU_WBEM_ROOT variable in the configuration file.

User response:
No action is required.

IZUG138E **Unable to read file *file-name*.**

Explanation
The permissions specified for the file does not allow read access.

In the message text:

file-name
Name of the file.

System programmer response:
Enable read access for the file.

User response:
No action is required.

IZUG139I **Has the Common Information Model (CIM) server been setup? [Y|N]:**

Explanation:
The message prompts to determine if the Common Information Model (CIM) server has been set up.

System programmer response:
Enter Y or N.

User response:
No action is required.

IZUG140I **Has the Common Information Model (CIM) server been setup? [Y/N]. Or press Enter to accept the default *value*:**

Explanation
The message prompts to determine if the Common Information Model (CIM) server has been setup. A default value is provided.

In the message text:

value
The default response value for the CIM setup option.

System programmer response:
Enter Y or N, or accept the default. Default is NO

User response:
No action is required.

IZUG141W No data directory specified. Using *directory-name*as the data directory.

Explanation

The message indicates that no data directory was specified and that the default data directory will be used.

In the message text:

directory-name
The default data directory.

System programmer response:
Ensure the default data directory use is correct to the configuration.

User response:
No action is required.

IZUG142I Enter the name of the target data set to be used for saving the updated parmlib members *ceaprm-parmlib-member* and *ieadmc-parmlib-member*. Specify the fully qualified data set name, or press Enter to accept the default: *parmlib-name*:

Explanation

The message prompts you for the name of the data set to be used for saving the updated parmlib members, IEADMCnn and CEAPRMnn, which are used for Incident Log task processing. A fully qualified data set name is expected.

In the message text:

ceaprm-parmlib-member
User-specified CEAPRMxx member

ieadmc-parmlib-member
The user-specified IEADMCxx member

parmlib-name
Default data set name.

System programmer response:
Specify the fully qualified data set name, or press Enter to accept the supplied default if it is correct for your environment. If you specify the data set name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response:
No action is required.

IZUG143I Enter the name of the target data set to be used for saving the updated parmlib members *ceaprm-parmlib-member* and *ieadmc-parmlib-member*. Specify the fully qualified data set name, or press Enter to use SYS1.PARMLIB:

Explanation

The message prompts you for the name of the data set to be used for saving the updated parmlib members, IEADMCnn and CEAPRMnn, which are used for Incident Log task processing. A fully qualified data set name is expected.

In the message text:

ceaprm-parmlib-member
User-specified CEAPRMxx member.

ieadmc-parmlib-member
User-specified IEADMCxx member.

System programmer response:
Specify the fully qualified data set name, or press Enter to save the updated members in SYS1.PARMLIB. If you specify the data set name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response:
No action is required.

IZUG144I Enter the mount point for the z/OSMF data file system:

Explanation:
The message prompts for the mount point for where the z/OSMF data file system is to be mounted.

System programmer response:
Enter the mount point for where the z/OSMF data file system is to be mounted.

User response:
No action is required.

IZUG145I Enter the mount point for the z/OSMF data file system, or press Enter to accept the default *mount-point*:

Explanation

The message prompts for the mount point for where the z/OSMF data file system is to be mounted.

In the message text:

mount-point
The default mount point for the z/OSMF data file system.

System programmer response:
Enter the mount point for where the z/OSMF data file system is to be mounted.

User response:
No action is required.

IZUG146I **Invoking script *script-name-options*.**

Explanation

The message displays the script name and options that are being invoked.

In the message text:

script-name-options
The script name and options that are being invoked.

System programmer response:
No action is required.

User response:
No action is required.

IZUG147W **Path /usr/lib not found in LIBPATH variable.**

Explanation:
The message indicates the path /usr/lib was not found in the LIBPATH environment variable.

System programmer response:
Set the path /usr/lib in LIBPATH environment variable.

User response:
No action is required.

IZUG148I **Stopping Common Information Model (CIM) server.**

Explanation:
The message indicates that the CIM server is being stopped.

System programmer response:
No action is required.

User response:
No action is required.

IZUG149W **Path /usr/lib not found in LIBPATH variable in file *file-name*.**

Explanation

The message indicates the path /usr/lib was not found in the LIBPATH variable in the specified file.

In the message text:

file-name
The name of the file being checked.

System programmer response:
Ensure the path /usr/lib in LIBPATH environment variable is set in the specified file.

User response:
No action is required.

IZUG150E **Mount point *mount-point*must be a fully-qualified path name.**

Explanation

The message indicates the mount point provided is not a fully-qualified path.

In the message text:

mount-point
The mount point for the file system.

System programmer response:
Provide a fully-qualified path.

User response:
No action is required.

IZUG151I **z/OSMF data file system will be created using SMS managed storage.**

Explanation:
This message confirms your selection to use the z/OS storage management subsystem (SMS) to manage the storage of the z/OSMF data file system.

System programmer response:
No action is required.

User response:
No action is required.

IZUG157I **Enter the z/OSMF data file system type for the file system: *file-system-name*, or press Enter to accept the default *file-system-type*:**

Explanation

This message prompts for the type (zfs or hfs) of the specified file system. A default value is provided.

In the message text:

file-system-name
Name of the file system

file-system-type
Default file system type.

System programmer response:
No action is required.

User response:
No action is required.

IZUG158I **Enter the name of the volume to use for creating the z/OSMF data file system, enter an asterisk (*) to use SMS managed storage, or press Enter to accept the default *volume-name*:**

Explanation

The message prompts you for the name of the volume to create the z/OSMF data file system. To have the z/OS storage management subsystem (SMS) manage the storage, enter an asterisk (*). A default value is provided.

In the message text:

volume-name
Default volume name.

System programmer response:
Perform the requested action. If you specify a volume, the volume must be on-line. If you specify SMS managed storage, ensure that you have an automatic class selection (ACS) routine in place to assign the appropriate SMS construct, based on the name of the data set to be used for the z/OSMF file system.

User response:
No action is required.

IZUG159I **Enter the size (in cylinders) to allocate for the data file system, or press Enter to accept the default *file-system-size*:**

Explanation
Enter the initial space allocation, in cylinders, for the z/OSMF data file system. z/OSMF uses 90 percent of this value for the primary allocation and 10 percent for the secondary allocation. The minimum suggested size is 100 cylinders, which causes the script to use 90 cylinders for the primary allocation and 10 cylinders for the secondary allocation. A default value is provided.

In the message text:

file-system-size
Default size for the file system.

System programmer response:
Perform the requested action.

User response:
No action is required.

IZUG160E **The file extension specified for the override file is incorrect. The file must have a .ovr extension.**

Explanation:
An error occurred because the specified override file does not have a .ovr extension.

System programmer response:
Modify the override file name so that it has the .ovr extension.

User response:
No action is required.

IZUG161E **Directory *directory-name*must be a fully-qualified path name.**

Explanation
The message indicates that the directory provided is not a fully-qualified path.

In the message text:

directory-name
Name of the directory.

System programmer response:
Provide a fully-qualified path.

User response:
No action is required.

IZUG162I **Select the plug-ins to be configured. Multiple plug-ins can be selected by separating plug-ins with a comma.**

Explanation:
The message indicates that multiple plug-ins may be selected by separating plug-in ids with a comma.

System programmer response:
No action is required.

User response:
No action is required.

IZUG163I **Select *plug-in-id* to configure *plug-in-name*.**

Explanation
The message indicates the plug-in ID and plug-in name for selection.

In the message text:

plug-in-id
Identifier of the plug-in

plug-in-name
Name of the plug-in.

System programmer response:
No action is required.

User response:
No action is required.

IZUG164I **Which plug-ins do you want to configure?**

Explanation:
Enter the plug-in IDs for selection. For multiple selections, separate plug-in IDs with a comma.

System programmer response:
Select the plug-in ids for configuration.

User response:
No action is required.

IZUG165I **You have selected to configure *plug-in-name*.**

Explanation
The message indicates the specified plug-in was selected for configuration.

In the message text:

plug-in-name
Name of the plug-in.

System programmer response:
No action is required.

User response:
No action is required.

IZUG166I **No configuration prompts are required for the plug-in *plug-in-name*.**

Explanation
The message indicates there are no prompts to be displayed for the selected plug-in.

In the message text:

plug-in-name
Name of the plug-in.

System programmer response:
No action is required.

User response:
No action is required.

IZUG167E **Value *plug-in-id*is ignored. Plug-in was already selected.**

Explanation
The plug-in ID is ignored because the plug-in has already been selected for configuration.

In the message text:

plug-in-id
Plug-in ID.

System programmer response:
No action is required.

User response:
No action is required.

IZUG168E **Expecting *number*arguments.**

Explanation
The message indicates the value that represents the number of plug-ins is incorrect.

In the message text:

number
Number of plug-ins.

System programmer response:
No action is required.

User response:
No action is required.

IZUG169E **Configuration file variable *variable-name*is not valid.**

Explanation
The message indicates the configuration file variable is not valid.

In the message text:

variable-name
The configuration file variable.

System programmer response:
No action is required.

User response:
No action is required.

IZUG170E **Log file variable *variable-name*is not valid.**

Explanation
The message indicates the log file is not valid.

In the message text:

variable-name
Log file variable.

System programmer response:
No action is required.

User response:
No action is required.

IZUG171I **Do you want to configure the Common Information Model (CIM) server as part of z/OSMF customization? If so, enter Y. To skip this step, enter N:**

Explanation:
Specify whether the z/OS Common Information Model (CIM) server is to be configured as part of the z/OSMF configuration process. z/OSMF requires that the CIM server be operational on your system. To have z/OSMF configure the CIM server for you, enter Y. Otherwise, if you have already configured the CIM server or plan to do this step yourself, specify N.

System programmer response:
Enter Y or N.

User response:
No action is required.

IZUG172I **Do you want to configure the Common Information Model (CIM) server as part of z/OSMF customization? If so, enter Y. To skip this step, enter N. To accept the default, press Enter: *value*:**

Explanation
Specify whether the z/OS Common Information Model (CIM) server is to be configured as part of the z/OSMF configuration process. z/OSMF requires that the CIM server be operational on your system. To have z/OSMF configure the CIM server for you, enter Y. Otherwise, if you have already configured the CIM server or plan to do this step manually, specify N. To accept the default value displayed in the message, press Enter.

In the message text:

value
Default selection for setting up the CIM server.

System programmer response:
Enter Y or N, or accept the default value.

User response:
No action is required.

IZUG173I Enter "N" to select none of these plug-ins.

Explanation:
The value N indicates that no plug-ins are selected.

System programmer response:
No action is required.

User response:
No action is required.

IZUG174E The value *value* is incorrect for *property*.

Explanation
The specified value is incorrect for the indicated property. During the configuration process, the izusetup.sh script collects installation-specific data that is used in the configuration of the product. The script starts with the variable settings that are contained in the configuration file (izudflt.cfg), and substitutes any installation-specific changes that you supply (through interactive prompting or an optional override file) to tailor the configuration for your environment.

In the message text:

value
Value that was specified for the property

property
Property containing the value.

System programmer response:
Specify a valid value for the indicated property and retry the operation. Depending on how you choose to configure z/OSMF, you might need to respecify this value interactively or as a setting in the optional override file. Some values are case sensitive. For more information, see IBM z/OS Management Facility Configuration Guide . Do not edit the izudflt.cfg file directly.

User response:
No action is required.

IZUG175I The configuration file *config-file* will be migrated to the format: *release-level*. Enter the *release-level* z/OSMF product file system mount point, or press Enter to accept the default path *default-code-root*:

Explanation:
The specified configuration file will be migrated to the specified release level. This message prompts for the default code root directory.

System programmer response:
Enter the root code directory path or press Enter to accept the default.

User response:
No action is required.

IZUG176I The configuration file *config-file* conforms to the expected format: *release-level*. No migration will be performed.

Explanation:
No migration is needed since the specified configuration file is at the correct version level.

System programmer response:
No action is required.

User response:
No action is required.

IZUG177I The configuration file *config-file* has been migrated to the format: *release-level*.

Explanation:
The specified configuration file has been migrated to the specified release level.

System programmer response:
No action is required.

User response:
No action is required.

IZUG178I The input configuration file *config-file* was saved to a backup file *back-up-config-file*.

Explanation:
The data of the source configuration file has been saved to the specified configuration file.

System programmer response:
No action is required.

User response:
No action is required.

IZUG179E Unable to back up configuration data.

Explanation:
The data of the source configuration file could not be saved. Ensure that the permission settings are correct for the file and directory.

System programmer response:
Ensure that the permission settings are correct for the file and directory.

User response:
No action is required.

IZUG180E The configuration file *config-file* does not conform to the expected format: *release-level*. Migrate the configuration file to the correct format and retry the operation.

Explanation:
The configuration file is not at the correct release level.

System programmer response:
Migrate the configuration file to the correct release level and retry the request.

User response:
No action is required.

IZUG181E The value for the property *plugin-property* is set inconsistently in the configuration file and the override file. In the configuration file, *plugin-property* is set to *plugin-property-value*. In the override file, *plugin-property* is set to *plugin-property-value*.

Explanation
In processing a izusetup.sh -add request, z/OSMF detected that the indicated property is specified inconsistently in the configuration file and the override file.

In the message text:

plugin-property
The property name

plugin-property
The property for the plug-in.

plugin-property-value
The value for the property for the plug-in.

plugin-property
The property for the plug-in.

plugin-property-value
The value for the property for the plug-in.

System programmer response:
Update the property with the correct value in the configuration file and in the override file. Then, retry the request.

User response:
No action is required.

IZUG182I The property *plugin-property* is set inconsistently in the configuration file and the override file. The property *plugin-property* will be set to *plugin-property-value*.

Explanation
In processing a izusetup.sh -add request, z/OSMF detected that the indicated property is specified inconsistently in the configuration file and the override file. Z/OSMF processing will set the property as indicated in the resulting configuration file.

In the message text:

plugin-property
Property for the plug-in

plugin-property
Property for the plug-in

plugin-property-value
The value for the property for the plug-in.

System programmer response:
No action is required.

User response:

IZUG183I The property *plugin-property* in the override file contains the value *plugin-property-value*. The value for the property *plugin-property* will be set to *plugin-property-value*.

Explanation
The indicated property was set incorrectly in the override file. z/OSMF processing uses a reset value as indicated and ignores the value specified in the override file.

In the message text:

plugin-property
Property for the plug-in

plugin-property-value
Value of the property

plugin-property
The property for the plug-in

plugin-property-value
The new value for the property

System programmer response:

No action is required.

User response:
No action is required.

IZUG184E **The property *plugin-property* in the specified configuration file is set to an incorrect value *plugin-property-value*.**

Explanation
In processing the izusetup.sh -add request, z/OSMF processing detected that the indicated variable was set incorrectly in the specified configuration file.

In the message text:

plugin-property
Property for the plug-in

plugin-property-value
Value that is incorrect

System programmer response:
Check the override file for errors. Some variables are initially set to the following value, which is not a valid setting: NO.DEFAULT.VALUE. Correct the errors and try the request again.

User response:
No action is required.

IZUG185I **Enter the value for the Common Information Model (CIM) server attribute *server-attribute*, or press Enter to accept the default *server-attribute-value*:**

Explanation:
The message prompts for CIM server attribute values.

System programmer response:
Provide the value for the server attribute.

User response:
No action is required.

IZUG186I **You have selected to add the following plug-ins.**

Explanation:
This message precedes the list of one or more plug-ins that have been selected for configuration.

System programmer response:
No action is required.

User response:
No action is required.

IZUG187I **Plug-in: *plug-in-name*.**

Explanation
The specified plug-in has been selected for configuration.

In the message text:

plug-in-name
Name of the plug-in to be added.

System programmer response:
No action is required.

User response:
No action is required.

IZUG188I **To accept these plug-in selections, press Enter. To edit these selections, enter E.**

Explanation:
The message prompts you to confirm your selection of which plug-ins are to be configured. You can change your selection.

System programmer response:
Enter E to modify the selection. Press enter with no value to accept the current selection.

User response:
No action is required.

IZUG189I **No plug-ins were selected for configuration.**

Explanation:
The izusetup.sh -add request identified no plug-ins to be added to the z/OSMF configuration.

System programmer response:
No action is required.

User response:
No action is required.

IZUG190I **The plug-in *plug-in-name* is set to the value *plug-in-value*, this indicates that it is already configured. The request to add this plug-in is ignored.**

Explanation
The plug-in is already configured. Your request is ignored.

In the message text:

plug-in-name
Name of the plug-in

plug-in-value
Value of the plug-in

System programmer response:
No action is required.

User response:
No action is required.

IZUG191I **No security setup procedure is required for the specified plug-ins.**

Explanation:
The RACF setup procedure is not required for the specified plug-ins.

System programmer response:
No action is required.

User response:
No action is required.

IZUG192I **Enter the Common Information Model (CIM) Server attribute *server-attribute*:**

Explanation:
You requested that z/OSMF set this CIM server attribute, but no value was supplied for the attribute in the configuration file or override file. Therefore, the script prompts you for the value.

System programmer response:
Enter the appropriate value for your installation.

User response:
No action is required.

IZUG193E **Group *group-name*does not exist.**

Explanation
In processing the izusetup.sh -verify racf request, z/OSMF detected that the specified group is not defined.

In the message text:

group-name
Name of the group.

System programmer response:
For more information, check the log file created for the error and the RACF report. Also, examine the generated RACF exec to ensure that the indicated group was created.

User response:
No action is required.

IZUG194E **The value for variable *property-name* contains an incorrect character *char-value*.**

Explanation
The specified value is incorrect because it contains an incorrect character.

In the message text:

property-name
The incorrect property.

char-value
The incorrect character within the input value.

System programmer response:
Correct the value.

User response:
No action is required.

IZUG195E **The value for variable *property-name*contains one or more spaces. Enter the value without spaces.**

Explanation
The value specified for the variable is not valid because it contains one or more spaces, which is not allowed.

In the message text:

property-name
Name of the incorrect property.

System programmer response:
Specify a value that does not contain spaces.

User response:
No action is required.

IZUG196E **The variable *property-name* contains an incorrect value *property-value*.**

Explanation
The specified value is incorrect.

In the message text:

property-name
Name of the property.

property-value
Value of the property.

System programmer response:
Correct the value.

User response:
No action is required.

IZUG197E **The file system name *file-system-name*is incorrect. The maximum allowable length is 44 characters.**

Explanation
The specified value is incorrect.

In the message text:

file-system-name
The incorrect value.

System programmer response:
Correct the value.

User response:
No action is required.

IZUG198E **Parmlib data set *parmlib-name*does not exist.**

Explanation
The specified parmlib data set does not exist.

In the message text:

parmlib-name
Parmlib name.

System programmer response:
Ensure that the specified parmlib exists. Retry your request.

User response:
No action is required.

IZUG199W File *file-name*already exists.

Explanation
The specified file already exists. Later during the configuration of CEAPRM parmlib member you will be given the option to overwrite the file.

In the message text:

file-name
File name.

System programmer response:
No action is required.

User response:
No action is required.

IZUG200E z/OSMF *process-name* process failed with return code *return-code*.

Explanation
The specified z/OSMF process failed with the specified return code.

In the message text:

process-name
Name of the z/OSMF process

return-code
Return code indicating the result of the process.

System programmer response:
For more information, review the log file created for the error.

User response:
No action is required.

IZUG201E User *user-id* could not be primed for z/OSMF. The action failed with return code *return-code*.

Explanation
The -prime request failed for the specified user ID. A return code is provided to indicate the cause of the error.

In the message text:

user-id
User ID that could not be processed by the -prime request

return-code
Return code indicating the result of the process.

The following return codes are valid:

1
Usage error.

2
Problem with the log directory.

3
Error writing to the log file.

4
Script encountered an error when running a z/OS UNIX shell command, such as mkdir or cp.

5
A repository already exists.

6
Specified user ID is not defined to the z/OS system.

7
The data directory specified by IZU_DATA_DIR does not exist or is not accessible.

This message is accompanied by one or more related messages with more information about the error.

System programmer response:
For more information, check for related messages. For return code 6, see the z/OSMF log file. After correcting the error, run the script again.

User response:
No action is required.

IZUG202E z/OSMF could not make user *user-name* owner of *directory-file name*.

Explanation
z/OSMF could not make the specified user owner of the specified file or directory.

In the message text:

user-name
User name

directory-file
Indication of directory or file

name
Name of the directory or file.

System programmer response:
Ensure that the caller has permission to set ownership. For more information, review the log file created for the error.

User response:
No action is required.

IZUG203E **The request to set permissions for the files in directory *directory-name*failed.**

Explanation
z/OSMF could not set permissions for the files in the specified directory.

In the message text:

directory-name
Name of the directory.

System programmer response:
Ensure that the caller has permission to set ownership. For more information, review the log file created for the error.

User response:
No action is required.

IZUG204E **The request to set permissions for file *file-name*failed.**

Explanation
z/OSMF could not set permissions for the specified file.

In the message text:

file-name
File name.

System programmer response:
Ensure that the caller has permission to set ownership. For more information, review the log file created for the error.

User response:
No action is required.

IZUG205E **The file extension specified for the configuration file is incorrect. The file must have a .cfg extension.**

Explanation:
An error occurred because the specified configuration file does not have a .cfg extension.

System programmer response:
Modify the configuration file name so that it has the .cfg extension.

User response:
No action is required.

IZUG206E **The variables specified in configuration file *file-name*could not be exported.**

Explanation
The variables included in the specified configuration file were not exported because an error occurred.

In the message text:

file-name
Name of the configuration file.

System programmer response:
For more information, review the log file created for the error.

User response:
No action is required.

IZUG207E **File *file-name*does not exist.**

Explanation
The specified file does not exist.

In the message text:

file-name
File name.

System programmer response:
Ensure that the specified file exists. Retry your request.

User response:
No action is required.

IZUG208E **The configuration file is incomplete. The value for variable *variable-name*is missing.**

Explanation
The request could not be completed because an error occurred. The configuration file is missing the specified information.

In the message text:

variable-name
Name of the variable that is missing from the configuration file.

System programmer response:
Enter the `izusetup.sh -config [ filename.cfg ]` command. *filename.cfg* is the name of the configuration file that is missing the specified data. When prompted, provide a value for the specified variable.

User response:
No action is required.

IZUG209I **Script *script-name* supports one or more of the following input options: *input-options*.**

Explanation
The valid script options are displayed. For information about the script options, see IBM z/OS Management Facility Configuration Guide .

In the message text:

script-name
Name of the script

input-options
Options supported by the script.

System programmer response:
No action is required.

User response:
No action is required.

IZUG210I The script *script-name*has completed.

Explanation
The specified script completed.

In the message text:

script-name
Name of the script.

System programmer response:
No action is required.

User response:
No action is required.

IZUG211E Script *script-name*encountered errors: exiting script.

Explanation
Processing of the script stopped because one or more errors occurred.

In the message text:

script-name
Name of the script.

System programmer response:
For more information, review the log file created for the error. Correct any errors and re-run the script.

User response:
No action is required.

IZUG212E Directory *directory-name*does not exist or is not accessible.

Explanation
The specified directory does not exist or is not accessible.

In the message text:

directory-name
Name of the directory.

System programmer response:
Ensure that the specified directory exists and is accessible. Retry your request.

User response:
No action is required.

IZUG213I Log information will be written to file *file-name*.

Explanation
Log information will be saved to the specified file.

In the message text:

file-name
Name of the file.

System programmer response:
No action is required.

User response:
No action is required.

IZUG214E Failed to create *directory-file directory-file-name*.

Explanation
The specified file or directory could not be created.

In the message text:

directory-file
Directory or file

directory-file-name
Name of the directory or file.

System programmer response:
Ensure that the caller is authorized to create files or directories. For more information, review the log file created for the error.

User response:
No action is required.

IZUG215I Starting z/OSMF *procedure-name*procedure.

Explanation
The specified procedure is being processed.

In the message text:

procedure-name
Name of the procedure.

System programmer response:
No action is required.

User response:
No action is required.

IZUG216E The command is missing one of the required arguments: *argument-name*.

Explanation

The command could not be completed because the specified argument was not found.

In the message text:

argument-name
Name of the argument.

System programmer response:

Re-enter the command and include the missing argument.

User response:

No action is required.

IZUG217E **The command could not be completed because it contains an incorrect argument.**

Explanation:

An incorrect argument was provided with the command. Typically, this error occurs when an argument that is not supported by the command is used or when the argument is misspelled.

System programmer response:

Verify that the correct argument is being used. Ensure that it is spelled correctly. Correct any errors and re-enter the command.

User response:

No action is required.

IZUG218E **The command could not be completed because it contains an incorrect argument *argument-name*.**

Explanation

An incorrect argument was provided with the command. The name of the incorrect argument is provided. Typically, this error occurs when an argument that is not supported by the command is used or when the argument is misspelled.

In the message text:

argument-name
Name of the incorrect argument.

System programmer response:

Verify that the correct argument is being used. Ensure that it is spelled correctly. Correct any errors and enter the command again.

User response:

No action is required.

IZUG220E **The Incident Log configuration request failed. The IZU_INCIDENT_LOG variable in the configuration file must be set to Y before the request can be processed.**

Explanation:

The Incident Log configuration request failed because the IZU_INCIDENT_LOG variable is not set to Y.

System programmer response:

Enter the `izusetup.sh -config [ filename.cfg ]` command. The configuration file name is optional. If the file name is omitted, the default configuration file is used. When prompted to configure the Incident Log, enter Y.

User response:

No action is required.

IZUG221E **A value must be provided for argument *argument-name*.**

Explanation

An error occurred because no value was found for the specified argument.

In the message text:

argument-name
Name of the required argument.

System programmer response:

Correct the input to the request.

User response:

No action is required.

IZUG222E **Unable to update configuration file *file-name*.**

Explanation

The specified configuration file could not be updated.

In the message text:

file-name
Name of the configuration file.

System programmer response:

Ensure that the caller is authorized to update the configuration file. For more information, review the log file created for the error.

User response:

No action is required.

IZUG223I **For more information, review log file *file-name*.**

Explanation

For more information, review the log file created for the error.

In the message text:

file-name
Name of the log file.

System programmer response:
No action is required.

User response:
No action is required.

IZUG224I The configuration data was saved in file *file-name*.

Explanation
The configuration data was saved in the specified file.

In the message text:

file-name
Name of the configuration file.

System programmer response:
No action is required.

User response:
No action is required.

IZUG225E Unable to mount file system *file-system-name*.

Explanation
The specified file system could not be mounted.

In the message text:

file-system-name
Name of the file system.

System programmer response:
For more information, review the log file created for the error.

User response:
No action is required.

IZUG226E Unable to allocate file system *file-system-name*.

Explanation
The specified file system could not be allocated.

In the message text:

file-system-name
Name of the file system.

System programmer response:
For more information, review the log file created for the error.

User response:
No action is required.

IZUG227I Creating *directory-file directory-file-name*.

Explanation
The specified file or directory is being created.

In the message text:

directory-file
Directory or file

directory-file-name
Name of the directory or file.

System programmer response:
No action is required.

User response:
No action is required.

IZUG228I Enter the fully qualified name of the z/OSMF *file-system-type*file system:

Explanation
The message prompts you for the name to be used for the z/OSMF data file system. A fully qualified name is expected.

In the message text:

file-system-type
File system type.

System programmer response:
Specify the fully qualified name of the z/OSMF data file system. If you specify the file system name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response:
No action is required.

IZUG229I Enter the fully qualified name of the z/OSMF *file-system-type* file system, or press Enter to accept the default *value* file system name :

Explanation
The message prompts you for the name to be used for the z/OSMF data file system. A fully qualified name is expected.

In the message text:

file-system-type
File system type.

value
Default file system name.

System programmer response:
Specify the fully qualified name of the z/OSMF data file system, or press Enter to accept the supplied default if it is correct for your environment. If you specify the file system name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response:
No action is required.

IZUG230E The value *value*is incorrect.

Explanation
The specified value is incorrect.

In the message text:

value
Name of the input field.

System programmer response:
Correct the value.

User response:
No action is required.

IZUG231W **A file system with the name *file-system-name* already exists. Do you want to use the existing file system as the z/OSMF *file-system-type*file system (Y|N)?**

Explanation
The specified file system already exists. Indicate whether you want to use the existing file system.

In the message text:

file-system-name
Name of the file system

file-system-type
File system type.

System programmer response:
To use the existing file system, enter Y. Otherwise, enter N. Prior to mounting a new file system, you must unmount the existing file system.

User response:
No action is required.

IZUG232I **The specified z/OSMF *file-system-type* file system with *name-type file-system-name-type*was accepted.**

Explanation
The value specified for the file system name or type was accepted.

In the message text:

file-system-type
File system type

name-type
The word name or type

file-system-name-type
File system name or file system type.

System programmer response:
No action is required.

User response:
No action is required.

IZUG233E **File system *file-system-name* could not be mounted. A file system with the same name is already mounted at *mount-point*.**

Explanation
The file system could not be mounted at the specified mount point because a file system with the same name is already mounted at another mount point.

In the message text:

file-system-name
Name of the file system

mount-point
Mount point of the file system.

System programmer response:
To mount a new file system at that mount point, you must unmount the existing file system and then mount the new file system.

User response:
No action is required.

IZUG234I **File system *file-system-name* is already mounted at mount point *mount-point*. Do you want to use the existing file system as the z/OSMF *file-system-type*file system (Y|N)?**

Explanation
The specified file system is already mounted at the mount point. Indicate whether you want to use the existing file system.

In the message text:

file-system-name
Name of the file system

mount-point
Mount point of the file system

file-system-type
File system type.

System programmer response:
To use the existing file system, enter Y. Otherwise, enter N. Prior to mounting a new file system, you must unmount the existing file system.

User response:
No action is required.

IZUG235E **The file system could not be mounted at mount point *mount-point*. File system *file-system-name*is already mounted at that mount point.**

Explanation
The file system could not be mounted at the specified mount point because another file system is already mounted at that mount point.

In the message text:

mount-point
Name of the mount point

file-system-name
Name of the file system.

System programmer response:
To mount a new file system at that mount point, you must unmount the existing file system and then mount the new file system.

User response:
No action is required.

IZUG236I **Enter zFS or HFS as the z/OSMF data file system type for the file system: *file-system-name*:**

Explanation
This message prompts for the type (zfs or hfs) of the specified file system.

In the message text:

file-system-name
Name of the file system.

System programmer response:
No action is required.

User response:
No action is required.

IZUG237I **Enter the name of the file to save the configuration data (must be .cfg extension), or press Enter to save as file *default-cfg-file*:**

Explanation
This message prompts the user to provide the name of the configuration file where the configuration data is to be saved. A default name is provided.

In the message text:

default-cfg-file
Configuration file name.

System programmer response:
No action is required.

User response:
No action is required.

IZUG238E **File name must be specified with the path.**

Explanation:
A value was provided but did not contain a file name.

System programmer response:
Provide a valid value and retry.

User response:
No action is required.

IZUG239W **File name *file-name*already exists: Overwrite (Y|N)?**

Explanation
The specified file name already exists. The message prompts the user to overwrite it.

In the message text:

file-name
File name.

System programmer response:
Try the action again.

User response:
No action is required.

IZUG240E **Overwrite reply was not (Y). Try again.**

Explanation:
A value of Y was not received to overwrite the file. The message prompts the caller to try again.

System programmer response:
Try the action again.

User response:
No action is required.

IZUG241E **File *file-name*cannot be saved to a read-only file system.**

Explanation
The file cannot be saved to a read-only file system.

In the message text:

file-name
File name.

System programmer response:
Review the location of where to save the file and try again.

User response:
No action is required.

IZUG242I **Do one of the following: Enter the system name, enter NONE not to set the name, or press Enter to accept the default *system-name*:**

Explanation
The message prompts the caller for the system name value to use. A default value is provided. Enter a value of NONE if you do not want to set the system name.

In the message text:

system-name
Default system name.

System programmer response:
No action is required.

User response:
No action is required.

IZUG243I Accepted input: *input-value*

Explanation
The value for the input has been accepted.

In the message text:

input-value
Input value.

System programmer response:
No action is required.

User response:
No action is required.

IZUG244I Enter the z/OSMF root code directory path:

Explanation:
The message prompts for the z/OSMF root code directory path.

System programmer response:
No action is required.

User response:
No action is required.

IZUG245I Enter the z/OSMF root code directory path or press Enter to accept the default path *path-name*:

Explanation
The message prompts for the root code directory for z/OSMF. A default value is provided.

In the message text:

path-name
Default root code directory path for z/OSMF.

System programmer response:
No action is required.

User response:
No action is required.

IZUG246I Enter the name of the volume to use for creating the z/OSMF data file system, or enter an asterisk (*) to use SMS managed storage:

Explanation:
The message prompts you for the name of the volume to create the z/OSMF data file system. If you enter an asterisk (*), it indicates that you want the z/OS storage management subsystem (SMS) to manage the storage.

System programmer response:
Perform the requested action. If you specify a volume, the volume must be on-line. If you specify SMS managed storage, ensure that you have an automatic class selection (ACS) routine in place to assign the appropriate SMS construct, based on the name of the data set to be used for the z/OSMF file system.

User response:
No action is required.

IZUG247I z/OSMF data file system will be created on volume: *volume-name*

Explanation
The file system will be created on the specified volume.

In the message text:

volume-name
Name of the volume to create the file system.

System programmer response:
No action is required.

User response:
No action is required.

IZUG248I Enter the size (in cylinders) to allocate for the data file system:

Explanation:
Enter the initial space allocation, in cylinders, for the z/OSMF data file system. z/OSMF uses 90 percent of this value for the primary allocation and 10 percent for the secondary allocation. The minimum suggested size is 100 cylinders, which causes the script to use 90 cylinders for the primary allocation and 10 cylinders for the secondary allocation.

System programmer response:
Perform the requested action.

User response:
No action is required.

IZUG249E Volume size must be greater than 10 cylinders.

Explanation:
The specified volume is too small (less than 10 cylinders).

System programmer response:
Specify a volume that is at least 10 cylinders in size.

User response:
No action is required.

IZUG250I **The z/OSMF data file system *file-system-name* has a *primary-secondary* allocation size of *cylinder-size*cylinders.**

Explanation

The specified file system was allocated with the specified number of cylinders for the primary or secondary extent.

In the message text:

file-system-name
Name of the file system

primary-secondary
Primary or secondary allocation for the file system.

cylinder-size
Size in cylinders of the allocation.

System programmer response:
No action is required.

User response:
No action is required.

IZUG251I **Allocating z/OSMF data file system *file-system-name*.**

Explanation

The procedure to allocate the specified file system has started.

In the message text:

file-system-name
Name of the file system.

System programmer response:
No action is required.

User response:
No action is required.

IZUG252I **Mounting *file-system-name* at *mount-point*.**

Explanation

The procedure to mount the specified file system at the specified mount point has started.

In the message text:

file-system-name
Name of the file system

mount-point
Mount point of the file system.

System programmer response:
No action is required.

User response:
No action is required.

IZUG253I **Enter the Common Information Model (CIM) administrator user ID, or press Enter to accept the default *default-value*:**

Explanation

The message prompts for the Common Information Model (CIM) administrator user ID. A default attribute value is provided.

In the message text:

default-value
Default value for the CIM administrator user ID.

System programmer response:
Perform the requested action, or accept the default.

User response:
No action is required.

IZUG254E **Unable to copy *source-file-name* to *target-file-name*.**

Explanation

Attempt to copy the specified file failed.

In the message text:

file-name
Name of the file source

target-file-name
Name of the file target

System programmer response:
Ensure that the caller is authorized to perform the copy.

User response:
No action is required.

IZUG255I **Enter the z/OSMF administrator *attribute-name*:**

Explanation

The message prompts for the z/OSMF administrator attributes used to create the z/OSMF administrator.

In the message text:

attribute-name
Name of the attribute to create z/OSMF administrator.

System programmer response:
No action is required.

User response:
No action is required.

IZUG256I **Enter the z/OSMF administrator *attribute-name-keyword*, or press Enter to accept the default *value*:**

Explanation
The message is used to prompt for the z/OSMF administrator attributes. The message individually prompts for the following attributes:

- User ID
- Home directory
- Shell program name
- Logon Procedure Name
- Account number
- Region size

These attributes are used to create the z/OSMF administrator user ID. A default attribute value is provided.

In the message text:

attribute-name-keyword
Name of the attribute

value
Default value of the attribute.

System programmer response:
Enter the requested information, or accept the default.

User response:
No action is required.

IZUG257W User *user-id*already exists.

Explanation
The user ID provided already exists.

In the message text:

user-id
User name.

System programmer response:
No action is required.

User response:
No action is required.

IZUG258I Enter the Common Information Model (CIM) administrator user ID:

Explanation:
The message prompts for the Common Information Model (CIM) administrator user ID.

System programmer response:
No action is required.

User response:
No action is required.

IZUG259I Enter the default RACF-defined group for the z/OSMF administrator:

Explanation:
The message prompts for the default group for the z/OSMF administrator.

System programmer response:
No action is required.

User response:
No action is required.

IZUG260I Enter the default RACF-defined group for the z/OSMF administrator, or press Enter to accept the default *group-id*:

Explanation
The message prompts for the default group for the z/OSMF administrator. A default value is provided.

In the message text:

group-id
Name of the default group.

System programmer response:
No action is required.

User response:
No action is required.

IZUG261E Attribute *attribute-name* must be *attribute-size*.

Explanation
The value provided for the attribute does not conform to the expected range or size in the number of characters.

In the message text:

attribute-name
Name of the attribute

attribute-size
Expected attribute size.

System programmer response:
Specify the value within the correct range or size.

User response:
No action is required.

IZUG262I Enter the server attribute *attribute-name*:

Explanation
The message prompts for the name of the z/OSMF server attributes.

In the message text:

attribute-name
Name of the attribute for the server.

System programmer response:
Enter the server attribute name.

User response:
No action is required.

IZUG263I **Enter the server attribute *attribute-name*, or press Enter to accept the default value *value*:**

Explanation
The message prompts for the z/OSMF server attributes. A default value is provided.

In the message text:

attribute-name
Name of the attribute

value
Name of the attribute to which the default applies.

System programmer response:
Enter the requested information, or accept the default.

User response:
No action is required.

IZUG264E **Value *attribute-name* must be alphanumeric and must be *attribute-size*characters.**

Explanation
The value provided for the z/OSMF server is incorrect or outside the expected range or size for that attribute.

In the message text:

attribute-name
Name of the attribute for the z/OSMF server.

attribute-size
Size or range for the attribute for the z/OSMF server.

System programmer response:
Specify with the correct range or size.

User response:
No action is required.

IZUG265I **Enter the root directory path of the z/OSMF server:**

Explanation:
The message prompts for the root directory path for the z/OSMF server.

System programmer response:
Enter the root directory path.

User response:
No action is required.

IZUG266I **Enter the root directory path of the z/OSMF server, or press Enter to accept the default *server-root-directory*:**

Explanation
The message prompts for the root directory path for the z/OSMF server. A default value is provided.

In the message text:

server-root-directory
Default root directory path of the z/OSMF server.

System programmer response:
Enter the root directory path or accept the default.

User response:
No action is required.

IZUG267I **Enter the SAF profile prefix (case sensitive) for z/OSMF resources:**

Explanation:
The message prompts for the SAF profile prefix.

System programmer response:
Enter the SAF profile prefix.

User response:
No action is required.

IZUG268I **Enter the SAF profile prefix (case sensitive) for z/OSMF resources, or press Enter to accept the default *saf-profile*:**

Explanation
The message prompts for the SAF profile prefix. A default value is provided.

In the message text:

saf-profile
Default SAF profile prefix.

System programmer response:
Enter the SAF profile prefix, or accept the default.

User response:
No action is required.

IZUG271I **Do you want to enable the common event adapter (CEA) component and update related parmlib options for using the Incident Log task? For yes, enter Y. For no, enter N:**

Explanation

The message prompts you to determine whether the Incident Log task is to be configured. When you select to configure the Incident Log task, z/OSMF verifies that the Common Information Model (CIM) server and the common event adapter (CEA) are properly configured. If you have already configured CIM and have set up the CEA parmlib, you still must enter Y. z/OSMF provides additional prompts allowing you to indicate whether the CIM server and the CEA parmlib need to be configured.

If you do not configure the Incident Log task, you cannot complete any other Incident Log set up steps, such as setting up RACF permissions for the Incident Log. In this case, the Incident Log task stills displays in the navigation area in z/OSMF; however, it will not be functional. To remove it from the navigation area, do not authorize any roles to access the Incident Log task.

System programmer response:
Enter Y or N.

User response:
No action is required.

IZUG272I **Do you want to enable the common event adapter (CEA) component and update related parmlib options for using the Incident Log task? For yes, enter Y. For no, enter N. Or press Enter to accept the default *value*:**

Explanation

The message prompts you to determine whether the Incident Log task should be configured. When you select to configure the Incident Log task, the Common Information Model (CIM) server and the common event adapter (CEA) are configured so that they can support the Incident Log task. If you have already configured CIM and have set up the CEA parmlib, you still need to enter Y. When you are asked whether CIM needs to be configured, you can say no. In this case, confirming that you want to set up the Incident Log task gives z/OSMF permission to verify that all of the settings are correct.

If you do not configure the Incident Log task, you cannot complete any other Incident Log set up steps, such as setting up RACF permissions for the Incident Log. The Incident Log task still displays the navigation area in z/OSMF; however, it will not be functional. To remove the Incident Log task from the navigation area, do not authorize any roles to access this task.

In the message text:

value
Default value to specify setup of the Incident Log task.

System programmer response:
Enter Y or N, or accept the default, which is Y.

User response:
No action is required.

IZUG273I **Enter the *dependency-name* *dependency-attribute*:**

Explanation
The message prompts for the Common Information Model (CIM) or common event adapter (CEA) attributes. The *attribute-name-keyword* can be a group user ID or the keyword AUTOGID, the user ID, or the keyword AUTOUID, or the group name. The *attribute-name* can be a group user ID, user ID, or group name.

In the message text:

dependency-name
Name of the Incident Log dependency

dependency-attribute
Name of the Incident Log attribute.

System programmer response:
Enter the incident dependency name and log attribute names.

User response:
No action is required.

IZUG274I **Enter the *component-name* *attribute-name-keyword*, or press Enter to accept *value*:**

Explanation
The message prompts for the Common Information Model (CIM) or common event adapter (CEA) attributes. The *attribute-name-keyword* can be a group user ID or the keyword AUTOGID, the user ID, or the keyword AUTOUID, or the group name. The *attribute-name* can be a group user ID, user ID, or group name. A default value is provided.

In the message text:

component-name
Name of the component

attribute-name-keyword
Name of the attribute keyword

value
Default value.

System programmer response:
Enter the information, or accept the default.

User response:
No action is required.

IZUG275I **Enter the member name suffix to use for the *parmlib-member-name* parmlib member, or press Enter to accept the default *suffix-value*:**

Explanation
The message prompts for the suffix to use for IEADMC and CEAPRM members. A default value is provided.

In the message text:

parmlib-member-name
Name of the parmlib member

suffix-value
Default suffix of the parmlib member.

System programmer response:
No action is required.

User response:
No action is required.

IZUG276I Enter the member name suffix to use for the *parmlib-member-name*parmlib member:

Explanation:
The message prompts for the suffix to use for IEADMC and CEAPRM members.

System programmer response:
Enter the parmlib suffix.

User response:
No action is required.

IZUG277I Enter the *branch-country-name* code, or press Enter to accept the default *attribute-value*:

Explanation
The message prompts for the country code or branch code value. A default is provided.

In the message text:

branch-country-name
Name of the branch or country

attribute-value
Default value for the branch or country.

System programmer response:
Enter the country or branch code, or accept the default.

User response:
No action is required.

IZUG278I Enter the *branch-country-name*code:

Explanation
The message prompts for the country code or branch code value.

In the message text:

branch-country-name
Name of the branch or country.

System programmer response:
enter the country or branch code.

User response:
No action is required.

IZUG279E The *branch-country-name* code must be *branch-country-range*alphanumeric characters (A-Z, 0-9).

Explanation
The value specified for the branch or country code does not conform to guidelines.

In the message text:

branch-country-name
Name of the branch or country

branch-country-range
Range for the branch or country attribute.

System programmer response:
Specify the correct value.

User response:
No action is required.

IZUG280I Do you want to accept storage value *storage-name*? (Y|N)?

Explanation:
The message prompts whether you want to use the existing specified storage option.

System programmer response:
Enter Y or N.

User response:
No action is required.

IZUG281I What storage option do you want to use? Enter V for VOLSER or S for STORCLAS.

Explanation:
The message prompts for the storage option to use.

System programmer response:
Enter a value.

User response:
No action is required.

IZUG282I Enter the name of the *SMS-storage-class*:

Explanation
The message prompts for the name of the specified SMS storage class.

In the message text:

SMS-storage-class
Type of storage option.

System programmer response:
Enter a storage class name.

User response:
No action is required.

IZUG283I Specify one or more of the non-SMS direct access volumes to use. When you are finished entering the values, press Enter again without a value to complete:

Explanation:
The message prompts for the volumes to use for the storage option.

System programmer response:
Enter the volume information. When you have entered all of the information for volume, to complete the input press Enter without specifying a value.

User response:
No action is required.

IZUG284I Enter the name of the source data set for your existing CEAPRM00 parmlib member. Specify the fully qualified data set name, or press Enter to accept the default *parmlib-name*:

Explanation
The message prompts you for the name of the data set that contains your existing CEAPRM00 parmlib member. A fully qualified data set name is expected.

In the message text:

parmlib-name
Default data set name.

System programmer response:
Specify the fully qualified data set name, or press Enter to accept the supplied default if it is correct for your environment. If you specify the data set name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response:
No action is required.

IZUG285I Enter the name of the source data set for your existing CEAPRM00 parmlib member. Specify the fully qualified data set name, or press Enter to use SYS1.PARMLIB:

Explanation:
The message prompts you for the name of the data set that contains your existing CEAPRM00 parmlib member. A fully qualified data set name is expected.

System programmer response:
Specify the fully qualified data set name, or press Enter to use SYS1.PARMLIB as the source for the CEAPRM00 member. If you specify the data set name in quotes, the quotes are ignored. Your input is stored without quotes in the configuration file.

User response:
No action is required.

IZUG286W Arguments are ignored.

Explanation:
The additional unknown arguments that have been supplied in the call will be ignored.

System programmer response:
No action is required.

User response:
No action is required.

IZUG287I z/OSMF RACF *racf-procedure* processing complete. Review and run *racf-rexx-file*before proceeding with configuration.

Explanation
RACF processing has completed for the specified procedure.

In the message text:

racf-procedure
Name of the RACF procedure being performed

racf-rexx-file
Name of the RACF REXX exec.

System programmer response:
Review and run the REXX script before proceeding.

User response:
No action is required.

IZUG288I The .profile is being created for the user.

Explanation:
User .profile was not found. Attempting to create a .profile for the user.

System programmer response:
No action is required.

User response:
No action is required.

IZUG289I The .profile is being updated with Common Information Model (CIM) environment variables.

Explanation:
User .profile does not contain Common Information model (CIM) environment variables. Attempting to update .profile with CIM environment variables.

System programmer response:
No action is required.

User response:
No action is required.

IZUG290E An attempt to update *file-name*has failed.

Explanation

Attempt to update the specified file failed.

In the message text:

file-name
File name.

System programmer response:

Review log file for details.

User response:

No action is required.

IZUG291I The .profile update is complete.

Explanation:

The .profile has been updated.

System programmer response:

No action is required.

User response:

No action is required.

IZUG292W Common Information Model (CIM) environment variables already set up in .profile: *wbem-root-value*

Explanation

The .profile already contains Common Information model (CIM) environment variables.

In the message text:

wbem-root-value
Home directory of WBEM in the .profile.

System programmer response:

Ensure that the value in .profile matches the value specified in the configuration.

User response:

No action is required.

IZUG293I Procedure *procedure*is being started.

Explanation

An attempt to start the specified procedure has been made.

In the message text:

procedure
Procedure being started.

System programmer response:

No action is required.

User response:

No action is required.

IZUG294E Common Information Model (CIM) server failed to start.

Explanation:

Attempt to start the Common Information Model (CIM) server failed.

System programmer response:

Review log file for details.

User response:

No action is required.

IZUG295E Verification process *ivp-name*has failed.

Explanation

The verification process has failed.

In the message text:

ivp-name
Name of the IVP task.

System programmer response:

Review the log file for details.

User response:

No action is required.

IZUG296I Verification process *ivp-name*has completed.

Explanation

The specified verification process has completed.

In the message text:

ivp-name
Name of the IVP task.

System programmer response:

No action is required.

User response:

No action is required.

IZUG297I Provider *provider-name*is already registered with Common Information Model (CIM).

Explanation

The specified provider was found to have been already registered with Common Information Model (CIM).

In the message text:

provider-name
Name of the provider.

System programmer response:

No action is required.

User response:

No action is required.

IZUG298E **Provider *provider-name*is not registered with Common Information Model (CIM).**

Explanation
The specified provider is not registered with Common Information Model (CIM).

In the message text:

provider-name
Name of the provider.

System programmer response:
No action is required.

User response:
No action is required.

IZUG299I **The provider *provider-name*is being registered with Common Information Model (CIM).**

Explanation
An attempt has been made to register the provider with Common Information Model (CIM).

In the message text:

provider-name
Name of the provider.

System programmer response:
No action is required.

User response:
No action is required.

IZUG300I **Processing of script *script-name* has started at *date-and-time*.**

Explanation
Script processing has started. The script name, data, and time are included.

In the message text:

script-name
Name of the script

date-and-time
Date and time that script processing started.

System programmer response:
No action is required.

User response:
No action is required.

IZUG301I **Log directory *log-directory*does not exist or is not writable: using temporary directory for log file.**

Explanation
For script processing, the named log directory (**logs**) within the z/OSMF data directory does not exist or the user who is executing the script does not have permission to write to this directory. The log file for processing of the script will be created in the temporary directory.

In the message text:

log-directory
Name of directory for the log files.

System programmer response:
No action is required.

User response:
No action is required.

IZUG302I **Log will be written to file *log-file-path-and-name*.**

Explanation
The path name of the log file for script processing is provided.

In the message text:

log-file-path-and-name
Directory and file name of the log.

System programmer response:
No action is required.

User response:
No action is required.

IZUG303I **Environment name and value being used are *env-var*.**

Explanation
The name and value for an environment setting is provided.

In the message text:

env-var
Name and value of an environment setting.

System programmer response:
No action is required.

User response:
No action is required.

IZUG304E **An error occurred writing to log file *log-file-path-and-name*: exiting script.**

Explanation
An error was encountered while attempting to write to the log file.

In the message text:

log-file-path-and-name
Directory and file name of the log.

System programmer response:
Check for additional error messages on the screen that describe the error. Rerun after correcting the error.

User response:
No action is required.

IZUG305E The script *script-name* failed with reason code *reason-code*; see log file *log-file-path-and-name*.

Explanation
The indicated script failed. A return code is provided to help indicate the cause of the error.

In the message text:

script-name
Script that failed

reason-code
Reason code for the error

log-file-path-and-name
Directory and file name of the log file.

For the **izuadmin.sh** script, the following reason codes are valid:

1
Script was called with incorrect arguments.

2
Problem with the log directory.

3
Error writing to the log file, or the log file is not accessible.

4
Required environment variable is missing or set incorrectly. Or, the izuadmin.env file does not exist.

5
Required environment setting is missing or incorrect. This error can occur if an expected configuration property or properties file, such as izuapps.properties, is not set, cannot be found, or is not readable.

6
Problem found during verification processing.

7
Installed z/OS level is incorrect for z/OSMF.

105
Exception encountered by an internal script.

For the **izuprime.sh** script, the following reason codes are valid:

1
Usage error.

2
Problem with the log directory.

3
Error writing to the log file.

4
Script encountered an error when running a z/OS UNIX shell command, such as mkdir or cp.

5
A repository already exists.

6
Specified user ID is not defined to the z/OS system.

System programmer response:
For more information, see the z/OSMF log file for related messages. After correcting the error, run the script again. For reason code 105, contact IBM Support for assistance.

User response:
No action is required.

IZUG306I Script *script-name* was invoked with options *input-options*.

Explanation
The options specified as input to the named script are provided.

In the message text:

script-name
Name of the script

input-options
Options passed to the script.

System programmer response:
No action is required.

User response:
No action is required.

IZUG311E IZU_APPSERVER_ROOT *server-root-directory*is not valid: exiting script.

Explanation
The z/OSMF server root directory is not valid. The processing for the script stops.

In the message text:

server-root-directory
Root directory of the z/OSMF server.

System programmer response:
Set IZU_APPSERVER_ROOT to the valid root directory and run again.

User response:
No action is required.

IZUG312I The administration request is being processed.

Explanation:
Processing of the administration request has started.

System programmer response:
No action is required.

User response:
No action is required.

IZUG313E A usage error has occurred: *error*.

Explanation
A problem with the usage has occurred. Context of the error is provided.

In the message text:

error
Explanation for the incorrect usage.

System programmer response:
Correct the problem indicated by the explanation of the error and run again.

User response:
No action is required.

IZUG314E IZU_CODE_ROOT *product-root-directory*is not valid: exiting script.

Explanation
The z/OSMF product root directory is not valid.

In the message text:

product-root-directory
Root directory of the z/OSMF product.

System programmer response:
Set IZU_CODE_ROOT to the valid z/OSMF product root directory and run again.

User response:
No action is required.

IZUG315E An incorrect environment setting has been detected: *env-var*.

Explanation
A problem exists with a setting in the environment file. Context of the error is provided.

In the message text:

env-var
Environment setting and associated problem.

System programmer response:
Review the included environment setting and the associated problem. Correct the error and run again.

User response:
No action is required.

IZUG316E PEGASUS_HOME directory *CIM-server-root-directory*is not valid: exiting script.

Explanation
The Common Information Model (CIM) server WBEM root directory is not valid. Processing for the script stops.

In the message text:

CIM-server-root-directory
WBEM root directory of the CIM server.

System programmer response:
Set PEGASUS_HOME to the Common Information Model (CIM) server WBEM root directory and run the script again.

User response:
No action is required.

IZUG317E IZU_CONFIG_DIR *configuration-directory*is not valid: exiting script.

Explanation
The z/OSMF configuration directory is not valid. Processing for the script stops.

In the message text:

configuration-directory
Configuration directory of the z/OSMF product.

System programmer response:
Set IZU_CONFIG_DIR to the valid z/OSMF configuration directory and run again.

User response:
No action is required.

IZUG318E Path *path-setting* member *member-name*must exist: exiting script.

Explanation
A directory or path that is a member of the specified path setting does not exist. Processing of the script stops.

In the message text:

path-setting
Name of the path setting

member-name
Directory or file specified in the path that does not exist.

System programmer response:
Determine why the file or directory does not exist. Correct the problem and run again.

User response:

No action is required.

IZUG319E Data directory *data-directory*must exist and be writable: exiting script.

Explanation
For script processing the z/OSMF data directory must exist and be capable of being written to. Processing of the script stops.

In the message text:

data-directory
Name of the data directory.

System programmer response:
Ensure the z/OSMF data directory exists. Ensure that the user running the script has permission to write to the directory. After correcting the error run again.

User response:
No action is required.

IZUG320E Users will not be able to launch z/OSMF. The installed z/OS level *installed-z/OS-level* is earlier than the minimum z/OS level *minimum-z/OS-level*that is required by z/OSMF.

Explanation
z/OSMF cannot be launched because it is installed on a system that is earlier than the minimum supported level of z/OS.

In the message text:

installed-z/OS-level
Installed operating system level

minimum-z/OS-level
Minimum operating system level that z/OSMF requires.

In the message text, the software level for the product (z/OS or z/OSMF) is indicated through a standard convention: *aa.bb.cc*, where:

- *aa* is the version
- *bb* is the release
- *cc* is the modification level.

You can correlate the returned value as follows:

- 04.02.00 indicates V2R2 of z/OS
- 04.01.00 indicates V2R1 for the product (z/OS or z/OSMF)
- 03.23.00 indicates V1R13 for the product (z/OS or z/OSMF)

Thus, for example, the value 04.01.00 indicates V2R1 of the product (z/OS or z/OSMF).

System programmer response:
Upgrade to a z/OS level that is supported by z/OSMF.

User response:
No action is required.

IZUG321W The installed z/OSMF level *product-level* is earlier than the z/OS level *os-level*.

Explanation
Your system is running z/OSMF level *product-level*, but a newer z/OSMF level might be available from IBM. Most likely, your installation has migrated to a new release of z/OS without upgrading the z/OSMF product. To allow z/OSMF to use the latest functions in z/OS level *os-level*, it is recommended that you upgrade z/OSMF to the latest level. Until you do so, z/OSMF will continue to operate at its current level of functionality.

In the message text:

product-level
Installed level of z/OSMF.

os-level
Operating system level.

In the message text, the software level for the product (z/OS or z/OSMF) is indicated through a standard convention: *aa.bb.cc*, where:

- *aa* is the version
- *bb* is the release
- *cc* is the modification level.

You can correlate the returned value as follows:

- 04.02.00 indicates V2R2 of z/OS
- 04.01.00 indicates V2R1 for the product (z/OS or z/OSMF)
- 03.23.00 indicates V1R13 for the product (z/OS or z/OSMF)

Thus, for example, the value 04.01.00 indicates V2R1 of the product (z/OS or z/OSMF)

System programmer response:
Upgrade z/OSMF to the latest level that is supported on your z/OS system.

User response:
No action is required.

IZUG333I Enter the z/OSMF Unauthenticated *unauthenticated-UID*, or enter the keyword AUTOUID:

Explanation
The message prompts you to input unauthenticated guest user UID in z/OSMF.

In the message text:

unauthenticated-UID
unauthenticated user UID.

System programmer response:
Enter a valid value.

User response:
No action is required.

IZUG334I **Enter the z/OSMF Unauthenticated *unauthenticated-UID*, or enter the keyword AUTOUID, or press Enter to accept the default *default-unauthenticated-UID*:**

Explanation
The message prompts you to input unauthenticated guest user UID in z/OSMF. To accept the default, press Enter.

In the message text:

unauthenticated-UID
unauthenticated guest user UID.

default-unauthenticated-UID
Default unauthenticated user UID.

System programmer response:
Enter a valid value.

User response:
No action is required.

IZUG335E **A symbolic link is required for the directory: /etc/zosmf. The link could not be created, however, because the directory already exists or etc/zosmf is already defined as the symbolic link for another directory.**

Explanation
While processing the izusetup.sh -finish script, z/OSMF detected that the z/OSMF configuration directory is set to use a directory name other than the product default: /etc/zosmf. This directory name is specified through the variable IZU_CONFIG_DIR. Most likely, your installation chose another name for this directory when configuring z/OSMF on your system.

Because the z/OSMF online help system requires /etc/zosmf as its mount point, z/OSMF attempts to create a symbolic link "etc/zosmf" that resolves to the path name of your specified directory. The link could not be created, however, either because directory /etc/zosmf already exists on your system, or "etc/zosmf" is already defined as a symbolic link for another directory.

System programmer response
To resolve this error, take one of the following actions, as appropriate:

- If the directory /etc/zosmf already exists on your system, examine the directory and its contents. Determine whether the directory can be deleted safely, or its contents moved to another directory. If so, take these steps to remove the directory. Then, run the configuration request again.
- Change your installation's specification for the IZU_CONFIG_DIR variable to the default value /etc/zosmf, and re-run the z/OSMF configuration process, starting with the izusetup.sh -config invocation. You can specify this directory name in the override file for variable IZU_CONFIG_DIR, or interactively, in response to the script prompt for the name of the z/OSMF configuration directory.

User response:
Contact your z/OSMF administrator or system programmer.

IZUG336I **Work manager *work-manager-name*is being created.**

Explanation
The work manager is being created.

In the message text:

work-manager-name
Name of the work manager.

System programmer response:
No action is required.

User response:
No action is required.

IZUG337I **Work manager *work-manager-name* property *property-name* is being set to value *value*.**

Explanation
The work manager property is being set to the indicated value.

In the message text:

work-manager-name
Name of the work manager

property-name
Name of the property

value
Value for the property.

System programmer response:
No action is required.

User response:
No action is required.

IZUG340I Variable substitution entry *variable-name* is being updated with value *value*.

Explanation
The variable substitution entry is being updated with the specified value.

In the message text:

variable-name
Name of the variable

value
Value of the variable.

System programmer response:
No action is required.

User response:
No action is required.

IZUG341I Variable substitution entry *variable-name* is being created with value *value*.

Explanation
The variable substitution entry is being created with the specified value.

In the message text:

variable-name
Name of the variable

value
Value of the variable.

System programmer response:
No action is required.

User response:
No action is required.

IZUG343I Shared library *shared-library-name* with class path *class-path* and native path *native-path*is being deleted.

Explanation
The specified shared library with the specified class path and native path is being removed.

In the message text:

shared-library-name
Name of the shared library

class-path
classpath value

native-path
Native path value.

System programmer response:
No action is required.

User response:
No action is required.

IZUG344I Shared library *shared-library-name* with class path *class-path* and native path *native-path*is being created.

Explanation
The specified shared library with the specified class path and native path is being created.

In the message text:

shared-library-name
Name of the shared library

class-path
classpath value

native-path
Native path value.

System programmer response:
No action is required.

User response:
No action is required.

IZUG345I Plug-in *plugin-name*is being removed.

Explanation
The specified plug-in is being removed from z/OSMF.

In the message text:

plugin-name
Name of the plug-in.

System programmer response:
No action is required.

User response:
No action is required.

IZUG346I Plug-in *plug-in-name* from location *file-location*is being installed.

Explanation
The plug-in is being installed into z/OSMF from the specified location.

In the message text:

plugin-name
Name of the plug-in.

file-location
Location of the Enterprise Archive (EAR) file.

System programmer response:
No action is required.

User response:
No action is required.

IZUG347I **Reference to shared library *shared-library-name* with scope *scope*is being added.**

Explanation
A reference to the shared library is being added with the specified scope.

In the message text:

shared-library-name
Name of the shared library

scope
Scope of the shared library reference.

System programmer response:
No action is required.

User response:
No action is required.

IZUG348I **Processing of your request has started. This process might require several minutes or more to complete.**

Explanation:
The requested script processing is running, but might take some time to complete. As it runs, the script writes messages to the script log file.

System programmer response:
No action is required.

User response:
No action is required.

IZUG349I **The function *function-name* can be accessed at link *link-name*after the z/OSMF server is started on your system.**

Explanation
The requested configuration process completed. z/OSMF will be available to users at the indicated URL after the z/OSMF server is restarted on this system.

In the message text:

function-name
The z/OSMF function that is available.

link-name
The link for accessing z/OSMF.

System programmer response:
No action is required.

User response:
No action is required.

IZUG350I **The z/OSMF server on this system will attempt to connect to the angel *angel-name*.**

Explanation
On start-up, the z/OSMF server attempts to connect to a WebSphere Liberty angel process. Your installation specifies the angel name on the ANGEL_PROC parameter in the IZUPRMxx member for this system. By default, the angel name is IZUANG1.

In the message text:

angel-name
Angel to be used by the z/OSMF server.

System programmer response:
No action is required.

User response:
No action is required.

IZUG352W **During the processing of the z/OSMF server started procedure, the PARM parameter was found to be missing one or more expected values: *missing-values***

Explanation
In the z/OSMF server started procedure, the PARM statement is missing the indicated values.

In the message text:

missing-values
Values that are missing from the PARM statement.

System programmer response:
No action is required.

User response:
This message indicates a potential problem with the z/OSMF server started procedure. In the started procedure, verify that the PARM= parameter list is complete and correct for your installation. For reference, see the sample procedures IZUSVR1 in SYS1.PROCLIB and IZUSVR2 in SYS1.SAMPLIB.

IZUG354I **Security option *option-name* with value *option-value*is being set.**

Explanation
A security setting in the z/OSMF server is being updated to the specified value.

In the message text:

option-name
Name of the option being set

option-value
Value of the option being set.

System programmer response:
No action is required.

User response:
No action is required.

IZUG356I Plug-in *plugin-name*is being stopped.

Explanation
The specified plug-in is being stopped.

In the message text:

plugin-name
Name of the plug-in.

System programmer response:
No action is required.

User response:
No action is required.

IZUG357I Plug-in *plugin-name*is being started.

Explanation
The specified plug-in is being started.

In the message text:

plugin-name
Name of the plug-in.

System programmer response:
No action is required.

User response:
No action is required.

IZUG358E Server *server-name*does not exist.

Explanation
The specified server does not exist.

In the message text:

server-name
Name of the server.

System programmer response:
Specify a valid server name and repeat this operation.

User response:
No action is required.

IZUG360I Script option *option-name*is deprecated. The z/OSMF configuration process ignores this option.

Explanation
The specified script option is deprecated. The z/OSMF process ignores the option and continues processing as normal. If you received this message when running the izusetup.sh script with the -service option, understand that the -service option is no longer required when you apply z/OSMF service to your system.

In the message text:

option-name
Option that was specified.

System programmer response:
To avoid receiving this message in the future, do not specify the indicated option. If you received this message when applying z/OSMF service, you are using an obsolete option. Review the HOLDDATA section of the PTF for instructions on applying service to your system.

User response:
No action is required.

IZUG361I Do you want to create a Certificate Authority? For yes, enter Y. For no, enter N:.

Explanation
The message prompts you to indicate whether (Y or N) the z/OSMF security setup should include the creation of a Certificate Authority (CA). The CA is used to sign server certificates that are used for secure (SSL) communication between the user's web browser and the z/OSMF server. Y is the default.

If you specify N, you must provide your own CA for enabling secure communications.

System programmer response:
Enter a valid value.

User response:
No action is required.

IZUG362I Do you want to create a Certificate Authority? For yes, enter Y. For no, enter N. Or press Enter to accept the default value *default-value*.

Explanation
The message prompts you to indicate whether (Y or N) the z/OSMF security setup should include the creation of a Certificate Authority (CA). The CA is used to sign server certificates that are used for secure (SSL) communication between the user's web browser and the z/OSMF server. The default value is provided.

In the message text:

default-value
Default value for creating Certificate Authority (Y or N).

System programmer response:
Enter the a valid value (Y or N) or press Enter to select the default value.

User response:
No action is required.

IZUG363E User *user-name* is not permitted to access the digital certificate *certificate-label*.

Explanation

The specified user lacks sufficient authorization to the indicated digital certificate.

In the message text:

user-name
Name of the user

certificate-label
Label of digital certificate.

System programmer response:

Determine whether the user requires access to the digital certificate. If so, grant access to the user.

User response:

No action is required.

IZUG364E User *user-name* did not connect label *certificate-label* to keyring *certificate-keyring*.

Explanation

The specified user lacks sufficient authorization to the indicated keyring.

In the message text:

user-name
Name of the user.

certificate-label
Label of the digital certificate.

certificate-keyring
Keyring of the digital certificate.

System programmer response:

Determine whether the user requires access to the keyring. If so, grant access to the user.

User response:

No action is required.

IZUG365I Process *process-name* with start command arguments is being updated to include value *value-1*. The value of the arguments is now *value-2*.

Explanation

The specified argument is being added to the start command arguments for the specified process.

In the message text:

process-name
Name of the server process

value-1
Value of the new argument being added

value-2
New value of the start command arguments.

System programmer response:

No action is required.

User response:

No action is required.

IZUG366E The supplied level of Java does not meet the minimum that is required by z/OSMF. Level found: *found-java-level* Level required: *required-java-level*.

Explanation

z/OSMF requires the indicated level of Java to be installed and operational on your system. During the configuration process, however, z/OSMF found an incorrect version of Java. To determine the installed level of Java, z/OSMF checks the location specified on the environment variable JAVA_HOME.

In the message text:

found-java-level
The level of Java that was found on your system.

required-java-level
The minimum level of Java that is required for z/OSMF operation.

System programmer response:

Determine whether the minimum level of Java is installed and mounted on your system. If so, ensure that the environment variable JAVA_HOME specifies the correct location. If your installation uses a mount point other than the product default, update the z/OSMF environment variable JAVA_HOME to refer to the correct location. This action will not affect any other products requiring a different level of Java.

User response:

No action is required.

IZUG367W Member *target-member-name* specifies HLQ value *hlq-value* for incidents. This setting will be overwritten by member *source-member-name* and HLQLONG value *hlqlong-value*. As a result, you might not be able to manage any previously created incidents. Do you want to continue? (Y|N)?

Explanation

The existing HLQ value in the indicated source member will be replaced by the HLQLONG value specified in the target member.

In the message text:

target-member-name
The target member name.

hlq-value
The current HLQ value.

source-member-name
source member name.

hlqlong-value
HLQLONG value.

System programmer response:
Enter Y to continue with this operation. Otherwise, enter N to cancel.

User response:
No action is required.

IZUG368I **Enter the z/OSMF unauthenticated user name *unauthenticated-name*.**

Explanation
The message prompts you to input unauthenticated guest user name in z/OSMF.

unauthenticated-name
unauthenticated user name.

System programmer response:
Enter a valid value.

User response:
No action is required.

IZUG369I **Enter the z/OSMF unauthenticated user name *unauthenticated-name*, or press Enter to accept the default value *default-unauthenticated-name*.**

Explanation
The message prompts you for the unauthenticated guest user name in z/OSMF. To accept the default, press Enter.

unauthenticated-name
unauthenticated guest user name.

default-unauthenticated-name
Default unauthenticated user name.

System programmer response:
Enter a valid value, or press Enter the accept the default value.

User response:
No action is required.

IZUG370I **User registry is being initialized with user ID *user-id*.**

Explanation
The z/OSMF user registry is being initialized with the specified user ID.

In the message text:

user-id
User ID with which the user registry is being initialized.

System programmer response:
No action is required.

User response:
No action is required.

IZUG371I **Role repository is being initialized for user ID *user-id*.**

Explanation
The z/OSMF role repository is being initialized for the specified user ID.

In the message text:

user-id
User ID for which the role repository is being initialized.

System programmer response:
No action is required.

User response:
No action is required.

IZUG372E **Command *command-name* returned an error. Command return code is *return-code*.**

Explanation
An error was received from a command invocation.

In the message text:

command-name
Command that returned the error

return-code
Return code from the command.

System programmer response:
Search the log for other error messages that indicate the problem. Correct the problem indicated by the messages and run again.

User response:
No action is required.

IZUG373E **Repository *repository-name*was not initialized because it already exists: exiting script.**

Explanation
A z/OSMF repository was not initialized because it already exists. A z/OSMF repository can only be

initialized if it does not exist. Processing of the script stops.

In the message text:

repository-name
Name of the existing repository.

System programmer response:
Do not attempt to initialize the existing repository.

User response:
No action is required.

IZUG374E User ID *user-id*for the z/OSMF administrator must exist: exiting script.

Explanation
The z/OSMF repositories were not initialized because the administrator user ID does not exist. Processing of the script stops.

In the message text:

user-id
User ID that does not exist.

System programmer response:
Search the log for other error messages that might indicate the problem. Correct the problem indicated by the messages and run again.

User response:
No action is required.

IZUG375I Verification has completed for *item-name*.

Explanation
Verification has completed for the specified item.

In the message text:

item-name
Item that was verified.

System programmer response:
No action is required.

User response:
No action is required.

IZUG376E Verification failed for *item-name* because of the following reason: *reason*

Explanation
Verification failed for the item because of the specified reason. Context of the error is provided.

In the message text:

item-name
Item that failed verification

reason
Reason verification failed.

System programmer response:
Perform action to correct the problem based on the indicated reason.

User response:
No action is required.

IZUG377E Unable to write to *directory-name*: exiting script.

Explanation
Attempt to write to the specified directory failed.

In the message text:

directory-name
Name of the directory being written to.

System programmer response:
Ensure user has access to write to the directory.

User response:
No action is required.

IZUG378I Process *process-name* JVM custom property *property-name* that has a value of *value*is being deleted.

Explanation
The specified property for the named process is being removed.

In the message text:

process-name
Name of the server process

property-name
Name of the property

value
Value of the property.

System programmer response:
No action is required.

User response:
No action is required.

IZUG379I Process *process-name* JVM custom property *property-name* that has a value of *value*is being created.

Explanation
The specified property for the named process is being added.

In the message text:

process-name
Name of the server process

property-name
Name of the property

value
Value of the property.

System programmer response:
No action is required.

User response:
No action is required.

IZUG380E **Unable to unmount file system *file-system-name*.**

Explanation
Attempt to unmount the indicated file system failed.

In the message text:

file-system-name
Name of the file system.

System programmer response:
For more information, see the log file.

User response:
No action is required.

IZUG381I **Unmounting *file-system-name*.**

Explanation
The procedure to unmount the specified file system has started.

In the message text:

file-system-name
Name of the file system.

System programmer response:
No action is required.

User response:
No action is required.

IZUG382E **File system *file-system-name*does not exist.**

Explanation
The specified file system does not exist.

In the message text:

file-system-name
Name of the file system.

System programmer response:
Specify a file system that does exist.

User response:
No action is required.

IZUG383I **File system *file-system-name* is mounted at mount point *mount-point*.**

Explanation
The indicated file system is mounted at that mount point.

In the message text:

file-system-name
Name of the file system

mount-point
Name of the mount point.

System programmer response:
No action is required.

User response:
No action is required.

IZUG384I **Object *object-name* property *property-name*, which has a value of *value*, is being deleted.**

Explanation
The indicated property for this object is being deleted. The current setting for the property is shown.

You have either selected to change the current setting of a property, or you are deleting the property altogether. When you change the value of a property, the property is first deleted and then created again with the new value. When you delete a property, z/OSMF uses the property default instead.

In the message text:

object-name
Name of the object

property-name
Name of the property

value
Value of the property.

System programmer response:
No action is required.

User response:
No action is required.

IZUG385I **The z/OSMF server is not started. To allow the -addlink request to complete, restart the z/OSMF server.**

Explanation:
The -addlink request cannot complete until you start the z/OSMF server.

System programmer response
Start the z/OSMF server.

After the server is started, see the z/OSMF log file for an indication of the success or failure of this request. The z/OSMF log file is named IZUG*n*.log, where *n* is a number from 0 to 9. The z/OSMF log file resides in the /logs subdirectory directory of the z/OSMF data file system. Your installation specified the z/OSMF data file system on the IZU_DATA_DIR variable when configuring z/OSMF. By default, this is directory /var/zosmf/data.

User response:
No action is required.

IZUG386E **The command is missing a required argument: *object-name*.**

Explanation
The command is missing the indicated argument and thus, cannot be performed.

In the message text:

argument-name
Name of the missing argument.

System programmer response:
Enter the command again with all of its required arguments.

User response:
No action is required.

IZUG387I **Setting *setting-name* has a value of *value*.**

Explanation
The setting will be set to the indicated value. The current value of the setting in the z/OSMF configuration is shown.

In the message text:

setting-name
Name of the setting

value
Value for the setting.

System programmer response:
No action is required.

User response:
No action is required.

IZUG388I **Setting *setting-name*is not set.**

Explanation
The indicated setting is not currently set in the z/OSMF configuration. z/OSMF will use the setting default.

In the message text:

setting-name
Name of the setting

value
Value for the setting.

System programmer response:
No action is required.

User response:
No action is required.

IZUG397I **The -addlink request was processed. To verify that the link was added, check the z/OSMF log file.**

Explanation:
To add a link to the z/OSMF navigation area, you invoked the izusetup.sh script with the -addlink option. For an indication of the success or failure of this request, see the z/OSMF log file.

System programmer response:
No action is required.

User response
To verify that the link was added, check the z/OSMF log file. This file is named IZUG*n*.log, where *n* is a number from 0 to 9. The z/OSMF log file resides in the /logs subdirectory directory of the z/OSMF data file system. Your installation specified the z/OSMF data file system on the IZU_DATA_DIR variable when configuring z/OSMF. By default, this is directory /var/zosmf/data.

To modify or remove a link after it is added, you must use the Links task in the z/OSMF navigation area.

IZUG398I **The z/OSMF server is not started. To allow the -addlink request to complete, start the server.**

Explanation:
The -addlink request cannot complete until you start the z/OSMF server.

System programmer response
Start the z/OSMF server.

After the server is started, see the z/OSMF log file for an indication of the success or failure of this request. The z/OSMF log file is named IZUG*n*.log, where *n* is a number from 0 to 9. The z/OSMF log file resides in the /logs subdirectory directory of the z/OSMF data file system. Your installation specified the z/OSMF data file system on the IZU_DATA_DIR variable when configuring z/OSMF. By default, this is directory /var/zosmf/data.

User response:
No action is required.

IZUG399I **Successfully copied *source-file-name* to *target-file-name*.**

Explanation
The input file was successfully copied to the destination.

In the message text:

source-file-name
Name of the source file

target-file-name
Name of the destination file.

System programmer response:
No action is required.

User response:
No action is required.

Appendix A. Security configuration requirements for z/OSMF

Using z/OSMF requires sufficient authority in z/OS. Specifically, on the z/OS system to be managed, the resources to be accessed on behalf of users (data sets, operator commands, and so on) are secured through the external security manager at your installation, such as RACF. Your installation's security administrator must create the authorizations in your external security manager. To assist your security administrator, z/OSMF provides sample jobs in SYS1.SAMPLIB and the information in this document. Your security administrator can use the sample jobs to create the groups, user IDs, and resource profiles for your z/OSMF configuration. Later, these z/OSMF constructs will require more permissions to a number of existing groups, user IDs, and resources on your system.

This appendix describes the security configuration requirements for z/OSMF. Included are the resource authorizations that are created when your installation runs the IZUSEC job for the core functions, and the IZU*xx*SEC jobs for the optional plug-ins. Also listed are the resource authorizations that your installation must define outside of the configuration process.

The security configuration requirements for z/OSMF are described in the sections that follow. Creating these permissions requires the assistance of your security administrator.

Class activations that z/OSMF requires

For a RACF installation, the security classes that are shown in Table 32 on page 288 must be active when you configure z/OSMF. Commands for activating the classes (with generic profile checking activated) are included in commented sections in the IZUxxSEC jobs. To allow the commands to be issued when the jobs run, uncomment the sections. Or, ask your security administrator to enter the commands directly, as shown in Table 32 on page 288.

Table 32. Class activations that z/OSMF requires

Class	Purpose	RACF commands for activating
ACCTNUM	Controls access to the account number used for the procedure for the z/OSMF REST interfaces, as described in “Updating your system for the z/OSMF REST interfaces” on page 24.	`SETROPTS CLASSACT(ACCTNUM)`

APPL	Controls access to the z/OSMF application domain. This access is required by:
	• Security group for z/OSMF administrators (IZUADMIN, by default)
	• Security group for z/OSMF unauthenticated guest users (IZUGUEST, by default)
	• Security group for the z/OSMF users (IZUUSER, by default)
	• Security group for the z/OS security administrator (IZUSECAD, by default).
	If there is no matching profile in the APPL class, RACF allows the user to access the application.
		`SETROPTS CLASSACT(APPL)`
		`SETROPTS RACLIST(APPL) GENERIC(APPL)`

EJBROLE	Controls the user’s ability to connect to the z/OSMF core functions and tasks. z/OSMF defines a resource name for each core function and task.	`SETROPTS CLASSACT(EJBROLE)`
		`SETROPTS RACLIST(EJBROLE) GENERIC(EJBROLE)`

FACILITY	Controls the user’s access to profiles when the user performs an action. This access is required by the z/OSMF started task user ID (IZUSVR, by default). Examples include the profiles that are used to control privileges in the z/OS UNIX environment.	`SETROPTS CLASSACT(FACILITY)`
		`SETROPTS RACLIST(FACILITY)`
		`GENERIC(FACILITY)`

JESSPOOL	Allows the user to retrieve messages from the system log (SYSLOG).	`SETROPTS`
		`CLASSACT(JESSPOOL)`
		`SETROPTS RACLIST(JESSPOOL)`

LOGSTRM	Allows the user to retrieve messages from the operations log (OPERLOG).	`SETROPTS`
		`CLASSACT(LOGSTRM)`
		
		`SETROPTS RACLIST(LOGSTRM)`

OPERCMDS	Allows the user to create an EMCS console by using the z/OS Operator Consoles task.	`SETROPTS CLASSACT(OPERCMDS)`
		`SETROPTS RACLIST(OPERCMDS)`

SERVAUTH	Controls the user’s ability to use CEA TSO/E address space services. In z/OSMF, this access is required by:
	• z/OSMF started task user ID (IZUSVR, by default)
	• Callers of the z/OS data set and file REST interface services
	• Users of the ISPF task.
		`SETROPTS CLASSACT(SERVAUTH)`
		`SETROPTS RACLIST(SERVAUTH)`
		`GENERIC(SERVAUTH)`

Table 32. Class activations that z/OSMF requires (continued)

Class	Purpose	RACF commands for activating

SERVER	Allows the z/OSMF started task user ID to request services from z/OS system components, such as the system authorization facility (SAF), workload management (WLM), and SVCDUMP services.	`SETROPTS CLASSACT(SERVER)`
		`SETROPTS RACLIST(SERVER) GENERIC(SERVER)`

STARTED	Assigns an identity to the z/OSMF started task during the processing of an MVS START command. By default, the started task runs under the IZUSVR user ID.	`SETROPTS CLASSACT(STARTED)`
		`SETROPTS RACLIST(STARTED) GENERIC(STARTED)`

TSOAUTH	Allows the user to create an EMCS console by using the z/OS Operator Consoles task.	`SETROPTS CLASSACT(TSOAUTH)`
		`SETROPTS RACLIST(TSOAUTH)`

TSOPROC	Controls access to the procedure for the z/OSMF REST interfaces, as described in "Updating your system for the z/OSMF REST interfaces" on page 24.	`SETROPTS CLASSACT(TSOPROC)`

ZMFAPLA	Controls the user's ability to use the z/OSMF core functions and tasks. z/OSMF defines a resource name for each core function and task.
	• Profile names in this class are case-sensitive.
	• The ZMFAPLA class requires the RACLIST option.
		`SETROPTS CLASSACT(ZMFAPLA)`
		`SETROPTS RACLIST(ZMFAPLA) GENERIC(ZMFAPLA)`

ZMFCLOUD	Allows the user to use the z/OSMF core functions and tasks that are related to IBM Cloud Provisioning. z/OSMF defines a resource name for each core function and task for IBM Cloud Provisioning.
	For more information, see Chapter 4, "Preparing to use Cloud Provisioning," on page 51.
	The ZMFCLOUD class requires the RACLIST option.
		`SETROPTS CLASSACT(ZMFCLOUD)`
		`GENERIC(ZMFCLOUD)`
		`RACLIST(ZMFCLOUD)`

If your installation uses an external security manager other than RACF, ask your security administrator to create equivalent commands for your environment.

SAF profile prefix for z/OSMF resources

During the configuration process, your security administrator runs the IZUxxSEC jobs to secure z/OSMF resources. In these jobs, your installation specifies a system authorization facility (SAF) profile prefix to be used for naming z/OSMF resources. The SAF prefix is prepended to the names of z/OSMF resource profiles, and is used in some of the RACF commands that are contained in the IZUxxSEC jobs.

In the examples in this document, the SAF prefix is shown as *<SAF-prefix>*. By default, the SAF prefix is IZUDFLT. If your installation selects to use a different value, substitute the value in the examples.

User IDs that z/OSMF creates during configuration

The IZUSEC job creates the user IDs that are described in Table 33 on page 290.

Table 33. User IDs that z/OSMF creates during the configuration process

User ID	Purpose	Default UID	Created by
IZUGUEST	User ID for performing unauthenticated work, such as guest user access to the Welcome page.	9011	IZUSEC job
IZUSVR	User ID for the z/OSMF started tasks, which are named IZUANG1 and IZUSVR1, by default.	9010	IZUSEC job

Table 33 on page 290 shows the IBM default values. Your security administrator can specify different user IDs in place of the default user IDs in the IZUSEC job.

Security groups that z/OSMF creates during configuration

The IZUSEC job creates a base set of security groups for your z/OSMF configuration. These groups are necessary for giving users the proper level of access to z/OSMF and z/OS system resources.

Your security team might determine that the existing group names would be preferred. If so, you can use your existing group names in place of the supplied z/OSMF default group names. For example, you might already have a group that is aligned with administrators; if so, you could use that group, instead of the z/OSMF default group for administrators, IZUADMIN.

Table 34 on page 290 lists the groups that the IZUSEC job creates. The group names can change, based on the values you provide during the configuration process. Table 34 on page 290 shows the IBM default values.

Table 34. Security groups that z/OSMF creates during the configuration process

Group	Purpose	Created by
IZUADMIN	Security group for the z/OSMF administrator role. Any user IDs connected to this group are considered to be z/OSMF administrators.	IZUSEC job
IZUUSER	Security group for the z/OSMF user role.	IZUSEC job
IZUSECAD	Security group for the z/OS security administrator role in z/OSMF.	IZUSEC job
IZUUNGRP	Security group for the z/OSMF unauthenticated user ID.	IZUSEC job

Resource authorizations for the z/OSMF core functions

Table 35 on page 291 describes the access requirements for the z/OSMF core functions. The IZUSEC job includes sample RACF commands for creating these authorizations on your system. These values can change, based on the values you provide during the configuration process. Table 35 on page 291 shows the IBM default values.

Table 35. Security setup requirements for z/OSMF core functions

Resource class	Resource name	Who needs access?	Type of access required	Why
ACCTNUM	IZUACCT	IZUADMIN IZUUSER	READ	Allows callers to access the account number that is used for the procedure for the z/OSMF REST interfaces, as described in "Updating your system for the z/OSMF REST interfaces" on page 24.
APPL	*<SAF-prefix>*	IZUADMIN IZUGUEST IZUUSER IZUSECAD	READ	Allow access to the z/OSMF application domain. If there is no matching profile in the APPL class, RACF allows the user to access the application.
CERT	DefaultzOSMFCert.*<SAF-prefix>*	Owned by the IZUSVR user ID	N/A	Needed for secure communications between the browser and the z/OSMF server.
CERT	zOSMFCA	N/A	N/A	Certificate authority; needed for secure communications between the browser and the z/OSMF server.
CSFSERV	CSF* profiles	IZUSVR	READ	z/OS Integrated Cryptographic Service Facility (ICSF) callable services. If your installation uses hardware cryptography with ICSF, you must permit the z/OSMF server user ID to these services, as described in "Resource authorizations for hardware cryptography" on page 299.
DATASET	*your_stack_include_dataset*	IZUSVR	ALTER	Allows the z/OSMF server to write to the configured include data sets when a network resource is provisioned or de-provisioned. There is one include data set per stack defined for IBM Cloud Provisioning. This definition is applicable only when your installation uses discrete or generic profiles to protect data set access.

Table 35. Security setup requirements for z/OSMF core functions (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
DATASET	*your_stack_dynamic_update_dataset*	IZUSVR	ALTER	Allows the z/OSMF server to write to the configured dynamic updates data sets when a network resource is provisioned or de-provisioned. One dynamic update data set per stack can be defined for IBM Cloud Provisioning. This definition is applicable only when your installation uses a discrete or generic profiles to protect data set access.
EJBROLE	<*SAF-prefix*>.IzuManagementFacility.izuUsers	IZUADMIN IZUUSER	READ	Allow the user to log on to z/OSMF and view the Welcome page.
EJBROLE	<*SAF-prefix*>.IzuManagementFacilityHelpApp.izuUsers	IZUADMIN IZUUSER	READ	Allow the user to connect to the z/OSMF online help system.
EJBROLE	<*SAF-prefix*>.IzuManagementFacilityImportUtility.izuUsers	IZUADMIN IZUUSER	READ	Allow the user to use the Import Manager task to import plug-ins, event types, event handlers, and links into z/OSMF.
EJBROLE	<*SAF-prefix*>.IzuManagementFacilityRestConsoles.izuUsers	IZUADMIN IZUUSER	READ	Allow the user to connect to the z/OS console REST interface
EJBROLE	<*SAF-prefix*>.IzuManagementFacilityRestJobs.izuUsers	IZUADMIN IZUUSER	READ	Allow the user to connect to the z/OS jobs REST interface.
EJBROLE	<*SAF-prefix*>.IzuManagementFacilityTsoServices.izuUsers	IZUADMIN	READ	Allow the user of the Operator Consoles task to start or reconnect to address spaces on other systems in the sysplex.
EJBROLE	<*SAF-prefix*>.IzuManagementFacilityWorkflow.izuUsers	IZUADMIN IZUUSER IZUSECAD	READ	Allow the user to connect to the Workflows task.
EJBROLE	<*SAF-prefix*> .com.ibm.ws.management.security. resource.allAuthenticatedUsers	IZUADMIN IZUUSER	READ	Allow the user to display information about the IBM Cloud Provisioning and Management for z/OS REST APIs. For more information about the REST services, see *IBM z/OS Management Facility Programming Guide*.IBM z/OS Management Facility Programming Guide.
FACILITY	BBG.SYNC.<*SAF-prefix*>	IZUSVR	CONTROL	Allow the z/OSMF server to synchronize any RunAs identity with the OS identity.

Table 35. Security setup requirements for z/OSMF core functions (continued)

Resource class	**Resource name**	**Who needs access?**	**Type of access required**	**Why**
FACILITY	BPX.CONSOLE	IZUSVR	READ	Allow the user to filter z/OS UNIX messages. Specifically, this setting suppresses the BPXM023I message prefix from any write-to-operator (WTO) messages that z/OSMF writes to the console.
FACILITY	BPX.WLMSERVER	IZUSVR	READ	Allows the z/OSMF server to use WLM functions to create and manage work requests.
FACILITY	HWI.APPLNAME.HWISERV	IZUADMIN	READ	Grant the administrator groups access to BCPii services.
FACILITY	HWI.TARGET.*<netid.nau>*	IZUADMIN	READ	Allow the administrator to access the BCPii request type of CPC.
FACILITY	HWI.TARGET.*<netid.nau>*.*<imagename>*	IZUADMIN	READ	Allow the administrator to access the BCPii request type of LPAR.
FACILITY	IRR.DIGTCERT.LIST	IZUSVR	READ	Allow the started task user ID to retrieve the status of the certificate.
FACILITY	IRR.DIGTCERT.LISTRING	IZUSVR	READ	Allow the started task user ID to list and get the certificate keyring.
FACILITY	IRR.RUSERMAP	IZUSVR	READ	Allow the started task user ID to use the **`R_usermap`** service. This authorization is required for the z/OSMF notification function. The z/OSMF server uses the **`R_usermap`** service to determine the application user identity associated with a RACF user ID, or to determine the RACF user ID associated with an application user identity or digital certificate.
KEYRING	IZUKeyring.*<SAF-`prefix`>*	IZUSVR	N/A	Needed for secure communications.
OPERCMDS	MVS.MCSOPER.IZU@*	IZUADMIN IZUUSER	READ	Allow the user to operate an extended MCS console.
OPERCMDS	MVS.VARY.TCPIP.OBEYFILE	IZUSVR	CONTROL	Allows the z/OSMF server to issue the **`VARY TCPIP OBEYFILE`** command for IBM Cloud Provisioning. This definition is applicable only when your installation utilizes the OPERCMDS class to restrict access to the **`VARY TCPIP OBEYFILE`** command.

Table 35. Security setup requirements for z/OSMF core functions (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
OPERCMDS	MVS.MCSOPER.ZCDPLM*	IZUSVR	READ	Allows the z/OSMF server to issue various operator commands for IBM Cloud Provisioning. The console name for this extended MCS console is the text string ZCDPLM, which is appended with the MVS sysclone value of the system of the z/OSMF instance.
OPERCMDS	MVS.DISPLAY.XCF	IZUSVR	READ	Allows the z/OSMF server to issue the DISPLAY XCF operator command for IBM Cloud Provisioning. This definition is applicable only when your installation utilizes the OPERCMDS class to restrict access to the DISPLAY XCF operator command.
OPERCMDS	MVS.ROUTE.CMD*<sysname>*	IZUSVR	READ	Allows the z/OSMF server to issue the **ROUTE** operator command for IBM Cloud Provisioning and Management for z/OS. This definition is applicable only if the installation uses this profile to restrict the use of the **ROUTE** command.
SERVAUTH	CEA.CEATSO.TSOREQUEST	IZUADMIN IZUUSER	READ	Allow the HTTP client applications on your z/OS system to start and manage TSO/E address spaces.
SERVAUTH	CEA.CEATSO.TSOREQUEST	IZUSVR	READ	Allow the z/OSMF server to start and manage TSO/E address space services.
SERVAUTH	CEA.SIGNAL.ENF83	IZUSVR	READ	Allow the z/OSMF server to use ENF83 to indicate its status to other systems in the sysplex.
SERVAUTH	EZB.INITSTACK.*sysname.tcpname*	IZUSVR	READ	Allows the z/OSMF server to access the TCP/IP stack during TCP/IP initialization. This authorization is needed if the TCP/IP profile activates Application Transparent Transport Layer Security (AT-TLS).
SERVAUTH	EZB.NETWORKUTILS.CLOUD.*mvsname*	IZUSVR	READ	Allows the z/OSMF started task user ID issue operator commands for IBM Cloud Provisioning. *mvsname* is the name of the system on which the z/OSMF server is running.

Table 35. Security setup requirements for z/OSMF core functions (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
SERVAUTH	EZB.NETSTAT.*<mvsname>*.*<tcpname>*	IZUSVR	READ	Allows the z/OSMF started task user ID to issue the **NETSTAT** command. Otherwise, the z/OSMF server fails on initialization. This definition is applicable only when your installation has configured an AT-TLS policy.
SERVAUTH	EZB.NETSTAT.*<mvsname>*.*<tcpprocname>*.CONFIG	IZUSVR		Allows the Network Configuration Assistant task to issue the command **NETSTAT CONFIG**. This definition is applicable only when your installation uses the SERVAUTH class to restrict usage of the **NETSTAT** command. When this definition is applicable, IZUSVR must be authorized for each stack defined for IBM Cloud Provisioning and Management for z/OS.
SERVAUTH	EZB.NETSTAT.*<mvsname>*.*<tcpprocname>*.VIPADCFG	IZUSVR	READ	Allows the z/OSMF started task user ID to issue the **NETSTAT VIPADCFG** command. This definition is applicable only when your installation utilizes the SERVAUTH class to restrict usage of the **NETSTAT** command. When this definition is applicable, the z/OSMF started task user ID must be authorized for each stack that is defined for IBM Cloud Provisioning.
SERVER	BBG.ANGEL	IZUSVR	READ	Allow the z/OSMF server to access the angel process.
SERVER	BBG.ANGEL.IZUANG1	IZUSVR	READ	Allow the z/OSMF server to access the z/OSMF named angel process.
SERVER	BBG.ANGEL.*proc-name*	IZUSVR	READ	Allows the z/OSMF server to use z/OS authorized services.
SERVER	BBG.AUTHMOD.BBGZSAFM	IZUSVR	READ	Allow the z/OSMF server to access the SAF authorized registry.
SERVER	BBG.AUTHMOD.BBGZSAFM.SAFCRED	IZUSVR	READ	Allow the z/OSMF server to access the SAF authorization services.
SERVER	BBG.AUTHMOD.BBGZSAFM.TXRRS	IZUSVR	READ	Allow the z/OSMF server to access the transaction services.
SERVER	BBG.AUTHMOD.BBGZSAFM.ZOSDUMP	IZUSVR	READ	Allow the z/OSMF server to access the SVC dump services.

Table 35. Security setup requirements for z/OSMF core functions (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
SERVER	BBG.AUTHMOD.BBGZSAFM.ZOSWLM	IZUSVR	READ	Allow the z/OSMF server to access the WLM services.
SERVER	BBG.SECCLASS.ZMFAPLA	IZUSVR	READ	Allow the z/OSMF server to authorize checks for the ZMFAPLA class.
SERVER	BBG.SECPFX.<*SAF-prefix*>	IZUSVR	READ	Allow the z/OSMF server to make authentication calls against the APPL-ID.
STARTED	IZUINSTP.IZUINSTP	IZUADMIN	N/A	Defines the started task for the z/OSMF dependent address space, which is used to determine whether z/OS UNIX and TCP/IP are available. The job name must be IZUINSTP. Otherwise, the z/OSMF dependent address space is not initialized during z/OSMF autostart processing.
STARTED	IZUSVR1.*jobname*	IZUADMIN	N/A	Define the started task for the z/OSMF server process.
STARTED	IZUANG1.*jobname*	IZUADMIN	N/A	Define the started task for the z/OSMF angel process.
TSOAUTH	CONSOLE	IZUADMIN IZUUSER	READ	Allow the user to issue the TSO/E CONSOLE command to activate the extended MCS console.
TSOPROC	IZUFPROC	IZUADMIN IZUUSER	READ	Allows callers to access the procedure for the z/OSMF REST interfaces, as described in "Updating your system for the z/OSMF REST interfaces" on page 24.
ZMFAPLA	<*SAF-prefix*>.ZOSMF	IZUADMIN IZUGUEST IZUUSER IZUSECAD	READ	Designates the user as a z/OSMF user, rather than a guest user. This authorization is the minimum requirement for allowing a user to do more than log in to z/OSMF and view the Welcome page. Without this authorization, the logged-in user is treated as an authenticated guest. Use the other ZMFAPLA resource names that follow in this table to create specific controls for each core function and task. See Table Notes 1 and 2.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.ADMINTASKS.APPLINKING	IZUADMIN	READ	Allow the user to access the Application Linking Manager task.

Table 35. Security setup requirements for z/OSMF core functions (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
ZMFAPLA	*<SAF-prefix>*.ZOSMF.ADMINTASKS.IMPORTMANAGER	IZUADMIN	READ	Allow the user to access the Import Manager task.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.ADMINTASKS.LINKSTASK	IZUADMIN	READ	Allow the user to access the Links task.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.ADMINTASKS.LOGGER	IZUADMIN	READ	Allow the user to manage the settings that control the behavior and content of the z/OSMF logs. This capability is used only in service situations.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.ADMINTASKS.UI_LOG _MANAGEMENT	IZUADMIN	READ	Allow the user to manage the settings that control the behavior of the user interface (UI) portion of z/OSMF logging. This capability is used only in service situations.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.ADMINTASKS.USAGESTATISTICS	IZUADMIN	READ	Allow the user to collect usage statistics about z/OSMF.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.LINK.*linkName*	IZUADMIN IZUUSER	READ	Allow the user to view an installation-specified link. See Table Notes 3 and 4.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.LINK.SHOPZSERIES	IZUADMIN IZUUSER	READ	Allow the user to view the ShopzSeries web site link.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.LINK.SUPPORT_FOR_Z_OS	IZUADMIN IZUUSER	READ	Allow the user to view the Support for z/OS web site link.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.LINK.SYSTEM_Z_REDBOOKS	IZUADMIN IZUUSER	READ	Allow the user to view the IBM Redbooks® web site link.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.LINK.WSC_FLASHES _TECHDOCS	IZUADMIN IZUUSER	READ	Allow the user to view the WSC Flashes and Techdocs web site link.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.LINK.Z_OS_BASICS _INFORMATION_CENTER	IZUADMIN IZUUSER	READ	Allow the user to view the z/OS Basic Skills Information Center web site link.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.LINK.Z_OS_HOME_PAGE	IZUADMIN IZUUSER	READ	Allow the user to view the z/OS Home Page web site link.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.LINK.Z_OS_INTERNET_LIBRARY	IZUADMIN IZUUSER	READ	Allow the user to view the z/OS Library web site link.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.NOTIFICATION.MODIFY	IZUADMIN IZUUSER	READ	Allow the user to compose a notification.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.NOTIFICATION.SETTINGS	IZUADMIN IZUUSER	READ	Allow the user to define an mail account for receiving notifications from z/OSMF. This action is performed through the Notification Settings task of z/OSMF.

Table 35. Security setup requirements for z/OSMF core functions (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
ZMFAPLA	<*SAF-prefix*>.ZOSMF.NOTIFICATION.SETTINGS.ADMIN	IZUADMIN	READ	Allow the user to manage the z/OSMF notification settings for mobile devices, push services, and SMTP server properties.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.SETTINGS.FTP_SERVERS	IZUADMIN IZUUSER	READ	Allow the user to access the FTP Servers task.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.SETTINGS.FTP_SERVERS.VIEW	IZUADMIN IZUUSER	READ	Allow the user to access the FTP Servers task *View* function.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.SETTINGS.FTP_SERVERS.MODIFY	IZUADMIN	READ	Allow the user to access the z/OSMF Task Settings task *Modify* function.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.SETTINGS.SYSTEMS	IZUADMIN IZUUSER	READ	Allow the user to access the Systems task.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.SETTINGS.SYSTEMS.VIEW	IZUADMIN IZUUSER	READ	Allow the user to access the Systems task *View* function.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.SETTINGS.SYSTEMS.MODIFY	IZUADMIN	READ	Allow the user to access the z/OSMF Task Settings task *Modify* function.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.VARIABLES.SYSTEM.ADMIN	IZUADMIN	READ	Allows the user to access the system variables in the Systems task.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.WORKFLOW.ADMIN	IZUADMIN	READ	Allow the user to change the assigned owner of a workflow.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.WORKFLOW.WORKFLOWS	IZUADMIN IZUSECAD IZUUSER	READ	Allow the user to access the z/OSMF Workflows task. See Table Note 5.

1. User authorizations to functions, tasks, and links are controlled through the system authorization facility (SAF) profile prefix. By default, the SAF prefix is IZUDFLT.
2. Users require READ access to at least the profile <*SAF-prefix*>.ZOSMF to do work in z/OSMF. Without this authorization, the user is treated as an authenticated guest. That is, the user can log in to z/OSMF and display the Welcome page, but cannot access the z/OSMF functions and tasks.
3. In a default z/OSMF configuration, all users are granted authority to all links through a wildcarded profile: <*SAF-prefix*>.ZOSMF.LINK.* *
4. You must provide a SAF resource name prefix for any links that you add to z/OSMF. You can control access to specific links by specifying a unique resource name for the link, for example, by including the link name as part of the resource name. For example: `IZUDFLT.ZOSMF.LINK.`**`mylink`**

   For more information about defining links to z/OSMF, see Chapter 13, "Adding links to z/OSMF," on page 185.
5. A user with access to the Workflows task can access any of the workflows that are displayed in the Workflows task. By default, the z/OSMF defined security groups IZUADMIN, IZUSECAD, and IZUUSER have access to the Workflows task.
6. If your installation uses hardware cryptography with z/OS Integrated Cryptographic Service Facility (ICSF), be aware that services such as CSFRNGL, CSFDSV, CSFOWH, CSFIQF, and others, might be protected through profiles that are established in your external security manager, such as RACF. In some cases, z/OSMF uses these services; therefore, you must permit the z/OSMF started task user ID

to these profiles. For more information, see "Resource authorizations for hardware cryptography" on page 299.

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

Resource authorizations for hardware compression

If your installation uses IBM zEnterprise® Data Compression (zEDC), the z/OSMF server requires READ access to the FPZ.ACCELERATOR.COMPRESSION resource in the FACILITY class. Otherwise, if this authorization is not in place, the z/OSMF server runs without the use of zEDC. The system issues an error message, such as the following:

```
XAT1 IZUSVRU  IZUSVR1 RACF ACCESS violation for IZUSVRU:
(READ,NONE) on FACILITY FPZ.ACCELERATOR.COMPRESSION
```

You can ignore the message.

Table 36 on page 299 shows which permissions must be granted to the z/OSMF server user ID. Commands for the creating the permissions are included in commented sections in the IZUSEC job. To issue the commands when the job runs, uncomment the sections.

Table 36. Security setup requirements for IBM zEnterprise Data Compression (zEDC)

Resource class	Resource name	Who needs access?	Type of access required	Why
FACILITY	FPZ.ACCELERATOR. COMPRESSION	IZUSVR	READ	Enable the z/OSMF server to run with IBM zEnterprise Data Compression (zEDC).

Resource authorizations for hardware cryptography

If your installation uses hardware cryptography with z/OS Integrated Cryptographic Service Facility (ICSF), the z/OSMF server requires access to the ICSF callable services. Table 37 on page 299 shows which permissions must be granted to the z/OSMF server user ID. Commands for the creating the permissions are included in commented sections in the IZUSEC job. To issue the commands when the job runs, uncomment the sections.

Table 37. Security setup requirements for hardware cryptography with ICSF

Resource class	Resource name	Who needs access?	Type of access required	Why
CSFSERV	CSFIQF	IZUSVR	READ	ICSF query facility callable service.
CSFSERV	CSFENC	IZUSVR	READ	Encipher callable service.
CSFSERV	CSFCVE	IZUSVR	READ	Cryptographic variable encipher callable service.
CSFSERV	CSFDEC	IZUSVR	READ	Decipher callable service.
CSFSERV	CSFSAE	IZUSVR	READ	Symmetric algorithm encipher callable service.
CSFSERV	CSFSAD	IZUSVR	READ	Symmetric algorithm decipher callable service.
CSFSERV	CSFOWH	IZUSVR	READ	One-way hash generate callable service.
CSFSERV	CSFRNG	IZUSVR	READ	Random number generate callable service.
CSFSERV	CSFRNGL	IZUSVR	READ	Random number generate long callable service.

Table 37. Security setup requirements for hardware cryptography with ICSF (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
CSFSERV	CSFPKG	IZUSVR	READ	PKA key generate callable service.
CSFSERV	CSFDSG	IZUSVR	READ	Digital signature generate service.
CSFSERV	CSFDSV	IZUSVR	READ	Digital signature verify callable service.
CSFSERV	CSFPKT	IZUSVR	READ	PKA key generate callable service.
CSFSERV	CSFRKL	IZUSVR	READ	Retained key list callable service.
CSFSERV	CSFPKX	IZUSVR	READ	PKA Public Key Extract callable service.
CSFSERV	CSFPKE	IZUSVR	READ	PKA encrypt callable service.
CSFSERV	CSFPKD	IZUSVR	READ	PKA decrypt callable service.
CSFSERV	CSFPKI	IZUSVR	READ	PKA key import callable service.
CSFSERV	CSFCKM	IZUSVR	READ	Multiple clear key import callable service.
CSFSERV	CSFKGN	IZUSVR	READ	Multiple clear key import callable service.
CSFSERV	CSFEDH	IZUSVR	READ	ECC Diffie-Hellman callable service.

Resource authorizations for Common Information Model

If your z/OSMF configuration includes tasks that use the Common Information Model (CIM) server on the host z/OS system, users of the plug-ins require the proper level of access to CIM server resources.

These authorizations are required for using any of the following optional plug-ins or core functions:

- Capacity Provisioning
- Incident Log
- Workload Management
- The asynchronous job notifications function of z/OSMF, which is described in Chapter 12, “Configuring your system for asynchronous job notifications,” on page 175.

CIM includes the CFZSEC job to help you create these authorizations. See the topic on CIM server quick setup and verification in *z/OS Common Information Model User's Guide*. IBM supplies the CFZSEC job in SYS1.SAMPLIB. If your installation does not plan to run the CFZSEC job, ensure that z/OSMF users, and, if you are configuring the Workload Management plug-in, the z/OSMF server user ID, have UPDATE access to the CIMSERV profile in the WBEM class. If necessary, refresh the WBEM class.

For more information about CIM authorization requirements, see “Reviewing your CIM server setup” on page 105.

Table 38 on page 300 lists the CIM security groups that are required for the optional plug-ins.

Table 38. CIM groups that might be required for the optional plug-ins

Group	Purpose	Default group ID (GID)	Created by
CFZADMGP	Security group for the CIM administrator role.	9502	Member CFZSEC in SYS1.SAMPLIB.
CFZUSRGP	Security group for the CIM user role. This group grants a user access to all resources that are managed through CIM. Depending on how granular you want to control user access to CIM, your installation might have created more groups to allow access to only a subset of resources that are managed through CIM.	9503	Member CFZSEC in SYS1.SAMPLIB.

With the IZUAUTH job, your security administrator can supply the names of the CIM groups, based on your selection of optional plug-ins. These values include the names of the CIM administrators group (by default, CFZADMGP) and the CIM users group (by default, CFZUSRGP). The IZUAUTH job contains commands for connecting users to the groups and thus, depend on the groups to exist.

Resource authorizations for Capacity Provisioning Manager

If your z/OSMF configuration includes the Capacity Provisioning plug-in, users of the plug-in must be defined and authorized for all resources that are accessed by the Provisioning Manager. IBM provides the CPOSEC1 and CPOSEC2 jobs in SYS1.SAMPLIB to help you create these authorizations when you set up a Capacity Provisioning domain. For more information, see the topic on setting up a Capacity Provisioning domain in *z/OS MVS Capacity Provisioning User's Guide*.

Table 39 on page 301 lists the default values for the Provisioning Manager. Your installation might have selected different values for these settings.

Table 39. Name information for a Capacity Provisioning domain

Provisioning Manager setting	Default value
Domain name	DOMAIN1
Started task procedure name	CPOSERV
High-level qualifier for runtime data set	CPO
Provisioning Manager user	CPOSRV

With the IZUCPSEC job, your security administrator can supply the names of the security groups that your installation created for authorizing users to the Provisioning Manager on your system. The IZUAUTH job contains commands for connecting users to the groups and thus, depend on the groups to exist.

Table 40 on page 301 lists the security groups that are required for the Capacity Provisioning plug-in.

Table 40. Security groups required for the Capacity Provisioning plug-in

Group	Purpose	Default group ID (GID)	Created by
CPOCTRL	Security group for users of the Capacity Provisioning task *Edit* function.	None; your installation must specify a GID for this group.	Member CPOSEC1 in SYS1.SAMPLIB.
CPOQUERY	Security group for users of the Capacity Provisioning task *View* function.	None; your installation must specify a GID for this group.	Member CPOSEC1 in SYS1.SAMPLIB.

Resource authorizations for common event adapter (CEA)

If your z/OSMF configuration includes tasks that use the common event adapter (CEA) component on the z/OS host system, users of the plug-ins require the proper level of access to CEA resources. IBM provides the CEASEC job in SYS1.SAMPLIB to help you create these authorizations.

These authorizations are needed if you plan to use one or more of the following z/OSMF tasks:

- Incident Log

- ISPF
- Sysplex Management

CEA has security profiles in the SERVAUTH class for protecting different portions of its processing. When you run the IZUILSEC job, you permit the z/OSMF groups to the CEA resources.

For more information, see the topic on customizing for CEA in *z/OS Planning for Installation*.

Resource authorizations for the z/OS console REST interface

In z/OSMF, users require access to z/OS console services when they use the following functions:

- z/OS console REST interface
- z/OS Operator Consoles
- IBM Cloud Provisioning and Management for z/OS, when using templates that issue operator commands or check for unsolicited command responses.

Users of the z/OS console REST interface require access to an extended MCS (EMCS) console for issuing commands and receiving console messages. Specifically, users require the following authorizations:

- READ access to the MVS.MCSOPER.*consolename* resource in the OPERCMDS class, where *consolename* is the name of the EMCS console that is used to issue the command.
- READ access to the CONSOLE resource in the TSOAUTH class.
- READ access to the *<SAF_PREFIX>*`.IzuManagementFacilityRestConsoles.izuUsers` resource in the EJBROLE class. Or, READ access to the *<SAF_PREFIX>*`.*.izuUsers` profile in the EJBROLE class.

z/OSMF uses TSO/E address space services to create a TSO address space as the host for the EMCS console. Therefore, users of the z/OS console REST interface require the following authorizations:

- READ access to the resource *account* in the ACCTNUM class, where *account* is the value that is specified in the COMMON_TSO ACCT option in parmlib member IZUPRMxx.
- READ access to the resource CEA.CEATSO.TSOREQUEST in the SERVAUTH class.
- READ access to the resource *proc* in the TSOPROC class, where *proc* is the value that is specified with the COMMON_TSO PROC option in parmlib member IZUPRMxx.

Also, the z/OSMF started task user ID, which is IZUSVR by default, requires READ access to the resource CEA.CEATSO.TSOREQUEST in the SERVAUTH class.

You can control which parameters are used for creating the TSO address space by setting the appropriate parameters in parmlib member IZUPRMxx. For example:

```
COMMON_TSO ACCT(IZUACCT) REGION(50000) PROC(IZUFPROC)
```

Ensure that your settings are configured before the z/OS console REST interface is used. Otherwise, the default values (shown here) are used.

The attributes of the EMCS console that is started by z/OSMF are controlled by the OPERPARM settings of the user profile *<consolename>*. Thus, for example, if a user wants the z/OS Operator Consoles task to create a console named `console1`, a user profile named `console1` must exist and contain an OPERPARM segment with the appropriate settings.

Most IBM Cloud Provisioning and Management for z/OS templates use the *defcn* Console REST API endpoint, which expects a predefined console name. The convention is to use *userid* plus "CN", where the value for *userid* is truncated to the first six characters. For example, if the user ID is IBMUSER, the *defcn* value is expected to be `IBMUSECN`.

Typically, z/OSMF uses the following console attributes from the user's OPERPARM segment:

AUTH
Specifies the command authority for the console.

ROUTCODE
Specifies the routing codes for the console, which affects which messages can be received by the console. The default value is NONE, which prevents the console from receiving any messages.

MSCOPE
Specifies the system message scope in the sysplex.

For more information about setting these attributes, see the commented sections in SAMPLIB jobs IZUGCSEC and IZUPRSEC. For information about creating OPERPARM segments for users, see *z/OS MVS Planning: Operations*.

In addition to the local system (the system on which z/OSMF is installed), users can enter system commands on other systems in the sysplex. To do so, users require READ access to the resource MVS.ROUTE.CMD.*<sysname>* in the OPERCMDS class.

Users can retrieve messages from OPERLOG or SYSLOG. To do so, users require the following authorizations:

- To retrieve messages from OPERLOG, users require READ access to the resource SYSPLEX.OPERLOG in the LOGSTRM class.
- To retrieve messages from SYSLOG, users require READ access to the resource *<sysname>*.+MASTER +.SYSLOG.*.* in the JESSPOOL class.

Table 41 on page 303 summarizes the security requirements for users of the z/OS console REST interface. IBM provides job IZUGCSEC in SYS1.SAMPLIB to assist you with performing these updates. The job contains RACF commands for creating the required security authorizations.

Table 41. Security setup requirements for the z/OS console REST interface

Resource class	Resource name	Who needs access?	Type of access required	Why
N/A	User profile *<consolename>* with the appropriate OPERPARM segment.	N/A	N/A	The attributes of the EMCS console that is started by the z/OS Operator Consoles task are controlled by the OPERPARM setting of user profile *<consolename>*. The setting of OPERPARM can restrict which messages are received by the EMCS console and limit the commands that the EMCS console can issue.
ACCTNUM	IZUACCT	Users of the z/OS console services REST interface.	READ	Allow the user to access the account number for the procedure for the z/OS console services, as described in "Updating your system for the z/OSMF REST interfaces" on page 24.
EJBROLE	*<SAF-prefix>* .IzuManagementFacilityRestConsoles .izuUsers	Users of: • z/OS console services • z/OS Operator Consoles task.	READ	Allow the user to use the z/OS console services to issue operator commands.
EJBROLE	*<SAF-prefix>* .IzuManagementFacilityTsoServices .izuUsers	IZUADMIN	READ	Allow the user of the Operator Consoles task to start or reconnect to address spaces on other systems in the sysplex.
JESSPOOL	*<sysname>*.+MASTER+ .SYSLOG.*.*	Users of the z/OS Operator Consoles task.	READ	Allows the user to retrieve messages from SYSLOG by using the z/OS Operator Consoles task.
LOGSTRM	SYSPLEX.OPERLOG	Users of the z/OS Operator Consoles task.	READ	Allows the user to retrieve messages from OPERLOG by using the z/OS Operator Consoles task.

Table 41. Security setup requirements for the z/OS console REST interface (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
OPERCMDS	MVS.MCSOPER.*consolename*	Users of the z/OS console services REST interface.	READ	Allow the user to operate the specified extended MCS console.
OPERCMDS	MVS.ROUTE.CMD.<*sysname*>	Users of the z/OS Operator Consoles task.	READ	Allows the user to use the **ROUTE** command to route commands to another system in sysplex, which is indicated by *sysname*. Otherwise, the user is limited to entering commands on the local system (the system on which z/OSMF is installed).
SERVAUTH	CEA.CEATSO.TSOREQUEST	Users of the z/OS console services REST interface.	READ	Allow the user to access the CEA TSO/E address space services. This setting allows HTTP client applications on your z/OS system to start and manage TSO/E address spaces.
SERVAUTH	CEA.CEATSO.TSOREQUEST	IZUSVR	READ	Allows the z/OSMF server to access the CEA TSO/E address space services. This setting allows the z/OSMF server to start and manage TSO/E address space services.
TSOAUTH	CONSOLE	Users of the z/OS console services REST interface.	READ	Allow the user to issue the TSO/E CONSOLE command to activate the extended MCS console.
TSOPROC	IZUFPROC	IZUADMIN IZUUSER	READ	Allow the user to access the procedure for the z/OS console services, as described in "Updating your system for the z/OSMF REST interfaces" on page 24.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.CONSOLES.ZOSOPER	Users of the z/OS Operator Consoles task.	READ	Allows the user to view and access the z/OS Operator Consoles task in the z/OSMF navigation tree.

Resource authorizations for the z/OS data set and file REST interface

The z/OS data set and file REST interface requires access to local resources on your z/OS system. Table 42 on page 304 describes the security requirements for the z/OS data set and file REST interface.

For more information about the z/OS data set and file REST interface services, see *IBM z/OS Management Facility Programming Guide*.

Table 42. Security setup requirements for the z/OS data set and file REST interface

Resource class	Resource name	Who needs access?	Type of access required	Why
ACCTNUM	IZUACCT	IZUADMIN IZUUSER	READ	Allows callers to access the account number that is used for the procedure for the z/OS data set and file REST interface services, as described in "Updating your system for the z/OSMF REST interfaces" on page 24.
SERVAUTH	CEA.CEATSO.TSOREQUEST	IZUADMIN IZUUSER	READ	Allows callers to access the CEA TSO/E address space services. This setting allows HTTP client applications on your z/OS system to start and manage TSO/E address spaces.

Table 42. Security setup requirements for the z/OS data set and file REST interface (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
SERVAUTH	CEA.CEATSO.TSOREQUEST	IZUSVR	READ	Allows the z/OSMF server to access the CEA TSO/E address space services. This setting allows the z/OSMF server to start and manage TSO/E address space services.
TSOPROC	IZUFPROC	IZUADMIN IZUUSER	READ	Allows callers to access the procedure for the z/OS data set and file REST interface services, as described in "Updating your system for the z/OSMF REST interfaces" on page 24.

Resource authorizations for the z/OS jobs REST interface

The z/OS jobs REST interface requires access to local resources on your z/OS system. Table 43 on page 305 describes the security requirements for the z/OS jobs REST interface. These authorizations allow the CIM server to interact with the common event adapter (CEA) component. CIM includes the CFZSEC job to help you create these authorizations.

Table 43. Security setup requirements for the z/OS jobs REST interface

Resource class	Resource name	Who needs access?	Type of access required	Why
SERVAUTH	CEA.CONNECT	CFZSRV	READ	If your installation uses the z/OS jobs REST interface, this setting is needed for interactions with the common event adapter (CEA) component.
SERVAUTH	CEA.SUBSCRIBE.*	CFZSRV	READ	If your installation uses the z/OS jobs REST interface, this setting allows HTTP client applications on your z/OS system to receive asynchronous job notifications.
SERVAUTH	CEA.SUBSCRIBE.ENF_0078*	CFZSRV	READ	If your installation uses the z/OS jobs REST interface, this setting allows HTTP client applications on your z/OS system to receive asynchronous job notifications.

For programs that use the z/OS jobs REST interface services to perform job modify operations, the caller's user ID must be authorized to the appropriate resources in the JESJOBS class, as shown in Table 44 on page 305.

Table 44. JESJOBS class authorizations needed for performing job modify operations

Operation	JESJOBS resource	Access required
Hold a job	HOLD.nodename.userid.jobname	UPDATE
Release a job	RELEASE.nodename.userid.jobname	UPDATE
Change the job class	MODIFY.nodename.userid.jobname	UPDATE
Cancel a job	CANCEL.nodename.userid.jobname	ALTER
Delete a job (cancel a job and purge its output)	CANCEL.nodename.userid.jobname	ALTER

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

If run asynchronously, the z/OS jobs REST interface services also require that the caller's user ID is authorized to the CIM server and permitted to the JES2-JES3Jobs CIM provider. CIM includes jobs

(CFZSEC and CFZRCUST) to help you configure the CIM server, including security authorizations and file system customization. For more information, see the topic on CIM server quick setup and verification in *z/OS Common Information Model User's Guide*. IBM supplies the CFZSEC job in SYS1.SAMPLIB.

Resource authorizations for the z/OSMF optional plug-ins

The z/OSMF optional plug-ins require access to local resources on your z/OS system. Table 45 on page 306 describes the security requirements that are required for the z/OSMF optional plug-ins. The IZUxxSEC jobs include sample RACF commands for creating these authorizations.

These values can change, based on the values you provide. The values in Table 45 on page 306 are based on the defaults. If your installation uses a different value, such as a different group name, the generated values can change.

Table 45. Security setup requirements for the z/OSMF optional plug-ins

Resource class	Resource name	Who needs access?	Type of access required	Why
Capacity Provisioning. The following access controls must be set for the Capacity Provisioning plug-in. For additional authorizations, see Table Notes 1 and 2.				
EJBROLE	<*SAF-prefix*>.IzuManagementFacilityCapacityProvisioning.izuUsers	IZUADMIN IZUUSER	READ	Allow the user to connect to the Capacity Provisioning task.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_ PROVISIONING.EDIT	IZUADMIN	READ	Allow the user to access the Capacity Provisioning task *Edit* function.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_ PROVISIONING.EDIT.DOMAIN	IZUADMIN	READ	Allow the user to use the Capacity Provisioning task *Edit* function to edit a Capacity Provisioning domain.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_ PROVISIONING.EDIT.POLICY	IZUADMIN	READ	Allow the user to use the Capacity Provisioning task *Edit* function to edit a Capacity Provisioning policy.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_ PROVISIONING.VIEW	IZUADMIN IZUUSER	READ	Allow the user to access the Capacity Provisioning task *View* function.
Network Configuration Assistant. The following access controls must be set for the Network Configuration Assistant plug-in.				
EJBROLE	<*SAF-prefix*>.IzuConfigurationAssistant.izuUsers	IZUADMIN IZUUSER	READ	Allow the user to connect to the Network Configuration Assistant task.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.CONFIGURATION_ ASSISTANT.CONFIGURATION_ASSISTANT	IZUADMIN IZUUSER	READ	Allow the user to access the Network Configuration Assistant task.
Incident Log. The following access controls must be set for the Incident Log plug-in. For additional authorizations, see Table Notes 1 and 3.				
ALIAS	CEA	N/A	N/A	If your installation has a user catalog set-up instead of using the master catalog, you may need to define CEA alias to the user catalog.

Table 45. Security setup requirements for the z/OSMF optional plug-ins (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
DATASET	CEA.*	IZUADMIN IZUUSER	ALTER	Allow the user to create data sets using the CEA high-level qualifier (HLQ).
DATASET	*your_master_catalog*	IZUADMIN IZUUSER	UPDATE	If your installation has master catalog setup, you might need to permit a user to the master catalog data set class.
EJBROLE	<*SAF-prefix*>.IzuManagementFacilityIncidentLog.izuUsers	IZUADMIN IZUUSER	READ	Allow the user to connect to the Incident Log task.
JESSPOOL	*your_system_name*.+MASTER+.SYSLOG.*.*	CEA	READ	If your installation is using the system log (SYSLOG) as the source for diagnostic log snapshots, the CEA user ID requires READ access to the JESSPOOL class. This authorization allows the JES subsystem to access SYSLOG on behalf of the common event adapter (CEA) component.
SERVAUTH	CEA.CEADOCONSOLECMD	IZUADMIN IZUUSER	READ	Allow the calling program to issue operator commands to accomplish its function.
SERVAUTH	CEA.CEADOCMD	IZUADMIN IZUUSER	READ	Allow the user to cancel the FTP job.
SERVAUTH	CEA.CEAGETPS	IZUADMIN IZUUSER	READ	Allow the user to obtain information about the FTP job.
SERVAUTH	CEA.CEAPDWB.CEACHECKSTATUS	IZUADMIN IZUUSER	READ	Allow the user to check status and return incident information.
SERVAUTH	CEA.CEAPDWB.CEADELETEINCIDENT	IZUADMIN IZUUSER	READ	Allow the user to delete selected incidents, including the dumps, all diagnostic snapshot files and the corresponding sysplex dump directory entry.
SERVAUTH	CEA.CEAPDWB.CEAGETINCIDENT	IZUADMIN IZUUSER	READ	Allow the user to obtain data associated with a specific incident.
SERVAUTH	CEA.CEAPDWB.CEAGETINCIDENTCOLLECTION	IZUADMIN IZUUSER	READ	Allow the user to obtain collection of incident data for all incidents that match a filter.
SERVAUTH	CEA.CEAPDWB.CEAPREPAREINCIDENT	IZUADMIN IZUUSER	READ	Allow the user to prepare data for FTP (locate and compress/ terse).
SERVAUTH	CEA.CEAPDWB.CEASETINCIDENTINFO	IZUADMIN IZUUSER	READ	Allow the user to set information that is associated with the incident, such as the Notes field.

Table 45. Security setup requirements for the z/OSMF optional plug-ins (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
SERVAUTH	CEA.CEAPDWB.CEASETPROBLEMTRACKINGNUMBER	IZUADMIN IZUUSER	READ	Allow the user to set a problem ID, such as a PMR number, or problem management tracking ID.
SERVAUTH	CEA.CEAPDWB.CEAUNSUPPRESSDUMP	IZUADMIN IZUUSER	READ	Allow user to allow a dump that is marked for suppression through DAE to be taken.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.INCIDENT_LOG.INCIDENT_LOG	IZUADMIN IZUUSER	READ	Allow the user to access the Incident Log task.
ISPF. The following access controls must be set for the ISPF plug-in. For more authorizations, see Table Note 3.				
EJBROLE	*<SAF-prefix>*.IzuManagementFacilityISPF.izuUsers	IZUADMIN IZUUSER	READ	Allow the user to connect to the ISPF task.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.ISPF.ISPF	IZUADMIN IZUUSER	READ	Allow the user to access the ISPF task.
Resource Monitoring. The following access controls must be set for the Resource Monitoring plug-in.				
EJBROLE	*<SAF-prefix>*.IzuManagementFacilityResourceMonitoring.izuUsers	IZUADMIN IZUUSER	READ	Allow the user to connect to the Resource Monitoring and System Status tasks.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.RESOURCE_MONITORING.PERFDESKS	IZUADMIN IZUUSER	READ	Allow the user to access the Resource Monitoring task.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.RESOURCE_MONITORING.OVERVIEW	IZUADMIN IZUUSER	READ	Allow the user to access the System Status task.
Software Deployment. The following access controls must be set for the Software Deployment plug-in.				
EJBROLE	*<SAF-prefix>*.IzuManagementFacilitySoftwareDeployment.izuUsers	IZUADMIN IZUUSER	READ	Allow the user to connect to the Software Management task.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_ MANAGEMENT	IZUADMIN IZUUSER	READ	Allow the user to access the Software Management task.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.SOFTWARE_ DEPLOYMENT.DATA.*objectType.objectSuffix* For more information about the possible values for *objectType* and *objectSuffix*, see "Creating access controls for the Software Management task" on page 135.	IZUADMIN IZUUSER	CONTROL	Allow the user to access the Software Management task objects.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_ MANAGEMENT.PRODUCT _INFO_FILE.RETRIEVE	IZUADMIN	READ	Allow the user to access the Software Management task *Product Information File Retrieve* function.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_ MANAGEMENT.CATEGORIES.MODIFY	IZUADMIN	READ	Allow the user to add, copy, modify, or remove Software Management categories.
UNIXPRIV	SUPERUSER.FILESYS.MOUNT	IZUADMIN IZUUSER	UPDATE	Allow the user to create workflow instances from workflow definition files that reside in UNIX file systems that are not currently mounted.

Table 45. Security setup requirements for the z/OSMF optional plug-ins (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
Sysplex Management. The following access controls must be set for the Sysplex Management plug-in.				
EJBROLE	*<SAF-prefix>*.IzuManagementFacilitySysplexManagement.izuUsers	IZUADMIN IZUUSER	READ	Allow the user to connect to the Sysplex Management task.
SERVAUTH	CEA.XCF.CDS	IZUADMIN IZUUSER	READ	Allow the user to access the couple data set for the Sysplex Management task.
SERVAUTH	CEA.XCF.CF	IZUADMIN IZUUSER	READ	Allow the user to access the coupling facility for the Sysplex Management task.
SERVAUTH	CEA.XCF.FLOW.<sysname>	IZUADMIN IZUUSER	READ	Allow the user to access the sysplex resources on remote systems for the Sysplex Management task. Replace <sysname> with the 8 character name of the system in the sysplex.
SERVAUTH	CEA.XCF.STRUCTURE	IZUADMIN IZUUSER	READ	Allow the user to access the coupling facility structures for the Sysplex Management task.
SERVAUTH	CEA.XCF.SYSPLEX	IZUADMIN IZUUSER	READ	Allow the user to access the sysplex general information and systems for the Sysplex Management task.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.SYSPLEX	IZUADMIN IZUUSER	READ	Allow the user to access the Sysplex Management task.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.SYSPLEX.LOG	IZUADMIN or a particular z/OS user ID.	READ	Allow the user to use the Sysplex Management task to clean up the command log table and specify clean-up settings.
ZMFAPLA	*<SAF-prefix>*.ZOSMF.SYSPLEX.MODIFY	IZUADMIN	READ	Allow the user to use the Sysplex Management task to modify sysplex resources.
Workload Management. The following access controls must be set for the Workload Management plug-in. For additional authorizations, see Table Note 1.				
EJBROLE	*<SAF-prefix>*.IzuManagementFacilityWorkloadManagement.izuUsers	IZUADMIN IZUUSER	READ	Allow the user to connect to the Workload Management task.
FACILITY	MVSADMIN.WLM.POLICY	IZUSVR	READ	Allow the z/OSMF server to access the WLM policies.

Table 45. Security setup requirements for the z/OSMF optional plug-ins (continued)

Resource class	Resource name	Who needs access?	Type of access required	Why
ZMFAPLA	<*SAF-prefix*>.ZOSMF.WORKLOAD_MANAGEMENT. WORKLOAD_ MANAGEMENT.ENWRP	IZUADMIN WLM resource pool administration group	READ	For z/OS Cloud Provisioning, allow the user to access the WLM Resource Pooling (WRP) functions of z/OSMF. Using a WRP definition, the user can associate cloud information (tenant name, domain ID, template type, service levels supported) with WLM elements (report classes and classification rules).
ZMFAPLA	<*SAF-prefix*>.ZOSMF.WORKLOAD_MANAGEMENT. WORKLOAD_ MANAGEMENT.VIEW	IZUADMIN IZUUSER	READ	Allow the user to access the Workload Management *View* function.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.WORKLOAD_MANAGEMENT. WORKLOAD_ MANAGEMENT.MODIFY	IZUADMIN	READ	Allow the user to access the Workload Management *Modify* function.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.WORKLOAD_MANAGEMENT. WORKLOAD_ MANAGEMENT.INSTALL	IZUADMIN	READ	Allow the user to access the Workload Management *Install* function.
IBM zERT Network Analyzer. The following access controls must be set for the IBM zERT Network Analyzer plug-in.				
EJBROLE	<*SAF-prefix*>.IzuZertNetworkAnalyzer.izuUsers	IZUZNA	READ	Allow the user to connect to the IBM zERT Network Analyzer task.
EJBROLE	<*SAF-prefix*>.com.ibm.ws.management.security.resource.Administrator	IZUZNA	READ	Allow the IBM zERT Network Analyzer to perform WebSphere Liberty administrative actions.
ZMFAPLA	<*SAF-prefix*>.ZOSMF	IZUZNA	READ	Designates the user as a z/OSMF user.
ZMFAPLA	<*SAF-prefix*>.ZOSMF.ZERT_NETWORK_ANALYZER	IZUZNA	READ	Allow the user to access the IBM zERT Network Analyzer task.

Table Notes:

1. This plug-in requires the CIM server; thus, you must also create the authorizations that are described in “Resource authorizations for Common Information Model” on page 300.
2. Users of this plug-in must be authorized for resources that are accessed by the Provisioning Manager. IBM provides the CPOSEC1 and CPOSEC2 jobs in SYS1.SAMPLIB to help you create these authorizations. For more information, see the topic on setting up a Capacity Provisioning domain in *z/OS MVS Capacity Provisioning User's Guide*.
3. Users of this plug-in must be authorized for resources that are accessed by the common event adapter (CEA) component of z/OS. IBM provides the CEASEC job in SYS1.SAMPLIB to help you create these authorizations. See “Resource authorizations for common event adapter (CEA)” on page 301.
4. If your installation plans to use the IBM Cloud Provisioning tasks, you might have more WLM authorizations to create. See “Resource authorizations for WLM administrators” on page 68.

Appendix B. z/OSMF Configuration Workflow

This topic describes how to use the z/OSMF Configuration Workflow to perform the system customization for the z/OSMF optional plug-ins.

Chapter 7, "Customizing your z/OS system for the z/OSMF plug-ins," on page 105 describes the manual steps that are required for customizing your system for the z/OSMF optional plug-ins. As an alternative, you can use the z/OSMF Configuration Workflow to perform the system customization for each plug-in. If you use the workflow, you are guided through the system customization steps.

About the z/OSMF Configuration Workflow

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

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

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

To run the z/OSMF Configuration Workflow, you require a user ID that is connected to the z/OSMF Administrator security group, which is IZUADMIN, by default. Your user ID also requires:

- RACF SPECIAL attribute, which gives the user full control over the RACF profiles in the RACF database.
- Authorizations that are described in "Grant the user access to the IRRXUTIL program" on page 311 and "Grant the user access to the OPERCMDS resources" on page 312.

If you prefer, you can manually perform the system customization for each plug-in. For descriptions of the customization that must be performed for each plug-in, see Chapter 7, "Customizing your z/OS system for the z/OSMF plug-ins," on page 105.

Grant the user access to the IRRXUTIL program

The z/OSMF Configuration Workflow uses the IRRXUTIL program to retrieve profile information about users, groups, general resources, and general RACF settings administered by the SETROPTS command. Therefore, your user ID requires READ authorization to the resource names listed in Table 46 on page 312.

Table 46. IRRXUTIL program authorizations required for using the z/OSMF Configuration Workflow			
Resource name	**Class**	**Access**	**Purpose**
IRR.RADMIN.LISTUSER	FACILITY	READ	Read USER profiles.
IRR.RADMIN.LISTGRP	FACILITY	READ	Read group profiles.
IRR.RADMIN.RLIST	FACILITY	READ	Read profiles of general resources.
IRR.RADMIN.SETROPTS.LIST	FACILITY	READ	Read RACF SETROPTS settings.

The IZUSEC job contains sample RACF commands for creating these authorizations. Figure 62 on page 312 shows the commands that are provided in the job.

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

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

SETROPTS RACLIST(FACILITY) REFRESH
```

Figure 62. RACF commands for authorizing the users of the z/OSMF Configuration Workflow

Grant the user access to the OPERCMDS resources

The z/OSMF Configuration Workflow uses the extended MCS console to issue operator commands. Therefore, your user ID requires READ authorization to the CONSOLE profile of the TSOAUTH class. Also, if the OPERCMDS class is active on your system, your user ID requires READ authorization to the generic profile `MVS.MCSOPER.IZU@*`. These authorization requirements are summarized in Table 47 on page 312.

Table 47. OPERCMDS authorizations required for using the z/OSMF Configuration Workflow			
Resource name	**Class**	**Access**	**Purpose**
MVS.MCSOPER.IZU@*	OPERCMDS	READ	Allow the user to operate an extended MCS console.
CONSOLE	TSOAUTH	READ	Allow the user to issue the TSO/E CONSOLE command to activate the extended MCS console.

The IZUSEC job contains sample RACF commands for creating these authorizations. Figure 63 on page 313 shows the commands that are provided in the job.

```
/* Allow workflow users to issue MVS commands from EMCS consoles */
SETROPTS CLASSACT(TSOAUTH)
SETROPTS RACLIST(TSOAUTH)
RDEFINE TSOAUTH CONSOLE UACC(NONE)
PERMIT CONSOLE CLASS(TSOAUTH) ID(IZUADMIN) ACCESS(READ)
PERMIT CONSOLE CLASS(TSOAUTH) ID(IZUUSER) ACCESS(READ)

SETROPTS RACLIST(TSOAUTH) REFRESH

/* Allow workflow users to access EMCS consoles. The console names are */
/* prefixed with the value “IZU@” */
SETROPTS CLASSACT(OPERCMDS)
SETROPTS RACLIST(OPERCMDS)
RDEFINE OPERCMDS MVS.MCSOPER.IZU@* UACC(NONE)
PERMIT MVS.MCSOPER.IZU@* CLASS(OPERCMDS) ID(IZUADMIN) ACCESS(READ)
PERMIT MVS.MCSOPER.IZU@* CLASS(OPERCMDS) ID(IZUUSER) ACCESS(READ)

SETROPTS RACLIST(OPERCMDS) REFRESH
```

Figure 63. OPERCMDS authorizations that are required for using the z/OSMF Configuration Workflow

Getting started

To create the z/OSMF Configuration Workflow, import the following workflow definition file into the Workflows task:

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

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

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

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

where `<user_dir>` is the data directory. By default, this directory is `/global/zosmf`.

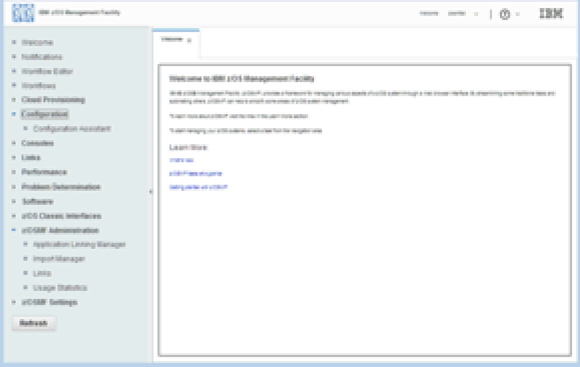
More information about the Workflows task is provided in the online help.

Steps for adding plug-ins to z/OSMF

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

1. Run the z/OSMF Configuration Workflow to customize your system for the plug-ins to be added.
2. Verify the results of your work by opening a web browser to the **Welcome** page. For more information, see “Step 5: Access the z/OSMF Welcome page” on page 30.

Figure 64 on page 314 shows the **Welcome** page after you log in with the installer user ID. Notice that the navigation area now includes expandable categories for the optional plug-ins. Figure 64 on page 314 shows the **Welcome** page as it would appear to the installer, who has access to the z/OSMF Administration and z/OSMF Settings categories by default. A user without administrator access would not see these categories.



Welcome to IBM z/OS Management Facility

[illegible]

[illegible]

[illegible]

Learn More

[illegible]

[illegible]

Getting started with z/OSMF

Figure 64. z/OSMF Welcome page (after optional plug-ins are added)

Appendix C. Common event adapter (CEA) reason codes

A problem in the configuration of z/OSMF might be indicated by reason codes from the common event adapter (CEA) component of z/OS.

This section describes the configuration-related CEA reason codes and includes a cross-reference of reason codes to CIM messages and z/OSMF messages. Where an associated z/OSMF message is indicated, check the z/OSMF message for more information about the error.

"CEA reason codes for the Incident Log task" on page 315 describes the CEA reason codes you might encounter during the configuration of the task. "CEA reason codes for the z/OS jobs REST interface services" on page 318 describes the CEA reason codes that an HTTP client application might encounter when using the z/OS jobs REST interface services. For other CEA reason codes, see the topic on using CEA TSO/E address space services in z/OS MVS Programming: Callable Services for High-Level Languages.

CEA reason codes for the Incident Log task

Table 48 on page 315 describes the CEA reason codes you might encounter when setting up or using the Incident Log task. By default, CEA reason codes without an associated z/OSMF message are accompanied by z/OSMF message IZUP631E.

Table 48. CEA reason codes related to Incident Log task processing

Reason code (decimal)	Reason code (hex)	Description	System programmer action	CIM message	z/OSMF message	IBM Support information
256	100	The CEA address space is not running.	Follow the steps in "Ensure that common event adapter (CEA) is configured and active" on page 124.	CEZ05002E	IZUP634E	CEAUNAVAIL
289	121	CIM indication processing is not available because the CEA address space is running in minimum (MIN) mode. To support Incident Log processing, CEA must be operated in full mode.	Use the **MODIFY CEA,MODE** command to change the CEA mode of operation to full mode. To do so, enter the command, as follows, from the operator console: `F CEA,MODE=FULL` Running CEA in full mode requires that z/OS UNIX system services is available.	CEZ05013E		CEAFORCEMINMODE
813	32D	The user is not authorized for this request.	Define the appropriate authority for the user.	CEZ05003E	IZUP635E	CEANOINSTRAUTH
830	33E	An abend occurred in the CEA task that interacts with the IPCS environment.	Report the problem to IBM Support.	CEZ05001E	IZUP639E	CEAIPRQSERVER ABENDED
834	342	The sysplex dump directory is empty.	Ensure that the sysplex dump directory is not empty.			CEASDDIREMPTY
835	343	A dump incident was not found. Most likely, the incident was deleted by another user.	No action is required.	CEZ05004E	IZUP636E	CEAADDFAILED

Table 48. CEA reason codes related to Incident Log task processing (continued)

Reason code (decimal)	Reason code (hex)	Description	System programmer action	CIM message	z/OSMF message	IBM Support information
850	352	The dump analysis and elimination (DAE) data set name (typically SYS1.DAE) could not be determined. Most likely, DAE is not configured or is not running. Or, the user attempted to unsuppress a dump without having write access to the DAE data set.	Ensure that: • DAE is active. • DAE is configured, as described in z/OS MVS Diagnosis: Tools and Service Aids. • User has write access to the active DAE data set. For more information, see "Configuring dump analysis and elimination" on page 121.		IZUP637E	CEADAEDSN NOTAVAILABLE
855	357	The called function could not generate a prepared data set name (DSN).	Verify that the compiled REXX exec CEACDMPP exists and can be run by System REXX.			CEAGENPREPARED DSNFAIL
857	359	An internal CEA error occurred when attempting to invoke a SYSREXX exec.	If this reason code is accompanied by the following codes (in decimal), check the SYSREXX concatenation for a missing exec: • DIAG=8 • DIAG2=851. Also, check message CEZ05000E in SYSLOG. CEAERRO_Msg contains the name of the SYSREXX exec.	CEZ05000E		CEAAXREXXERROR
866	362	The source description for a requested dump incident was not found in the sysplex dump directory.	Determine why the dump incident was not identified in the sysplex dump directory. Possible reasons include: • Dump has not yet been taken • Dump has not yet been written out • Dump is being entered into a different sysplex dump directory than the one that is used by the Incident Log task.	CEZ05001E	IZUP631E	CEADMPINCIDENT NOTFOUND
869	365	The System REXX address space or the functions it provides are not available.	Follow the steps in "Ensuring that System REXX is set up and active" on page 126.	CEZ05005E	IZUP640E	CEASYSREXX NOTACTIVE
870	366	System REXX cannot process an exec.	This problem usually indicates that the run time support for compiled REXX has not been set up. See "Ensuring that System REXX is set up and active" on page 126.	CEZ05006E	IZUP643E	CEASYSREXXBAD ENVIRONMENT
871	367	System REXX cannot process the exec at this time.	Try the request again later.	CEZ05007 W	IZUP644E	CEAEXECTIMEOUT
872	368	System REXX cannot schedule the exec to run at this time.	Try the request again later.	CEZ05008 W	IZUP645E	CEASYSREXX OVERLOADED
879	36F	The user is not authorized to view the operations log (OPERLOG) snapshot information.	Ask the security administrator to authorize the user to the data set, which is specified in the CEAPRMxx parmlib member.	CEZ05010E		CEANOSAF OPERLOGSNAP

Table 48. CEA reason codes related to Incident Log task processing (continued)

Reason code (decimal)	Reason code (hex)	Description	System programmer action	CIM message	z/OSMF message	IBM Support information
880	370	The system logger component is not available.	For an explanation of the logger reason code in CEAERRO_DIAG4, see mapping macro IXGCON. If the system is not running with a logger couple data set, this is a permanent condition for the IPL. Otherwise restart system logger and enter the request again. For more information, see "Defining a couple data set for system logger" on page 113. For information about the IXGCON macro, see z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG.	CEZ05011E		CEALOGGER NOTAVAIL
881	371	The function that prepares incident materials to be sent through FTP could not allocate a new data set for the tersed diagnostic snapshot.	Check the CIM trace file for system messages associated with the return code indicating the reason for the failure. For assistance, contact IBM Support.			CEABADALLOCNEW
882	372	The function that prepares an incident to be sent through FTP could not allocate the data set to be tersed.	Check the CIM trace file for system messages associated with the return code indicating the reason for the failure. For assistance, contact IBM Support.			CEATERSE BADALLOC1
886	376	The operations log (OPERLOG) snapshot was not created. When attempting to access the OPERLOG snapshot, the system logger service IXGCONN received a bad return or reason code indicating that the OPERLOG snapshot does not exist.	Check SYSLOG for message CEA0600I, which contains the return and reason codes.			CEANOSNAPSHOT
888	378	No log data was accumulated in diagnostic snapshot.	If this problem occurs frequently, adjust the DUMPCAPTURETIME setting in the CEAPRMxx parmlib member.			CEAPDWB DIAGDATAEMPTY
889	379	An incorrect format or value was supplied for the IBM PMR number.	Correct the IBM PMR number and try again. The format of the IBM PMR number should be *nnnnn.ccc.bbb* where *nnnnn* is the PMR number, *bbb* is the branch code, and *ccc* is the country code.			CEAWRONG IBMPMRFORMAT
893	37D	An attempt to obtain the enqueue on the sysplex dump directory failed; another program already holds the enqueue.	Ensure that only one user is attempting to access the dump information at one time. To check for enqueue contention, enter the command **D GRS,C** at the operator console. Wait for the enqueue to be released and try again.	CEZ05017E	IZUP641E	CEAIPCSENQ ERROR
894	37E	The requested function failed to open the sysplex dump directory.	Verify that the sysplex dump directory (default name SYS1.DDIR) is set up and usable. For more information, see "Creating the sysplex dump directory" on page 122.	CEZ05016E	IZUP642E	CEASDDIR OPENERROR
898	382	The component table is corrupted.	Report the problem to IBM Support.			CEAXMLTAGS TOODEEP
901	385	The diagnostic data to be sent is currently in use.	Try the request again later.			CEAPREPARE OBJINUSE
902	386	The diagnostic data to be sent is currently in use.	Try the request again later.			CEAPREPAREENQERR
908	38C	The sysplex dump directory has no space available to record new SVC dumps.	See "Establishing a larger sysplex dump directory" on page 123.			CEACKST INVALIDALLOC VALUE

Table 48. CEA reason codes related to Incident Log task processing (continued)

Reason code (decimal)	Reason code (hex)	Description	System programmer action	CIM message	z/OSMF message	IBM Support information
913	391	The JES subsystem is not available.	Determine why the JES subsystem is not accessible. Perhaps, it has not been started.			CEAJESNOT AVAILABLE
919	397	The Set Incident field data was truncated at 256 characters.	Specify a smaller amount of data for the user comment field to prevent truncation. Retry the request.			CEASETINCIFVAL DATATRUNC
920	398	The request failed because one or more of the affected dump data sets are migrated.	If the data set is migrated and automatic recall is enabled for the hierarchical storage manager (HSM), the system issues a recall request for the data set. Wait for the recall request to complete and then retry the request.			CEAMIGRATED DATASETS
921	399	The request failed because one or more of the requested dump data sets are migrated and the hierarchical storage manager (HSM) encountered an error occurred when attempting to recall the data sets.	Determine why HSM is not functioning properly. The problem might be that HSM is inactive or unresponsive. Correct the problem and retry the request.			CEAMIGRATED DATASETSWHSMERR
922	39A	The request failed because CEA could not allocate an internal buffer to satisfy the request.	Try the request again. If the problem persists, determine why there is insufficient storage on the system. Consider reducing the number of inactive incidents on your system through the **ceatool** program, which is described in Chapter 14, “Deleting incidents and diagnostic data,” on page 189. Correct the problem and retry the request. If the problem persists, contact IBM Support.			CEAUNABLETO ALLOCATE3

CEA reason codes for the z/OS jobs REST interface services

Table 49 on page 318 describes the CEA reason codes that an HTTP client application might encounter when using the z/OS jobs REST interface services.

Table 49. CEA reason codes related to z/OS jobs REST interface processing

Reason code (decimal)	Reason code (hex)	Description	System programmer action	IBM Support information
923	39B	The request failed because the caller is not authorized to modify the job.	Check with your installation’s security administrator to ensure that the caller’s user ID is authorized to the appropriate resources in the JESJOBS class. For the specific authorizations required, see “Resource authorizations for the z/OS jobs REST interface” on page 305.	CEANOJESAUTHORITY
925	39D	An internal CEA error occurred.	Report the problem to IBM Support.	CEANOENTITY POSSIBLE
926	39E	The request failed because the specified job was not found on the system.	Examine the request to determine whether the job was identified correctly, either through the job name and job ID (jobname/jobid), or the job correlator.	CEASSIJOBNOTFOUND

Appendix D. ENF listener code examples

A program can use one of the following methods to determine whether the z/OSMF server is up or down in the sysplex:

- An APF-authorized program can use the ENFREQ LISTEN service to specify a listen exit for ENF event code 83 that tells the program the z/OSMF server is up and running. For an example of this technique, see the coded samples in "Examples for an authorized program" on page 320.
- An unauthorized program cannot use the ENFREQ LISTEN service. However, it can periodically check the global storage pointer, which is mapped by macro IZUGSP. For an example of this technique, see the coded sample in "Example for an unauthorized program" on page 323.

Examples for an authorized program

Example program IZULSTEN shows how an APF-authorized program can listen for z/OSMF server status. IZULISTEN invokes the sample exit routine, IZULST00, which must reside in the link pack area (LPA). Both sample programs are written in assembler language.

- Figure 65 on page 320
- Figure 66 on page 321

```
IZULSTEN  CSECT
IZULSTEN  AMODE 31
IZULSTEN  RMODE ANY

          STM   14,12,12(13)        Save caller's registers
          BALR  12,0                Establish module base

@ESTART   EQU   *
          SAM31                     Ensure 31 bit mode
          USING @ESTART,12          Establish addressability
          MODID                     Eyecatcher and date
          SR    15,15               Set return code to 0

* Set mode to Supervisor State
          WTO   'ENTERING PGM...'
          MODESET MODE=SUP
          MODESET EXTKEY=ZERO,SAVEKEY=(2),WORKREG=7
          LR    8,2                 Save user key

* Load ENF IZULST00 Listen Exit from LPA area
          LOAD  EP=IZULST00,LOADPT=IZULS00@

          SR    15,15               Set return code to 0
          L     2,IZULS00@
          L     4,A31MASK
          OR    2,4             Must be 31-bit addressing

          ST    13,SAVEA+4
          LA    13,SAVEA           Provide save area

          WTO   'Now registering as a listener for ENF code 83.'
* Issue LISTEN Request for z/OSMF event code (all functions)
          ENFREQ ACTION=LISTEN,   -- Function                          +
               CODE=ENFC83,       -- Event code                        +
               EXIT=(2),          -- Exit address                      +
               QUAL=ENF83CUP,     -- z/OSMF is up?                     +
               QMASK=ALL,         -- Set mask of all 4 bytes           +
               ESTBNME=THISMOD,   -- Establisher name                  +
               EXITNME=IZULST00,  -- Exit name                         +
               DTOKEN=IZULTOKN    -- Returned token field
          LTR   15,15
          JNZ   ERRGO
          B     @LEXIT

* Error exit, to print the return code
ERRGO     DS    0H
          ST    15,RETC
          WTO   'ENFREQ request error!'

          MVC   DataToConvert,RETC
          UNPK  ZonedArea,DataToUnpack
          TR    CharData,TRTBL
          MVC   ERRCODE,CharData

          MVC   WTOAREA,WTOLIST
          LA    5,ERRLEN
          STH   5,ERRMSGA
          MVC   ERRMSG,ERRMSGC

          LA    2,ERRMSGA                   Point to message in storage
          WTO   TEXT=(2),MF=(E,WTOAREA)     Write the message

@LEXIT    DS    0H
          LR    2,8                     Restore user key
          MODESET KEYADDR=(2),WORKREG=7
          MODESET MODE=PROB
          WTO   'End of zOSMF listener routine.'
```

Figure 65. Example of an authorized program that listens for z/OSMF server events (Part 1 of 2)

```
* Return control
          L     13,SAVEA+4
          L     14,12(13)                  RESTORE CALLERS REGS
          LM    0,12,20(13)                PRESERVE REG 15 - RC
          BR    14                         RETURN TO CALLER

          DS    0F
ENFC83    EQU   83
ENF83CUP  DC    X'80000000'          z/OSMF is up
A31MASK   DC    X'80000000'          High bit for 31-bit addressing

IZULTOKN   DS    F
ENFPTR    DS    A
SAVEA     DS    18F
RETC      DS    F
IZULST00  DC    CL8'IZULST00'
IZULS00@  DS    A
THISMOD   DC    CL8'IZULSTEN'

* Work area for conversion of addr to char string
DataToUnpack   DS    CL5
               ORG   DataToUnpack
DataToConvert  DS    CL4
DataToCvtXtra  DS    CL1
ZonedArea      DS    CL9
               ORG   ZonedArea
CharData       DS    CL8
ExtraChar      DS    CL1

* Table for converting
TRTBL           DC    XL256'00'
                ORG   TRTBL+240            Advance to offset F0 in table
                DC    C'0123456789ABCDEF'  Get ch 0 (F0x) at off F0
                DS    0F

WTOLIST   WTO   TEXT=,MF=L           List form
WTOLEN    EQU   *-WTOLIST            Length to move
WTOAREA   DS   CL(WTOLEN)   WTO in dyn area for modifiable msgs
ERRMSGC   DC   C'The return code of ENQREQ is: '
*
* Error message format
          DS  0F
ERRMSGA   DC  AL2(ERRLEN)
ERRMSG    DS  CL(L'ERRMSGC)
ERRCODE   DS  CL8
ERRLEN    EQU *-ERRMSG

*
* - External control blocks
          CVT   DSECT=YES
* ENF facility vector table create by system. Pointed to from CVT.
          IEFENFCT
* ENFREQ Macro area mapping
DATAAREA  DSECT
          IEFENFPM
LENODATA  EQU   *-DATAAREA
          END
```

Figure 66. Example of an authorized program that listens for z/OSMF server events (Part 2 of 2)

Figure 67 on page 322 shows IZULST00, which is an example of an ENF listener exit routine for the listener program that is shown in Figure 65 on page 320 and Figure 66 on page 321. To be used by an authorized program, the exit routine must reside in the link pack area (LPA).

```
IZULST00  CSECT
IZULST00  AMODE 31
IZULST00  RMODE ANY

          STM   14,12,12(13)        Save caller's registers
          BALR  12,0                Establish module base

@ESTART   EQU   *
          SAM31                     Ensure 31 bit mode
          USING @ESTART,12          Establish addressability
          MODID                     Eyecatcher and date
          SR    15,15               Set return code to 0
          LR    2,1                 Save Register 1
          WTO   'z/OSMF listen exit (IZULST00) receives control.'
          L     3,0(2)              Address of IZUENF83 data area
          USING IZUENF83,3          Establish addressability

* For reentrancy, obtain storage for the local modifiable variables.
          USING WORKAREA,8          WORKAREA mapped at addr in Reg 8
          GETMAIN RU,LV=WORKAREL,LOC=31  Allocated save/work area
          LR    8,1                 Save the addr of obtained storage
* Clear WORKAREA
          MVI   WORKAREA,X'00'      Clear the first byte
          MVC   WORKAREA+1((L'WORKAREA)-1),WORKAREA
          ST    13,SAVEA+4
          LA    13,SAVEA           Provide save area

* Add your process logic here, for example ...
* Check if the event is for UP/DOWN
          L     7,IZUENF83_Status
          L     9,TESTBIT
          NR    7,9
          LTR   7,7
          BNZ   IZUON               When High bit is on
          WTO   'z/OSMF is down.'
          B     NEXTDO
IZUON     DS 0H
          WTO   'z/OSMF is up.'

NEXTDO    DS 0H
* Print host and uri information
          MVC   WTOMSG(PARTURIL),IZUENF83_URI
          MVC   WTOAREA,WTOLIST
          LA    9,WTOMSGL
          STH   9,WTOMSGA
          LA    5,WTOMSGA                   Point to msg in storage
          WTO   TEXT=(5),MF=(E,WTOAREA)     Write the message

* Return control
          L     13,SAVEA+4
          FREEMAIN RU,A=(8),LV=WORKAREL    Free save/workarea
          L     14,12(13)                  RESTORE CALLERS REGS
          LM    0,12,20(13)                PRESERVE REG 15 - RC
          BR    14                         RETURN TO CALLER

WTOLIST   WTO   TEXT=WTOMSG,MF=L     List Form
WTOLEN    EQU   *-WTOLIST            Length to move
TESTBIT   DC    X'80000000'

WORKAREA  DSECT
SAVEA     DS    18F
WTOAREA   DS   CL(WTOLEN)   WTO in dyn area for modifiable msgs

WTOMSGA   DC  AL2(WTOMSGL)
WTOMSG    DS  CL(PARTURIL)
WTOMSGL   EQU *-WTOMSG
PARTURIL  EQU 80
WORKAREL  EQU *-WORKAREA        WORKAREA DSECT length
          IZUENF83 DSECT=YES
          END
```

Figure 67. Example of an ENF listener exit routine for ENF code 83

Example for an unauthorized program

Figure 68 on page 323 shows a sample program in REXX that can be used to query the z/OSMF global storage area, which is mapped by the macro IZUGSP.

```
/* rexx  */

/* Locate the system ECVT area */
CVT@ = C2d(Storage(10,4))
ECVT@   = C2d(Storage(D2x(CVT@ + 140),4))

/* Locate Address of z/OSMF Global Storage */
/* ECVTIZUGSP offset is 976                */
IZUGSP@   = C2d(Storage(D2x(ECVT@ + 976),4))
if IZUGSP@ = 0 then exit

/* Format the address to HEX string for visible */
IZUGSP$HEX  = C2x(Storage(D2x(ECVT@ + 976),4))

/* Print values from area mapped by IZUGSP */
IZUGSP_ID   = Storage(D2x(IZUGSP@),8)
IZUGSP_STATUS$HEX = C2x(Storage(D2x(IZUGSP@+8),4))
IZUGSP_URI = storage(D2x(IZUGSP@+12),274)

Say "Address of z/OSMF Global Storage is :"IZUGSP$HEX
Say "Eyecather field is :"IZUGSP_ID

/* High Bit is on when z/OSMF is active,
otherwise z/OSMF is inactive.            */
Say "Status and URI length field in HEX format is :"IZUGSP_STATUS$HEX

Say "URI field is :"IZUGSP_URI

exit
```

Figure 68. Example of a REXX routine that allows an unauthorized program to listen for z/OSMF server events

Appendix E. Accessibility

Accessible publications for this product are offered through IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SSLTBW/welcome).

If you experience difficulty with the accessibility of any z/OS information, send a detailed email message to mhvrcfs@us.ibm.com.

Accessibility features

Accessibility features help users who have physical disabilities such as restricted mobility or limited vision use software products successfully. The accessibility features in z/OS can help users do the following tasks:

- Run assistive technology such as screen readers and screen magnifier software.
- Operate specific or equivalent features by using the keyboard.
- Customize display attributes such as color, contrast, and font size.

Consult assistive technologies

Assistive technology products such as screen readers function with the user interfaces found in z/OS. Consult the product information for the specific assistive technology product that is used to access z/OS interfaces.

Keyboard navigation of the user interface

You can access z/OS user interfaces with TSO/E or ISPF. The following information describes how to use TSO/E and ISPF, including the use of keyboard shortcuts and function keys (PF keys). Each guide includes the default settings for the PF keys.

- *z/OS TSO/E Primer*
- *z/OS TSO/E User's Guide*
- *z/OS ISPF User's Guide Vol I*

Dotted decimal syntax diagrams

Syntax diagrams are provided in dotted decimal format for users who access IBM Knowledge Center with a screen reader. In dotted decimal format, each syntax element is written on a separate line. If two or more syntax elements are always present together (or always absent together), they can appear on the same line because they are considered a single compound syntax element.

Each line starts with a dotted decimal number; for example, 3 or `3.1` or `3.1.1`. To hear these numbers correctly, make sure that the screen reader is set to read out punctuation. All the syntax elements that have the same dotted decimal number (for example, all the syntax elements that have the number `3.1`) are mutually exclusive alternatives. If you hear the lines `3.1 USERID` and `3.1 SYSTEMID`, your syntax can include either `USERID` or `SYSTEMID`, but not both.

The dotted decimal numbering level denotes the level of nesting. For example, if a syntax element with dotted decimal number 3 is followed by a series of syntax elements with dotted decimal number 3.1, all the syntax elements numbered 3.1 are subordinate to the syntax element numbered 3.

Certain words and symbols are used next to the dotted decimal numbers to add information about the syntax elements. Occasionally, these words and symbols might occur at the beginning of the element itself. For ease of identification, if the word or symbol is a part of the syntax element, it is preceded by the backslash (\) character. The * symbol is placed next to a dotted decimal number to indicate that the syntax element repeats. For example, syntax element `*FILE` with dotted decimal number 3 is given the format `3 \* FILE`. Format `3* FILE` indicates that syntax element `FILE` repeats. Format `3* \* FILE` indicates that syntax element `* FILE` repeats.

Characters such as commas, which are used to separate a string of syntax elements, are shown in the syntax just before the items they separate. These characters can appear on the same line as each item, or on a separate line with the same dotted decimal number as the relevant items. The line can also show another symbol to provide information about the syntax elements. For example, the lines `5.1*, 5.1 LASTRUN, and 5.1 DELETE` mean that if you use more than one of the `LASTRUN` and `DELETE` syntax elements, the elements must be separated by a comma. If no separator is given, assume that you use a blank to separate each syntax element.

If a syntax element is preceded by the `%` symbol, it indicates a reference that is defined elsewhere. The string that follows the `%` symbol is the name of a syntax fragment rather than a literal. For example, the line `2.1 %OP1` means that you must refer to separate syntax fragment OP1.

The following symbols are used next to the dotted decimal numbers.

? indicates an optional syntax element

The question mark (?) symbol indicates an optional syntax element. A dotted decimal number followed by the question mark symbol (?) indicates that all the syntax elements with a corresponding dotted decimal number, and any subordinate syntax elements, are optional. If there is only one syntax element with a dotted decimal number, the ? symbol is displayed on the same line as the syntax element, (for example `5? NOTIFY`). If there is more than one syntax element with a dotted decimal number, the ? symbol is displayed on a line by itself, followed by the syntax elements that are optional. For example, if you hear the lines `5 ?, 5 NOTIFY`, and `5 UPDATE`, you know that the syntax elements `NOTIFY` and `UPDATE` are optional. That is, you can choose one or none of them. The ? symbol is equivalent to a bypass line in a railroad diagram.

! indicates a default syntax element

The exclamation mark (`!`) symbol indicates a default syntax element. A dotted decimal number followed by the `!` symbol and a syntax element indicate that the syntax element is the default option for all syntax elements that share the same dotted decimal number. Only one of the syntax elements that share the dotted decimal number can specify the ! symbol. For example, if you hear the lines `2? FILE, 2.1! (KEEP), and 2.1 (DELETE)`, you know that `(KEEP)` is the default option for the `FILE` keyword. In the example, if you include the `FILE` keyword, but do not specify an option, the default option KEEP is applied. A default option also applies to the next higher dotted decimal number. In this example, if the `FILE` keyword is omitted, the default `FILE(KEEP)` is used. However, if you hear the lines `2? FILE, 2.1, 2.1.1! (KEEP)`, and `2.1.1 (DELETE)`, the default option KEEP applies only to the next higher dotted decimal number, `2.1` (which does not have an associated keyword), and does not apply to `2? FILE`. Nothing is used if the keyword `FILE` is omitted.

*** indicates an optional syntax element that is repeatable**

The asterisk or glyph (*) symbol indicates a syntax element that can be repeated zero or more times. A dotted decimal number followed by the * symbol indicates that this syntax element can be used zero or more times; that is, it is optional and can be repeated. For example, if you hear the line `5.1* data area`, you know that you can include one data area, more than one data area, or no data area. If you hear the lines `3* , 3 HOST, 3 STATE`, you know that you can include `HOST, STATE`, both together, or nothing.

Notes:

1. If a dotted decimal number has an asterisk (*) next to it and there is only one item with that dotted decimal number, you can repeat that same item more than once.
2. If a dotted decimal number has an asterisk next to it and several items have that dotted decimal number, you can use more than one item from the list, but you cannot use the items more than once each. In the previous example, you can write `HOST STATE`, but you cannot write `HOST HOST`.

3. The * symbol is equivalent to a loopback line in a railroad syntax diagram.

+ indicates a syntax element that must be included

The plus (+) symbol indicates a syntax element that must be included at least once. A dotted decimal number followed by the + symbol indicates that the syntax element must be included one or more times. That is, it must be included at least once and can be repeated. For example, if you hear the line `6.1+ data area`, you must include at least one data area. If you hear the lines `2+, 2 HOST, and 2 STATE`, you know that you must include `HOST, STATE,` or both. Similar to the * symbol, the + symbol can repeat a particular item if it is the only item with that dotted decimal number. The + symbol, like the * symbol, is equivalent to a loopback line in a railroad syntax diagram.

Notices

This information was developed for products and services that are offered in the USA or elsewhere.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

This information could include missing, incorrect, or broken hyperlinks. Hyperlinks are maintained in only the HTML plug-in output for the Knowledge Centers. Use of hyperlinks in other output formats of this information is at your own risk.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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
Site Counsel
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 document 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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

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 illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s name, email address, phone number, or other personally identifiable information for purposes of enhanced user usability and single sign-on configuration. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at ibm.com/privacy and IBM’s Online Privacy Statement at ibm.com/privacy/details in the section entitled “Cookies, Web Beacons and Other Technologies,” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at ibm.com/software/info/product-privacy.

Policy for unsupported hardware

Various z/OS elements, such as DFSMS, JES2, JES3, and MVS, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Minimum supported hardware

The minimum supported hardware for z/OS releases identified in z/OS announcements can subsequently change when service for particular servers or devices is withdrawn. Likewise, the levels of other software products supported on a particular release of z/OS are subject to the service support lifecycle of those products. Therefore, z/OS and its product publications (for example, panels, samples, messages, and product documentation) can include references to hardware and software that is no longer supported.

- For information about software support lifecycle, see: IBM Lifecycle Support for z/OS (www.ibm.com/software/support/systemsz/lifecycle)
- For information about currently-supported IBM hardware, contact your IBM representative.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available at Copyright and Trademark information (www.ibm.com/legal/copytrade.shtml).

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Intel is a trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle, its affiliates, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names might be trademarks or service marks of others.

Index

SC27-8419-30