Auditing Essentials

VOLUME 3

SECURING z/OSMF

Julie Bergh – J & S Consulting, LLC.

Richard Faulhaber – NewEra Software

02/20/2020

Foreword

The security set-up of z/OSMF is an integral part of its overall installation and configuration. To secure it properly can only be accomplished by Systems Programmers working in close conjunction with Security Administrators on a z/OS system that is already secured by Systems Administrations Best Practices. These Best Practices are detailed in our previously published series Auditing Essentials Volume 2: Taming RACF – SETROPTS, Mastering CA ACF2 GSO, and Controlling CA Top Secret. With the release of z/OS V2R4, z/OSMF is now a mandatory part of its configuration. Going forward, through the use of the Network Configuration Assistant, it will be the only way to adequately secure the z/OS platform from outside threats.

This book is a distillation of the essential security portions of the z/OSMF configuration and programming documentation available from IBM, which cannot, and should not, be ignored. The process of co-authoring this book, by myself and Julie Bergh, took many months of research, gathering and sifting through data, and debating what to include and what to exclude. We tried to strike a balance, showing the essential areas that required attention, while also providing tips on security configuration from real-world experience.

As z/OSMF has continued to evolve since its introduction, through its many iterations, the proper installation, security setup and configuration has been a moving target. A majority of those who answered our surveys about installing, configuring, and maintaining z/OSMF say the most challenging part has been configuring the security settings. Differences between z/OS environments will call for different z/OSMF's security configurations.

If your shop has yet to implement z/OSMF, or if you've already tried to tackle it but have been stymied by its many security settings, you will find the topics in this book to be useful talking points to bridge the gap between your System Programmers and Security Administrators who have been tasked with getting the job done.

Richard Faulhaber
NewEra Software, Inc.

Table of Contents

1 A Step Towards Modernization — Why Use z/OSMF?

What it is and What it isn't

On the surface, IBM's z/OS Management Facility (z/OSMF) is a takes a big step towards modernizing the management of the z/OS environment. Its main purpose is to simplify z/OS system management. To accomplish this, it provides a modern, task-oriented user interface that runs in a standard web browser. The intent of z/OSMF is to improve productivity, automate some z/OS system management activities, and make system programmers' work less prone to errors.

Because the z/OSMF user interface runs in a standard web browser, it allows users to access its functions from virtually anywhere. The novice systems programmer will find in it familiar and intuitive web-based conventions making more approachable than the traditional 3270 terminal screen. It enables those with smaller z/OS skillsets to perform useful work with less training. More experienced systems programmers will benefit from z/OSMF by the reduced complexity of accessing important information, performing specific manual functions, and the automating others.

A defining feature of z/OSMF is the collecting of manual system management tasks under a single, common interface, that have previously only been accessible separately.

z/OSMF is not intended to be a training tool nor is it a learning environment for new systems programmers. It is not meant to replace the many years of experience of a seasoned systems programmer. Though it may provide tools to accomplish many complex tasks, it is not a replacement for specific knowledge gained from running z/OS in any particular organization's environment.

Beyond the functions provided within, it is possible to customize z/OSMF, interfacing it with any number of REST APIs, creating unique workflow definitions, and coding plug-ins to perform functions tailored to the specific needs of your organization.

This document discusses the security settings of z/OSMF from a z/OS 2.3 perspective. IBM has introduced further changes and enhancements to z/OSMF with the release of z/OS 2.4, which will be covered in future updates to this document.

2 How This Document is Organized

The setup and configuration of z/OSMF has evolved over time. IBM has made a lot of effort to simplify the process. Comments from those who have tried to tackle the installation and configuration of z/OSMF since its first release have noted many challenges. In two surveys of z/OSMF usage we conducted between August 2018 and February 2019 (the results of which are in APPENDIX A of this document), we found few respondents who had no trouble at all with its installation, configuration, and setup. Of the comments from numerous SHARE presentations, and the results of our surveys, getting the plug-ins configured and operating properly has proved to be the biggest hurdle. The major headache for many has been with the security settings – which is the sole topic of this book.

This document is by no means a replacement for IBM's own documentation. Nor is it meant as a stand-alone guide to configuring z/OSMF security, as a whole, since the security setup is an integral part of getting z/OSMF up and running. Rather, it is meant to be an overview of the z/OSMF security setup process and a general discussion of all those parts necessary to secure z/OSMF. We hope this document can help to open up communication between the persons and groups whose skills will be needed in order to get z/OSMF up and running securely in your organization.

First, we will describe the security settings underlying a base configuration of z/OSMF. Next, we will describe the core functions, and any categories or tasks, not including the plug-ins, which may require additional attention for configuring security. Last, we will describe the plug-ins and provide the necessary keys to successfully configuring them.

Our main references for this guide are the following IBM documents:

z/OS - V2R3 - IBM z/OS Management Facility Configuration Guide (SC27-8419-30 Last updated: 6-27-2019)

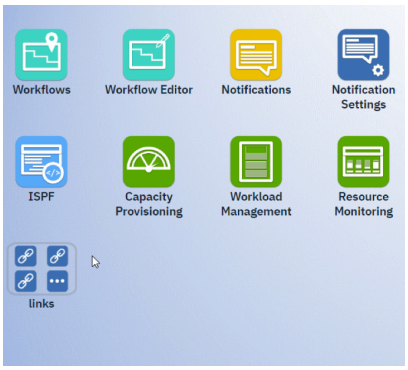
IBM z/OS Management Facility V2R3 by Redelf Janssen & Tobias Rotthove (Third Edition - April 2018)

3 Highlights of z/OSMF Components

To better understand how z/OSMF is setup and organized, it is important to describe some of the terms used within z/OSMF and its documentation. When one initially logs into z/OSMF a navigation area appears at the left side of the screen. This is the standard view of the navigation area. z/OSMF offers an option to use a desktop view, allowing the user to arrange selections and tasks as icons on a desktop. For the purpose of consistency in this document, we will refer to the standard view for navigation.

Standard View

Desktop View



Tasks are functions that can be used to manage different aspects of the z/OS system. Some tasks are core functions, others must be configured separately from a base configuration of z/OSMF.

Core functions are those tasks which are always enabled when you initially configure the product. They are installed and can run without the need for the additional plug-ins. When the started tasks are brought up, a base configuration of z/OSMF contains only these functions. Some core functions are the Workflows task, the Resource Management task, and the Usage Statistics task.

Plug-ins are collections of one or more system management tasks that add significant functionality to z/OSMF and require additional steps to configure and deploy. Plug-ins require the creation of security profiles for the tasks that

are associated with them. Examples of plug-ins are the Network Configuration Assistant, Cloud Provisioning, and the Incident Log.

Categories are collections of tasks and/or plug-ins with shared characteristics. An example of a category is the Performance category which contains the Capacity Provisioning, Resource Monitoring, and Workload Management plug-ins along with the System Status task.

The table on the next page helps to understand these different terms by listing the tasks, categories, and plug-ins as they appear in the navigation area of the standard view of z/OSMF.

Core Functions	Categories	Plug-ins	Menu / Sub-Menu Items (tasks, as the manual says it this way sometimes.)
•			Welcome
•			Notifications
•			Workflow Editor
•			Workflows
	•	•	Cloud Provisioning
			Marketplace
			Marketplace Administration
			Resource Management
			Software Services
	•		Configuration
		•	Network Configuration Assistant
	•		Consoles
			z/OS Operator Consoles
	•		Jobs & Resources
			SDSF
•	•		Links
			Shopz
			Support for z/OS
			WSC Flashes & Techdocs
			Z Systems
			z/OS Basic Information Center
			z/OS Home Page
			z/OS Internet Library
	•		Performance
		•	Capacity Provisioning
		•	Resource Monitoring
			System Status
		•	Workload Management
	•		Problem Determination
		•	Incident Log
	•		Software
		•	Software Management

Core Functions	Categories	Plug-ins	Menu / Sub-Menu Items (tasks, as the manual says it this way sometimes.)
	•		Sysplex
		•	Sysplex Management
	•		z/OS Classic Interfaces
		•	ISPF
	•		z/OSMF Administration
•			Application Linking Manager
•			Import Manager
•			Links
•			Usage Statistics
			z/OSMF Settings
•			FTP Settings
•			General Settings
•			Notification Settings
			SDSF Settings
•			System
•			z/OSMF Diagnostic Assistance
			z/OSMF Diagnostic Assistance

4 Security Setup for z/OSMF — The IZUxxSEC Jobs

Configuring the security definitions for z/OSMF is no simple task and no single setup will suit all environments. IBM provides sample jobs in the SYS1.SAMPLIB library specifically for z/OSMF setup. These sample jobs are designated by names with this format: IZUxxSEC. The sample jobs we will discuss in this document comprise almost 2000 lines of code. The IZUSEC job, used to set up the core functions alone contains 97 PERMIT and 53 RDEFINE commands.

This table gives a mere sampling of the amount of code requiring consideration and review in order to configure z/OSMF and its plug-ins.

Job Name	Function	Approximate number of RACF commands
IZUSEC	CORE FUNCTIONS	170
IZUPRSEC	CLOUD PROVISIONING	30
IZUCPSEC	CAPACITY PROVISIONING	10
IZUILSEC	INCIEDENT LOG	50
IZUISSEC	ISPF PLUGIN	4
IZUCASEC	NETWORK CONFIG ASSIST	4
IZUDMSEC	SOFTWARE DEPLOYMENT	13
IZUSPSEC	SYSPLEX MANAGEMENT	20
IZUWMSEC	WORKLOAD MANAGEMENT	13
IZUGCSEC	OPERATOR CONSOLES TASK	22

5 Security Setup for the Core Functions of z/OSMF

The z/OSMF Core functions are available with a basic installation of z/OSMF. This is what is available with a bare-bones installation. These are installed and run without the need for the additional plug-ins.

For the core functions, sample RACF commands are contained within the sample job **IZUSEC**, found in SYS1.SAMPLIB (listed in its entirety in **APPENDIX F** of this document).

RACF class ZMFAPLA is the class used to secure the basic core function accesses as well as the plug-ins.

The following table describes the core functions and the basic RACF profiles required for them.

MENU ITEM	**MENU - SUB-ITEM (TASK**	**RACF Profiles – ZMFAPLA Class**
Welcome		
NOTIFICATION	The Notification section is a core function that allows you to view and act on the z/OSMF notifications that have been assigned to you.	
Notifications		*Saf-prefix*.ZOSMF.NOTIFICATION *Saf-prefix*.ZOSMF.NOTIFICATION.MODIFY *Saf-prefix*.ZOSMF.NOTIFICATION.SETTINGS *Saf-prefix*.ZOSMF.NOTIFICATION.SETTINGS.ADMIN
WORKFLOW EDITOR	The Workflow Editor is a core function that allows you to view, create, modify workflow definitions.	
Workflow Editor		*Saf-prefix*.ZOSMF.WORKFLOW *Saf-prefix*.ZOSMF.WORKFLOW.ADMIN *Saf-prefix*.ZOSMF.WORKFLOW.EDITOR
WORKFLOWS	The Workflow section is a core function that performs a guided set of steps to accomplish various tasks, for example, to configure components or products in your installation.	
Workflows		*Saf-prefix*.ZOSMF.WORKFLOW.WORKFLOW
LINKS	The Links area is a core function that contains helpful links to other tools and information on the web. Links to areas like • Shopz • IBM Support • IBM Techdocs • IBM redbooks • IBM Z/OS Basic mainframe skills • z/OS home page • z/OS manuals	
Links		*Saf-prefix*.ZOSMF.ADMINTASKS.LINK.linkname
	Shopz	*Saf-prefix*.ZOSMF.LINK.SHOPZSERIES
	Support for z/OS	*Saf-prefix*.ZOSMF.LINK.SUPPORT_FOR_Z_OS
	WSC Flashes & Techdocs	*Saf-prefix*.ZOSMF.LINK.WAS_FLASHES_TECHDOCS

MENU ITEM	MENU - SUB-ITEM (TASK	RACF Profiles – ZMFAPLA Class
	z Systems	*Saf-prefix*.ZOSMF.LINK.SYSTEM_Z_REDBOOKS
	z/OS Basics Information Center	*Saf-prefix*.ZOSMF.LINK.Z_OS_BASICS_ INFORMATION_CENTER
	z/OS Home Page	*Saf-prefix*.ZOSMF.LINK.Z_OS_HOME_PAGE
	z/OS Internet Library	*Saf-prefix*.ZOSMF.LINK.Z_OS_INTERNET_LIBRARY
z/OSMF ADMINISTRATION	A z/OSMF installation has one or more users that are authorized to access z/OSMF as administrators. This administrator can perform administration tasks as needed. The z/OSMF Administration section is a category containing these core functions accessible to administrators: • Application Linking Manager - The Application Linking Manager is a core function that provides access to z/OSMF administrators to manage the event types that allow for linking or connecting z/OSMF tasks and external applications. • Import Manager - The Import Manager is a core function that allows the z/OSMF Administrator to import plug-ins, event types, event handlers, and links into z/OSMF. • Links - The Links section is a core function that allows z/OSMF administrators to add links to external resources that might be useful for managing your z/OS systems. • Usage Statistics - The Usage Statistics task is a core function that allows a z/OSMF administrator to see which users are logged in to z/OSMF, perhaps as a precautionary check before making a critical update to z/OSMF.	
z/OSMF Administration		*Saf-prefix*.ZOSMF.ADMINTASKS *Saf-prefix*.ZOSMF.ADMINTASKS.LOGGER *Saf-prefix*.ZOSMF.ADMINTASKS.UI_LOG_ MANAGMENT
	Application Linking Manager	*Saf-prefix*.ZOSMF.ADMINTASKS.APPLINKING
	Import Manager	*Saf-prefix*.ZOSMF.ADMINTASKS.IMPORTMANAGER
	Links	*Saf-prefix*.ZOSMF.ADMINTASKS.LINKSTASK
	Usage Statistics	*Saf-prefix*.ZOSMF.ADMINTASKS.USAGESTATISTICS
z/OSMF SETTINGS	The z/OSMF Settings section is a category containing several critical core functions. Depending on the core functions installed this area can be used for the settings that are specific for z/OSMF tasks including: • FTP Servers Settings - The FTP Servers section is a core function that provides the information required for an FTP client to log into an FTP server and download and upload files. • General Settings - Manages the diagnostics and customization tasks • Notification Settings - The Notification Settings section is a core function that defines configuration values used for notifications from z/OSMF tasks and z/OS products. • SDSF Settings – lets you define configuration values for the SDSF task. • Systems Settings - The System Settings section is a core function that provides the information required to access the z/OS systems in your installation.	

MENU ITEM	MENU - SUB-ITEM (TASK	RACF Profiles – ZMFAPLA Class
z/OSMF Settings		*Saf-prefix*.ZOSMF *Saf-prefix*.ZOSMF.SETTINGS
	FTP Servers	*Saf-prefix*.ZOSMF.SETTINGS.FTP_SERVERS *Saf-prefix*.ZOSMF.SETTINGS.FTP_SERVERS.MODIFY *Saf-prefix*.ZOSMF.SETTINGS.FTP_SERVERS.VIEW
	General Settings	*Saf-prefix*.ZOSMF.SETTINGS.SYSTEMS *Saf-prefix*.ZOSMF.SETTINGS.SYSTEMS.MODIFY *Saf-prefix*.ZOSMF.SETTINGS.SYSTEMS.VIEW
	Notification Settings	*Saf-prefix*.ZOSMF.NOTIFICATION.MODIFY *Saf-prefix*.ZOSMF.NOTIFICATION.SETTINGS *Saf-prefix*.ZOSMF.NOTIFICATION.SETTINGS.ADMIN
	SDSF Settings	*Saf-prefix*.ZOSMF.IBMSDSF.JOBS *Saf-prefix*.ZOSMF.IBMSDSF.SETTINGS
	Systems	*Saf-prefix*.ZOSMF.SETTINGS.SYSTEMS *Saf-prefix*.ZOSMF.SETTINGS.SYSTEMS.MODIFY *Saf-prefix*.ZOSMF.SETTINGS.SYSTEMS.VIEW
Z/OSMF Diagnostic Assistance	The z/OSMF diagnostic Assistant is used to collect diagnostic data about z/OSMF and download it as a compressed file package.	
	Z/OSMF Diagnostic Assistance	*Saf-prefix*.ZOSMF.ADMINTASKS.DIAGNOSTIC_ ASSISTANT

Configuring z/OSMF is a three-stage process.

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

The IZUSEC job contains RACF commands for creating security definitions.

As this document is concerned with the security settings, that will be the sole focus of this section. This is not intended to replace or reproduce the information in the installation manuals, rather it is intended to complement the information that is provided based on user experiences.

Before we start with the commands, one needs to understand the dependency on the sample JCL and what is defined in the start-up parameter library member for z/OSMF. That member is IZUPRMxx. Below is an abbreviated version of it to demonstrate the interdependencies between the JCL and these parameters.

******NOTE – the IZUACCT is what is defined in the various sample JCL. If it is changed in either place, one needs to ensure it is consistent.**

```
RESTAPI_FILE ACCT(IZUACCT) REGION(32768) PROC(IZUFPROC)
COMMON_TSO ACCT(IZUACCT) REGION(50000) PROC(IZUFPROC)
```

******NOTE – As you will see going forward in this document, we reference the prefix as *Saf-prefix* where in the IZUPRMxx member by default that prefix is set to IZUDFLT. If you decide to change this prefix, the JCL needs to be review and changed as appropriate.**

```
SAF_PREFIX('IZUDFLT')
```

******NOTE – Similar to the *Saf-prefix*, below is the default. If you decide to change this**

prefix, the JCL needs to be review and changed as appropriate.

```
CLOUD_SAF_PREFIX('IYU')
```

******NOTE – z/OSMF is going to define groups for owning the started task as well as for users of z/OSMF and for z/OSMF security administrators. The z/OSMF security administrator may be the same as the RACF administrator or it could be someone else. If you decide to change these groups and ownership, one may need to do further security definitions**

```
SEC_GROUPS USER(IZUUSER),ADMIN(IZUADMIN),SECADMIN(IZUSECAD)
```

******NOTE – By default the z/OSMF Server and Angle process will run under the same userid. You may want to change this, and you will have to check permissions to the started tasks based on this**

```
SERVER_PROC('IZUSVR1')
ANGEL_PROC('IZUANG1')
```

******NOTE – If you are going to use the AUTOSTART feature, the group is defined below and if you change that, like any of the above, other permissions may need to be granted. The same is true for the unauthorized user userid.**

```
AUTOSTART_GROUP('IZUDFLT')
UNAUTH_USER(IZUGUEST)
```

Security setup stage

Running the IZUSEC job establishes security for z/OSMF through traditional SAF-based authorizations.

Your Security Administrator will need to review this and tailor it to fit your site-specific requirements. Some definitions will need to be commented out based on your existing security environment.

If your environment has an External Security Manager other than RACF, you cannot use the IZUSEC job, as it is. You will need to create equivalent commands for your security product. (See Appendix A in the z/OSMF Configuration Guide for a list of resources, groups, IDs, and authorizations that need to be defined to your security product.)

The following is some observations based on experiences and we are going to break down the various parts of the IZUSEC job. Observations are documented with the ******NOTE** before the comment.

Some recommendations:

- RACF commands provided **do not** always include fields like OWNER, SUPERIORGROUP
  - This is applicable for ADDGROUP, ADDUSER, RDEFINE, CONNECT
  - Did not provide all the instances. One should review the commands before executing
- The IZUSEC job asks you to enable RACF classes before profiles are defined. We recommend that profiles be defined before classes are activated.
- We recommend that one looks to ensure that generics and generic commands are activated for this classes in your environment. For example the ZMFAPLA class.
- This section also includes some setup for other plug-ins, like ISPF.
- In addition, depending on the classes, if some of these classes are not

already active in your environment, caution should be taken when activating these classes as they do not cause something else to not work. They will be described as we go through the JCL. For example, use of the TSOAUTH for access to consoles.

- If the SERVER class is not active in your system, it will check for BPX.WLMSERVER in the FACILITY class, and you may have security issues with the PROGRAM class. The sample JCL provides a definition for BPX.WLMSERVER without any permissions.
- Access permissions for the started task are given at the user level and not at a group level. You may want to change this to suit your site's standards.
- Profiles in the ZMFAPLA class assume a default prefix of IZUDFLT. See the previous tables where it describes the ***Saf-prefix*** for the RACF profile definitions. This also has implications for what is set up in the IZUPRMxx member.
- This job, as it is, assumes items like UNIXPRIV, JESSPOOL, LOGSTRM are already active on your system.
- The member has RACF commands for all these different RACF classes ACCTNUM, APPL, DATASET, EJBROLE, FACILITY, SERVAUTH, SERVER, TSOAUTH, TSOPROC, ZMFAPLA.
- The RACF PERMIT commands that are provided do them to for the groups that are created. One needed to CONNECT users to those groups so they have access. Those commands are not part of the setup.
- Check these RDEFINEs for new profiles in your environment as they may be undercutting other profiles. There also may need to be other permission if they are undercut to other user ids.
- A thorough review should be done of IZUSEC to ensure one understands what is being set up and why.

What follows is a breakdown of what each part of the IZUSEC JCL does.

APPENDIX F contains a copy of the JCL in its entirety without the comments.

The JCL header contains the following information:

DESCRIPTIVE NAME: z/OSMF SERVER default security setup

The JCL contains the security setup for z/OSMF server. You can customize this JCL to create a security setup for the z/OSMF Server as you wish.

NOTE: Step V2R3 is added to job IZUSEC in this release. This step contains the profiles which are new in z/OS V2R3. If you have previously installed and configured z/OSMF, step V2R3 is the only step you need to run.

This job must be run using a user ID that has the RACF SPECIAL attribute.

******NOTE – Review this as your environment may not have BPX.NEXT.USER setup. If not, the JCL will need to be changed to suit your company standards.**

This job assumes that the BPX.NEXT.USER profile has been defined in the FACILITY class to enable the use of AUTOUID and AUTOGID. See the topic "Automatically assigning unique IDs through UNIX services" in z/OS Security Server RACF Security Administrator's Guide for additional information about automatic UID and GID assignment. If this function has not been enabled, you must assign unique UIDs to the IZUSVR and IZUGUEST user IDs, and unique GIDs to the groups: IZUADMIN, IZUSECAD, IZUUSER, and IZUUNGRP.

CORE SECURITY SETTINGS

****** NOTE – This next section activates the following classes.**

APPL	**EJBROLE**	**FACILITY**	**SERVER**
SERVAUTH	**STARTED**	**ZMFAPLA**	**ACCTNUM**
TSOPROC	**TSOAUTH**	**OPERCMDS**	

****** NOTE – These classes are probably active in your environment**

FACILITY	**STARTED**	**TSOPROC**	**ACCTNUM**
TSOAUTH	**OPERCMDS**		

****** Note – the following classes may NOT be active in your environment and one should check before they are activated as activating these may cause other security errors.**

APPL	**EJBROLE**	**SERVER**	**SERVAUTH**
ZMFAPLA			

******NOTE – ZMFAPLA should also have GENERICS and GENERIC COMMANDS activate**
SETR GENERIC(ZMFAPLA) GENCMD(ZMFAPLA)

As noted above, a number of these classes are likely already active.

```
/* Begin "Core" Setup                                              */
/*                                                                 */
/* This commented section contains the CLASS activation commands.*/
/* Ensure the following classes are active before executing this */
/* script or creating profiles in these classes.                  */
/*  */
/* Activate and RACLIST the APPL class                            */
/*SETROPTS CLASSACT(APPL)                                         */
/*SETROPTS RACLIST(APPL) GENERIC(APPL)                            */
/*                                                                */
/* Activate and RACLIST the EJBROLE class                         */
/*SETROPTS CLASSACT(EJBROLE)                                      */
/*SETROPTS RACLIST(EJBROLE) GENERIC(EJBROLE)                      */
/*                                                                */
/* Activate and RACLIST the FACILITY class                        */
/*SETROPTS CLASSACT(FACILITY)                                     */
/*SETROPTS RACLIST(FACILITY)                                      */
/*                                                                */
/* Activate and RACLIST the SERVER class                          */
/*SETROPTS CLASSACT(SERVER)                                       */
/*SETROPTS RACLIST(SERVER)                                        */
/*                                                                */
/* Activate and RACLIST the SERVAUTH class                        */
/*SETROPTS CLASSACT(SERVAUTH)                                     */
/*SETROPTS RACLIST(SERVAUTH) GENERIC(SERVAUTH)                    */
/*                                                                */
/* Activate and RACLIST the STARTED class                         */
/*SETROPTS CLASSACT(STARTED)                                      */
/*SETROPTS RACLIST(STARTED) GENERIC(STARTED)                      */
/*                                                                */
/* Activate and RACLIST the ZMFAPLA class                         */
/*SETROPTS CLASSACT(ZMFAPLA)                                      */
/*SETROPTS RACLIST(ZMFAPLA) GENERIC(ZMFAPLA)                      */
/*                                                                */
/* Activate the ACCTNUM class                                     */
/*SETROPTS CLASSACT(ACCTNUM)                                      */
/* Activate the TSOPROC class                                     */
/*SETROPTS CLASSACT(TSOPROC)                                      */
/* Refresh the ACCTNUM class                                      */
/* SETROPTS RACLIST(ACCTNUM) REFRESH                              */
```

```
/* Refresh the TSOPROC class                                    */
/* SETROPTS RACLIST(TSOPROC) REFRESH                            */
/*                                                              */
/* Activate the TSOAUTH class                                   */
SETROPTS CLASSACT(TSOAUTH)
/* Refresh the TSOAUTH class                                    */
SETROPTS RACLIST(TSOAUTH)
/*                                                              */
/* Activate the OPERCMDS class                                  */
SETROPTS CLASSACT(OPERCMDS)
/* Refresh the OPERCMDS class                                   */
SETROPTS RACLIST(OPERCMDS)
```

Adds groups IZUADMIN, IZUUSER, IZUUNGRP -

- This corresponds to what is defined in IZUPRMxx in SYS1.PARMLIB. They must match otherwise z/OSMF will not start correctly.
- Assumes AUTOGID (****Note: Check to see if your site is using AUTOGID)
- The group IZUADMIN is used to own the started task userid, as well as the profiles. In addition, the started task is set up to run under the same userid IZUSVR. Autouid is used for UNIX Systems Services.

****** NOTE – IZUADMIN is the group that will own the STARTED class profiles, and various accesses throughout the IZUSEC job. IZUUSER is the group for various permissions in the various classes. IZUUNGRP is for the group for unauthenticated users. Also notice in the IZUSEC job that there are NO connections of users to the groups IZUADMIN and IZUUSER. It is up to the customer to determine the appropriate people to CONNECT to these groups.**

```
/* Create the z/OSMF Administrators group                       */
ADDGROUP IZUADMIN OMVS(AUTOGID)
/* Create the z/OSMF Users group                                */
ADDGROUP IZUUSER OMVS(AUTOGID)
/* Create the z/OSMF Unauthenticated group                      */
ADDGROUP IZUUNGRP OMVS(AUTOGID)
```

When creating these groups, we recommend that you specify an OWNER, with a group name, and a SUPerior group, with a group name. For example:

```
ADDGROUP IZUADMIN OMVS(AUTOGID) OWNER(some_group) SUP(some_group)
```

Where some_group is some group defined in your organization. If you decide to change the group name, there will need to be other changes throughout the JCL.

Adds user IZUSVR – this will be userid for the 2 started tasks -

- DEFAULTGROUP(IZUADMIN)
- Assumes AUTOUID

****** NOTE – in the following ADDUSER command there is no OWNER defined for the ADDUSER – it is recommended that this be added. It is used for the 2 started tasks. You may want to create different users for each started task. -**

```
/* Create the started task USERID for the z/OSMF Server        */
/* Note: The HOME directory will be created by the IZUMKFS      */
/* sample job.                                                  */
ADDUSER IZUSVR DFLTGRP(IZUADMIN) OMVS(AUTOUID   +
    HOME(/global/zosmf/data/home/izusvr) +
    PROGRAM(/bin/sh)) NAME('zOSMF Started Task USERID')  +
    NOPASSWORD
 /* Change concurrent open file number for started task
    USERID                                                      */
```

```
ALTUSER IZUSVR OMVS(FILEPROC(10000))
```

Adds user IZUGUEST – this is unauthenticated user -

- Makes user RESTRICTED. If you are not aware of the use of the RESTRICTED attribute in RACF, one should look at the RACF security administration guide. One may also want to look at the UNIXPRIV class for the appropriate attribute to secure.
- This corresponds to what is defined in IZUPRMxx in SYS1.PARMLIB
- DEFAULTGROUP(IZUUNGRP)

```
/* Create the z/OSMF unauthenticated USERID                    */
ADDUSER IZUGUEST RESTRICTED DFLTGRP(IZUUNGRP) OMVS(AUTOUID)  +
  NAME('zOSMF Unauthenticated USERID') NOPASSWORD
```

Defines the 2 started task of IZUSVR1 and IZUANG1 using the userid IZUSVR -

****** NOTE – The 2 started tasks are running with the same userid defined above. Also note that the RDEFINE commands do not specify an OWNER. It is recommended that this be added to the command before it is executed. One should also check to see if TRACE is needed in your environment.**

```
/* 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))
```

Define IZUDFLT in the APPL class –

****** Note – check to see if the APPL class is active in your environment.**

```
/* Define the APPL profile for the z/OSMF server               */
RDEFINE APPL IZUDFLT UACC(NONE)
```

Define z/OSMF server in the SERVER class -

****** Note – check to see if the SERVER class is active in your environment.**

```
/* Define the SERVER profiles for the z/OSMF server            */
RDEFINE SERVER BBG.SECPFX.IZUDFLT UACC(NONE)
RDEFINE SERVER BBG.ANGEL UACC(NONE)
RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM UACC(NONE)
RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM.SAFCRED UACC(NONE)
RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM.ZOSWLM UACC(NONE)
RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM.TXRRS UACC(NONE)
RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM.ZOSDUMP UACC(NONE)
```

Permit IZUGUEST to IZUDFLT in APPL class -

****** Note – Before you log on the IZUGUEST is the ID that needs to have access to the APPL class.**

```
/* Permit the z/OSMF unauthenticated USERID access            */
PERMIT IZUDFLT CLASS(APPL)    ID(IZUGUEST) ACCESS(READ)
```

****** Note – The started task user id IZUSVR is not permitted to the various accesses. Check to ensure this is what is wanted in your environment or whether there is a specific group.**

Permits IZUSVR (started task ID) to the SERVER class permissions -

- You may want to review your standards and define as appropriate.

```
/* Permit the started task USERID access                          */
PERMIT BBG.SECPFX.IZUDFLT CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.ANGEL CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.AUTHMOD.BBGZSAFM CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.AUTHMOD.BBGZSAFM.SAFCRED CLASS(SERVER) ACCESS(READ)
D(IZUSVR)
PERMIT BBG.AUTHMOD.BBGZSAFM.ZOSWLM CLASS(SERVER) ACCESS(READ)
ID(IZUSVR)
PERMIT BBG.AUTHMOD.BBGZSAFM.TXRRS CLASS(SERVER) ACCESS(READ)
ID(IZUSVR)
PERMIT BBG.AUTHMOD.BBGZSAFM.ZOSDUMP CLASS(SERVER) ACCESS(READ)
ID(IZUSVR)
```

Define various BPX, BBG, IRR profiles in the FACILTY class -

- Grant IZUSVR access to these profiles

****** Note – The started task user id IZUSVR is the ID that is permitted to the various accesses. Check to ensure this is what is wanted in your environment or whether there is a specific group.**

****** Note – Also check these RDEFINEs for new profiles in your environment as they may be undercutting other profiles. There also may need to be other permission if they are undercut to other user ids.**

```
/* Define the BPX.CONSOLE profile to suppress the BPXM023I message */
/* prefix for console messages                                     */
RDEFINE FACILITY BPX.CONSOLE UACC(NONE)

/* Permit the started task USERID access                          */
PERMIT  BPX.CONSOLE CLASS(FACILITY) ID(IZUSVR) ACCESS(READ)

/* Define the Sync-to-OS-thread FACILITY profile                  */
RDEFINE FACILITY BBG.SYNC.IZUDFLT UACC(NONE)

/* Permit the started task USERID access                          */
PERMIT  BBG.SYNC.IZUDFLT CLASS(FACILITY) ID(IZUSVR) ACCESS(CONTROL)

/* Define the FACILITY class profiles for working with digital    */
/* certificates                                                   */
RDEFINE FACILITY IRR.DIGTCERT.LIST UACC(NONE)
RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE)

/* 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 started task USERID access                          */
PERMIT IRR.DIGTCERT.LIST CLASS(FACILITY) ID(IZUSVR) ACCESS(READ)
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(IZUSVR)  ACCESS(READ)
```

Create certificates for the z/OSMF server -

- Keyring name needs to correspond to what is defined in IZUPRMxx in SYS1. PARMLIB

****** Note – The following steps assumes that RACF will be the CA for the certificates. If you have an enterprise CA, then a different procedure will need to be followed.**

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

Define the CEA to the SERAUTH class –

****** Note – Check what other profiles may be defined in the SERVAUTH class. Check these RDEFINEs for new profiles in your environment as they may be undercutting other profiles. There also may need to be other permission if they are undercut to other user ids**

****** Note – the RDEFINE below you may want to change to CEA.CEATSO.****

```
/* Assumption: SERVAUTH class is active                            */
/* SETROPTS GENERIC(SERVAUTH)                                      */

/* Define the CEA resource profile required for z/OSMF server      */
RDEFINE SERVAUTH CEA.CEATSO.* UACC(NONE)
```

****** Note – This is creating other account numbers and TSO logon procs. You can use something that has already been defined in your environment.**

Define ACCTNUM, TSOPROC -

- This corresponds to what is defined in IZUPRMxx in SYS1.PARMLIB

```
/* Define the Account Number resource profile for REST File API    */
RDEFINE ACCTNUM IZUACCT UACC(NONE)

/* Define the TSO Procedure resource profile for REST File API     */
RDEFINE TSOPROC IZUFPROC UACC(NONE)
```

****** Note – Most people have LIST OF GROUPs checking on in their environment.**

```
/* List-of-groups authority checking supplements the normal RACF */
/* access authority checking by allowing all groups of which a   */
/* user ID is a member to enter into the access list checking     */
/* process. Uncomment the following line to activate this.        */
/* SETROPTS GRPLIST                                               */
```

Define group IZUSECAD for Security Administrators -

****** Note – IZUSECAD is the group that is created to do security administration within z/OSMF. Once again, you will need to add the OWNER and SUPERIORGROUP to the definitions.**

****** Note – The definition of the group IZUSECAD does not include CONNECTing anyone to these groups. You will need to review your environment to determine who should be connected to this group.**

```
/* Create the z/OS Security Administrators group                  */
    ADDGROUP IZUSECAD OMVS(AUTOGID)
```

Define the ZMFAPLA profile <saf.profile>.ZOSMF -

- This corresponds to what is defined in IZUPRMxx in SYS1.PARMLIB

****** Note – You will need to add the OWNER for the RDEFINEs described below. Also, the IZUDFLT is assumed from the IZUPRMxx member in SYS1.PARMLIB.**

****** Note – This is granting access to the IZUSVR userid and not a group ID. It is also for both started tasks.**

****** Note – In these definitions, it is assuming the SERVAUTH class is active and the permissions that are granted won't interfere with other definitions.**

****** Note – This is using the IZUUSER and IZUADMIN groups, and the connections to these groups is not set up as part of this process.**

****** Note – One may want to change the RDEFINE below to the following**
RDEFINE ZMFAPLA IZUDFLT.ZOSMF

```
/* Define the ZMFAPLA profile for the z/OSMF server                */
RDEFINE ZMFAPLA IZUDFLT.ZOSMF UACC(NONE)

/* The EJBROLE definitions are case-sensitive in RACF. Insure you */
/* preserve case for these commands                                */
/* Assumption: EJBROLE is defined, activated, and raclisted.      */
RDEFINE EJBROLE IZUDFLT.*.izuUsers UACC(NONE)

/* Define the z/OSMF Server profile                                */
 RDEFINE SERVER BBG.SECCLASS.ZMFAPLA UACC(NONE)

/* Permit the started task USERID access                           */
PERMIT BBG.SECCLASS.ZMFAPLA CLASS(SERVER) ID(IZUSVR) ACCESS(READ)

/* Roles processing will permit the z/OSMF Server groups to the    */
/* Application Server resources                                    */
/* Assumption: APPL class has been defined, activated, raclisted. */

/* Permit the Administrators group to this profile                 */
PERMIT CEA.CEATSO.* CLASS(SERVAUTH) ID(IZUADMIN) ACCESS(READ)

/* Permit the Users group to this profile                          */
PERMIT CEA.CEATSO.* CLASS(SERVAUTH) ID(IZUUSER) ACCESS(READ)

/* Permit the started task USERID to this profile                  */
PERMIT CEA.CEATSO.* CLASS(SERVAUTH) ID(IZUSVR) ACCESS(READ)

/* Make changes effective                                          */
SETROPTS RACLIST(SERVAUTH) REFRESH

/* Permit the Administrators group to these profiles               */
PERMIT IZUACCT CLASS(ACCTNUM) ID(IZUADMIN) ACCESS(READ)
PERMIT IZUFPROC CLASS(TSOPROC) ID(IZUADMIN) ACCESS(READ)

/* Permit the Users group to these profiles                        */
PERMIT IZUACCT CLASS(ACCTNUM) ID(IZUUSER) ACCESS(READ)
PERMIT IZUFPROC CLASS(TSOPROC) ID(IZUUSER) ACCESS(READ)
```

Define CONSOLE in TSOAUTH –

****** Note – You will need to add the OWNER for the RDEFINEs described below. In addition, check to see if adding the CONSOLE authority in TSOAUTH is something that is recommended.**

```
/* Define console profile in class TSOAUTH to issue MVS commands   */
 /* via EMCS consoles                                              */
   RDEFINE TSOAUTH CONSOLE UACC(NONE)
```

Permit IZUADMIN and IZUUSER access to CONSOLE in TSOAUTH –

****** Note – You will need to add the OWNER for the RDEFINEs described below.**

****** Note – This is granting access to the IZUADMIN and IZUUSER groups to have CONSOLE access in the TSOAUTH class. One may want to check to see if this is really recommended.**

****** Note – Check access to various OPERCMDS that are defined in your installation.**

```
/* Permit the Administrators group to these profile                */
PERMIT CONSOLE CLASS(TSOAUTH) ID(IZUADMIN) ACCESS(READ)

/* Permit the Users group to these profiles                        */
PERMIT CONSOLE CLASS(TSOAUTH) ID(IZUUSER) ACCESS(READ)

/* Make changes effective                                          */
SETROPTS RACLIST(TSOAUTH) REFRESH
```

****** Note – For the RDEFINEs below you may want to add the MVS.MCSOPER.IZU@*.** to the definition.**

```
/* Define MCS operator profile starting with prefix IZU@           */
RDEFINE OPERCMDS MVS.MCSOPER.IZU@* UACC(NONE)

/* Permit the Administrators group to these profiles               */
PERMIT MVS.MCSOPER.IZU@* CLASS(OPERCMDS) ID(IZUADMIN) ACCESS(READ)

/* Permit the Users group to these profiles                        */
PERMIT MVS.MCSOPER.IZU@* CLASS(OPERCMDS) ID(IZUUSER) ACCESS(READ)

/* Make changes effective                                          */
SETROPTS RACLIST(OPERCMDS) REFRESH
```

Permit started task user ID to use ICSF Service -

****** Note – The CSFCERV class does not deny access by default. If you define the profiles below, other areas may not work. Be cautious on what id defined and granted in the areas below.**

****** Note – This is also granting access to the IZUSVR userid that is for both the z/OSMF started tasks.**

If your installation uses hardware crypto in combination with ICSF, the use of various ICSF services might be restricted by your security policy. Some z/OSMF functions use these services. To use those functions if their use has been restricted by profiles in the CSFSERV class, the user ID assigned to the z/OSMF started task will need to be granted access to those profiles. The commands below will permit the started task user ID to use the necessary ICSF services.

****** Note – The following are for permissions that may not be defined in your environment.**

```
/*PERMIT CSFIQF  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*encipher callable service                                      */
/*PERMIT CSFENC  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*cryptographic variable encipher callable                       */
/*PERMIT CSFCVE  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*decipher callable service                                      */
/*PERMIT CSFDEC  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*symmetric algorithm encipher callable service                  */
/*PERMIT CSFSAE  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*symmetric algorithm decipher callable service                  */
/*PERMIT CSFSAD  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*one-way hash generate callable service                         */
/*PERMIT CSFOWH  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*random number generate callable service                        */
```

```
/*PERMIT CSFRNG  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*random number generate long callable service                   */
/*PERMIT CSFRNGL CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*PKA key generate callable service                              */
/*PERMIT CSFPKG  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*digital signature generate service                             */
/*PERMIT CSFDSG  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*digital signature verify callable service                      */
/*PERMIT CSFDSV  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*PKA key token change callable service                          */
/*PERMIT CSFPKT  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*retained key list callable service                             */
/*PERMIT CSFRKL  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*PKA Public Key Extract callable service                        */
/*PERMIT CSFPKX  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*PKA encrypt callable service                                   */
/*PERMIT CSFPKE  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*PKA decrypt callable service                                   */
/*PERMIT CSFPKD  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*PKA key import callable service                                */
/*PERMIT CSFPKI  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*multiple clear key import callable service                     */
/*PERMIT CSFCKM  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*key generate callable service                                  */
/*PERMIT CSFKGN  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*ECC Diffie-Hellman callable service                            */
/*PERMIT CSFEDH  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)          */
/*SETROPTS RACLIST(CSFSERV) REFRESH                              */
/*                                                               */
```

Various definitions in ZMFAPLA for the z/OSMF ADMINTASKS, WORKFLOWS, NOTIFICATIONS, z/OSMF Settings -

Profile definitions for the core functions

****** Note – OWNERs should be added to the RACF RDEFINEs below.**

```
/*   Profile Definitions for Core                               */
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.ADMINTASKS.APPLINKING UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.ADMINTASKS.IMPORTMANAGER UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.ADMINTASKS.LINKSTASK UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.ADMINTASKS.LOGGER UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.ADMINTASKS.UI_LOG_MANAGEMENT +
   UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.ADMINTASKS.USAGESTATISTICS +
   UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.LINK.** UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SETTINGS.SYSTEMS.VIEW UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SETTINGS.SYSTEMS.MODIFY UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SETTINGS.SYSTEMS UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS.VIEW UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS.MODIFY
   UACC(NONE)
```

Setup for Workflows Task –

****** Note – OWNERs should be added to the RACF RDEFINEs below.**

```
/*   Profile Definitions for “Workflow”                         */
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.WORKFLOW.WORKFLOWS UACC(NONE)
/* Profile Definitions for “Workflow administrator role”        */
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.WORKFLOW.ADMIN UACC(NONE)
```

Setup for Notification Task -

****** Note – OWNERs should be added to the RACF RDEFINEs below. In addition, you may want to define a backstop entry for the notifications**

```
/* Profile Definitions for "z/OSMF notification" */
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.NOTIFICATION.SETTINGS UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.NOTIFICATION.SETTINGS.ADMIN UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.NOTIFICATION.MODIFY UACC(NONE)
```

This is the end of the JCL for the Core set-up of z/OSMF.

The next section describes the z/OSMF security setup.

z/OSMF User Role Setup -

```
PERMIT IZUDFLT             CLASS(APPL)     ID(IZUUSER)  ACCESS(READ)
PERMIT IZUDFLT.*.izuUsers  CLASS(EJBROLE)  ID(IZUUSER)  ACCESS(READ)
PERMIT IZUDFLT.ZOSMF       CLASS(ZMFAPLA)  ID(IZUUSER)  ACCESS(READ)

/*   Permit definitions for Core                                  */
PERMIT IZUDFLT.ZOSMF.LINK.** CLASS(ZMFAPLA) ID(IZUUSER) +
   ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.SYSTEMS.VIEW CLASS(ZMFAPLA) +
   ID(IZUUSER) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.SYSTEMS CLASS(ZMFAPLA) ID(IZUUSER) +
   ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS CLASS(ZMFAPLA) +
   ID(IZUUSER) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS.VIEW CLASS(ZMFAPLA) +
   ID(IZUUSER) ACCESS(READ)
```

Permissions for Workflows Task –

```
/*   Permit definitions for Workflow                              */
PERMIT IZUDFLT.ZOSMF.WORKFLOW.WORKFLOWS CLASS(ZMFAPLA) +
   ID(IZUUSER) ACCESS(READ)
```

Permissions Setup for Notification Task -

```
/*   Permit definitions for notification                          */
PERMIT IZUDFLT.ZOSMF.NOTIFICATION.SETTINGS CLASS(ZMFAPLA) +
   ID(IZUUSER) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.NOTIFICATION.MODIFY CLASS(ZMFAPLA) +
   ID(IZUUSER) ACCESS(READ)
```

Permissions z/OSMF Administrator Role Setup -

```
/*                                                               */
/*  End zOSMF User Role Setup                                    */
/*                                                               */
/*   Begin zOSMF Administrator Role Setup                        */
/*                                                               */

PERMIT IZUDFLT             CLASS(APPL)     ID(IZUADMIN)  ACCESS(READ)
PERMIT IZUDFLT.*.izuUsers  CLASS(EJBROLE)  ID(IZUADMIN)  ACCESS(READ)
PERMIT IZUDFLT.ZOSMF       CLASS(ZMFAPLA)  ID(IZUADMIN)  ACCESS(READ)

/*   Permit definitions for Core                                  */
PERMIT IZUDFLT.ZOSMF.ADMINTASKS.APPLINKING CLASS(ZMFAPLA) +
   ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.ADMINTASKS.IMPORTMANAGER   CLASS(ZMFAPLA) +
   ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.ADMINTASKS.LINKSTASK  CLASS(ZMFAPLA) +
   ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.ADMINTASKS.LOGGER   CLASS(ZMFAPLA) +
```

```
    ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.ADMINTASKS.UI_LOG_MANAGEMENT  CLASS(ZMFAPLA) +
    ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.ADMINTASKS.USAGESTATISTICS   +
    CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.LINK.** CLASS(ZMFAPLA) ID(IZUADMIN) +
    ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.SYSTEMS.VIEW CLASS(ZMFAPLA) +
    ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.SYSTEMS.MODIFY CLASS(ZMFAPLA) +
    ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.SYSTEMS CLASS(ZMFAPLA) ID(IZUADMIN) +
    ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS CLASS(ZMFAPLA) +
    ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS.VIEW CLASS(ZMFAPLA) +
    ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS.MODIFY CLASS(ZMFAPLA) +
    ID(IZUADMIN) ACCESS(READ)
```

Permissions for Workflows –

```
/*   Permit definitions for Workflow                              */
PERMIT IZUDFLT.ZOSMF.WORKFLOW.WORKFLOWS CLASS(ZMFAPLA) +
    ID(IZUADMIN) ACCESS(READ)

/* Permit definitions for "Workflow administrator role"  */
PERMIT IZUDFLT.ZOSMF.WORKFLOW.ADMIN CLASS(ZMFAPLA) +
    ID(IZUADMIN) ACCESS(READ)
```

Permissions for Notification Task -

```
/* Permit definitions for "z/OSMF notification"                  */
PERMIT IZUDFLT.ZOSMF.NOTIFICATION.SETTINGS CLASS(ZMFAPLA) +
    ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.NOTIFICATION.SETTINGS.ADMIN CLASS(ZMFAPLA) +
    ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.NOTIFICATION.MODIFY CLASS(ZMFAPLA) +
    ID(IZUADMIN) ACCESS(READ)
```

Permissions for RADMIN tasks -

```
/* 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)
```

Permissions Security Administrator Role Setup -

```
PERMIT IZUDFLT            CLASS(APPL)    ID(IZUSECAD)  ACCESS(READ)
PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ID(IZUSECAD)  ACCESS(READ)
PERMIT IZUDFLT.ZOSMF      CLASS(ZMFAPLA) ID(IZUSECAD)  ACCESS(READ)
```

Permissions for Workflow Editor Task -

```
/*   Permit definitions for Workflow                              */
PERMIT IZUDFLT.ZOSMF.WORKFLOW.WORKFLOWS CLASS(ZMFAPLA) +
    ID(IZUSECAD) ACCESS(READ)
```

Setup for API Discovery User Interface.

****** NOTE – The following section may not be applicable for the initial setup.**

```
/*-------------------------------------------------------------*/
/* Begin Setup for API Discovery Swagger User Interface        */
/*-------------------------------------------------------------*/
/* The API Discovery feature lets you view z/OSMF REST APIs in */
/* a Swagger User Interface. That feature uses the Liberty REST */
/* handler framework, which requires the following RACF resource */
/* permissions to allow all z/OSMF users to access the Swagger */
/* User Interface.                                             */
RDEFINE EJBROLE +
   IZUDFLT.com.ibm.ws.management.security.resource.+
   allAuthenticatedUsers UACC(NONE)
PERMIT IZUDFLT.com.ibm.ws.management.security.resource.+
   allAuthenticatedUsers CLASS(EJBROLE) ID(IZUUSER) ACCESS(READ)
PERMIT IZUDFLT.com.ibm.ws.management.security.resource.+
   allAuthenticatedUsers CLASS(EJBROLE) ID(IZUADMIN) ACCESS(READ)
/*-------------------------------------------------------------*/
/* End Setup for API Discovery Swagger User Interface          */
/*-------------------------------------------------------------*/

/* Need to REFRESH these classes for Roles                     */
SETROPTS RACLIST(APPL) REFRESH
SETROPTS RACLIST(EJBROLE) REFRESH
SETROPTS RACLIST(ZMFAPLA) REFRESH
SETROPTS RACLIST(SERVER) REFRESH
SETROPTS RACLIST(STARTED) REFRESH
SETROPTS RACLIST(FACILITY) REFRESH

/* Connect the started task USERID to the CIM USER group       */
CONNECT (IZUSVR) GROUP(CFZUSRGP)

/*
//V2R3   EXEC PGM=IKJEFT01
//SYSPRINT DD SYSOUT=*
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
 /*                                                           */
 /*  The V2R3 step contains the profiles which are added in V2R3  */
 /*  release                                                  */

 /* Define the STARTED profiles for auto start function       */
 RDEFINE STARTED IZUINSTP.* UACC(NONE) STDATA(USER(IZUSVR) +
   GROUP(IZUADMIN) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))

 /* Define the CEA resource profile required for auto start   */
 /* function                                                  */
 RDEFINE SERVAUTH CEA.SIGNAL.* UACC(NONE)

 /* Permit the started task USERID to this profile            */
 PERMIT CEA.SIGNAL.* CLASS(SERVAUTH) ID(IZUSVR) ACCESS(READ)

 /* Profile for general setting                               */
 RDEFINE ZMFAPLA IZUDFLT.ZOSMF.GENERAL.SETTINGS UACC(NONE)

 /* Permit the Administrators group to this profile           */
 PERMIT IZUDFLT.ZOSMF.GENERAL.SETTINGS CLASS(ZMFAPLA) +
   ID(IZUADMIN) ACCESS(READ)

 /* Profile Definitions for “z/OSMF email function” */
 RDEFINE FACILITY IRR.RUSERMAP UACC(NONE)

 /* Permit the started task USERID to this profile            */
 PERMIT IRR.RUSERMAP CLASS(FACILITY) ID(IZUSVR) ACC(READ)
```

```
/*-------------------------------------------------------------*/
/* Begin Setup for Discovery CPC function in Systems task      */
/*-------------------------------------------------------------*/
/* Replace the <netid.nau> with the 3-17 character SNA name of */
/* the particular CPC.                                         */
/* Replace the <uppercasecommunityname> with the SNMP community */
/* name that is associated with the CPC.                       */
/* Replace the <imagename> with the 1-8 character which        */
/* represents LPAR name.                                       */
/*                                                             */
/* RDEFINE FACILITY HWI.APPLNAME.HWISERV UACC(NONE)            */
/* PERMIT HWI.APPLNAME.HWISERV CLASS(FACILITY) ID(IZUADMIN) +  */
/*   ACCESS(READ)                                              */
/* RDEFINE FACILITY HWI.TARGET.<netid.nau> UACC(NONE) +        */
/*   APPLDATA('<uppercasecommunityname>')                      */
/* RDEFINE FACILITY HWI.TARGET.<netid.nau>.<imagename> UACC(NONE) */
/* PERMIT HWI.TARGET.<netid.nau> CLASS(FACILITY) ID(IZUADMIN) + */
/*   ACCESS(READ)                                              */
/* PERMIT HWI.TARGET.<netid.nau>.<imagename> CLASS(FACILITY) + */
/*   ID(IZUADMIN) ACCESS(READ)                                 */
/*-------------------------------------------------------------*/
/* End Setup for Discovery CPC function in Systems task        */
/*-------------------------------------------------------------*/

/* If AT_TLS is enabled, the z/OSMF started task userid needs to */
/* be permitted on resource EZB.INITSTACK.sysname.tcpname      */
/*                                                             */
/* PERMIT EZB.INITSTACK.sysname.tcpname CLASS(SERVAUTH)  +     */
/*   ID(IZUSVR) ACCESS(READ)                                   */

/* Profile Definitions for "zOS Operator Consoles" task        */
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.CONSOLES.ZOSOPER UACC(NONE)
/* Permit definitions for "zOS Operator Consoles" task         */
PERMIT IZUDFLT.ZOSMF.CONSOLES.ZOSOPER CLASS(ZMFAPLA) +
  ID(IZUUSER) ACCESS(READ)
/* Permit definitions for "zOS Operator Consoles" task         */
PERMIT IZUDFLT.ZOSMF.CONSOLES.ZOSOPER CLASS(ZMFAPLA) +
  ID(IZUADMIN) ACCESS(READ)

/* Profile definitions for Named Angel Support                 */
RDEFINE SERVER BBG.ANGEL.IZUANG1 UACC(NONE)
PERMIT BBG.ANGEL.IZUANG1 CLASS(SERVER) ID(IZUSVR) ACCESS(READ)

/* Define security setup to permit Authorized WLM Service(ZOSWLM ) */
RDEFINE FACILITY BPX.WLMSERVER UACC(NONE)

/* Profile for TSO RESTful API remote support */
RDEFINE SERVAUTH CEA.CEATSO.FLOW.* UACC(NONE)
PERMIT CEA.CEATSO.FLOW.* CLASS(SERVAUTH) ID(IZUSVR) ACCESS(READ)
PERMIT CEA.CEATSO.FLOW.* CLASS(SERVAUTH) ID(IZUADMIN) ACCESS(READ)
PERMIT CEA.CEATSO.FLOW.* CLASS(SERVAUTH) ID(IZUUSER) ACCESS(READ)

/* Profile Definitions for z/OSMF Diagnostic Assistant support */
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.ADMINTASKS.DIAGNOSTIC_ASSISTANT +
  UACC(NONE)
PERMIT IZUDFLT.ZOSMF.ADMINTASKS.DIAGNOSTIC_ASSISTANT +
  CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)

/* Make changes effective                                      */
SETROPTS RACLIST(SERVER) REFRESH
SETROPTS RACLIST(SERVAUTH) REFRESH
SETROPTS RACLIST(ZMFAPLA) REFRESH
SETROPTS RACLIST(FACILITY) REFRESH

/*                                                             */
/*   End V2R3 step Setup                                       */
```

```
 /*                                                                 */
/*
//CLOUD  EXEC PGM=IKJEFT01
//SYSPRINT DD SYSOUT=*
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
 /*                                                                 */
 /*  The CLOUD step performs setup that is required as part of      */
 /*  base Core setup in support of Cloud Provisioning and           */
 /*  Management.                                                    */

 /* Connect the started task user ID to the IZUSECAD group.         */
 /* This is needed so z/OSMF initialization processing can create   */
 /* a CLOUD properties file and assign its group ownership to       */
 /* IZUSECAD.                                                       */
 /*                                                                 */
 /* If this is not done, the server job log will contain an         */
 /* IZUG202E error message about failing to set the group           */
 /* ownership.  An IYURM0041E message will also be written to the   */
 /* console and IZUG log.  Cloud Provisioning and Management        */
 /* operations requiring automatic security processing will be      */
 /* disabled.  The rest of z/OSMF is not affected and will operate  */
 /* normally.                                                       */

 CONNECT (IZUSVR) GROUP(IZUSECAD)

 /*                                                                 */
 /* End CLOUD step Setup                                            */
 /*                                                                 */
```

This is the end of the JCL to set up z/OSMF for V2R3.

6 Additional Security Setup Areas

The following table provides a high level overview of the additional areas in z/OSMF with a brief description and the RACF profiles. More details will follow afterwards.

MENU ITEM	MENU– SUB-ITEM (TASK)	RACF Profiles – ZMFAPLA Class
Welcome		
CONSOLES – z/OS Operator Consoles	The z/OS Operator Consoles task allows you to work with z/OS consoles, view system messages, and issue system commands, for systems that are defined with the Systems task of the z/OSMF settings category	
z/OS Operator Consoles		*Saf-prefix*.ZOSMF.CONSOLES.ZOSOPER
Jobs and Resources – SDSF	The SDSF task of z/OSMF lets you see key summary information about your sysplex in a graphical form, work with jobs and checks for the IBM z/OS Health Checker. It includes the functions you would normally see in SDSF on TSO. Access to the views in SDSF is protected in the same way as the corresponding panel command in z/OS SDSF	
SDSF		*Saf-prefix*.ZOSMF.IBMSDSF.JOBS *Saf-prefix*.ZOSMF.IBMSDSF.SETTINGS
z/OSMF Diagnostic Assistant – z/OSMF Diagnostic Assistant	The SDSF task of z/OSMF lets you see key summary information about your sysplex in a graphical form, work with jobs and checks for the IBM z/OS Health Checker. It includes the functions you would normally see in SDSF on TSO. Access to the views in SDSF is protected in the same way as the corresponding panel command in z/OS SDSF	
z/OSMF Diagnostic Assistant		*Saf-prefix*.ZOSMF.ADMINTASKS.DIAGNOSTIC.ASSISTANT
Cloud Provisioning	• From within the Cloud Provisioning plug-in, you can perform software provision for z/OS middleware. This work includes creating instances of CICS, Db2, IMS, MQ, and Websphere Application Server (WAS)	
Cloud Provisioning	ZMFAPLA class	*Saf-prefix*.ZOSMF.PROVISIONING.SOFTWARE_SERVICES *Saf-prefix*.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT *Saf-prefix*.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.ENWRP *Saf-prefix*.ZOSMF.WORKFLOW.EDITOR *Saf-prefix*.ZOSMF.VARIABLES.SYSTEM.ADMIN *Saf-prefix*.ZOSMF.SECURITY.ADMIN

MENU ITEM	MENU– SUB-ITEM (TASK)	RACF Profiles – ZMFAPLA Class
	ZMFCLOUD class	*Saf-prefix*.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT *Saf-prefix*.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT *Saf-prefix*.ZOSMF.PROVISIONING.RESOURCE_POOL.WLM *Saf-prefix*.ZOSMF.PROVISIONING.RESOURCE_POOL.NETWORK *Saf-prefix*.ZOSMF.TEMPLATE.APPROVERS *Saf-prefix*.ZOSMF.SECURITY.ADMIN
Configuration – Network Configuration Assistant	The Network Configuration Assistant plug-in simplifies and optimizes the configuration of policy-based networking of the z/OS Communications Server.	
	Application Linking Manager	*Saf-prefix*.ZOSMF.ADMINTASKS.APPLINKING
Performance	This area provides the plug-ins for capacity provisioning, resource monitoring, system status, and workload management,	
Capacity Provisioning Task	The Capacity Provisioning plug-in manages domain configurations and provisioning policies and can request reports of the status of the Capacity Provisioning Manager	
		Saf-prefix.ZOSMF.CAPACITY_PROVISIONING *Saf-prefix*.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT *Saf-prefix*.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT.DOMAIN *Saf-prefix*.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT.POLICY *Saf-prefix*.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.VIEW
Resource Monitoring Task	The Resource Monitoring plug-in monitors the performance of the z/OS, AIX, Linux, and Windows systems in your enterprise	
		Saf-prefix.ZOSMF.RESOURCE_MONITORING *Saf-prefix*.ZOSMF.RESOURCE_MONITORING.OVERVIEW *Saf-prefix*.ZOSMF.RESOURCE_MONITORING.PERFDESKS
Workload Management Task	The Resource Monitoring plug-in monitors the performance of the z/OS, AIX, Linux, and Windows systems in your enterprise	

MENU ITEM	MENU– SUB-ITEM (TASK)	RACF Profiles – ZMFAPLA Class
		Saf-prefix. ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.VIEW *Saf-prefix*. ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.MODIFY *Saf-prefix*. ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.INSTALL *Saf-prefix*. ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.ENWRP
System Task	The System Status task in z/OSMF require the RMF feature of z/OS.	
Problem Determination – Incident Log	The Incident Log plug-in can diagnose system problems and send diagnostic data to IBM or other vendors for further diagnostics	
Incident Log		*Saf-prefix*. ZOSMF.INCIDENT_LOG *Saf-prefix*. ZOSMF.INCIDENT_LOG.INCIDENT_LOG
Software-Software Management	The Software Management plug-in manages z/OS software inventory, deploys SMP/E packaged and installed software, and generates reports about your software	
Software Management		*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 *Saf-prefix*. ZOSMF. SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT *Saf-prefix*. ZOSMF. SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT
Sysplex Management – Sysplex Management Task	The Sysplex Management plug-in allows you to view sysplex resources graphically as well as view the systems in a sysplex. You can view physical configurations, such as coupling facilities and LPARs	
Sysplex Management Task		*Saf-prefix* ZOSMF.SYSPLEX *Saf-prefix* ZOSMF.SYSPLEX.LOG *Saf-prefix* ZOSMF.SYSPLEXMODIFY
z/OS Classic Interface – ISPF	The ISPF plug-in feature of z/OSMF provides access to traditional ISPF applications within a browser-based environment	
ISPF		*Saf-prefix* ZOSMF.ISPF.ISPF
z/ERT – zERT Network Analyzer Plug-in -z	The z/OS Encryption Readiness (zERT) Network Analyzer Plug-in provides the capability to analyze SMF data to identify the cryptographic protection characteristics of TCP and Enterprise Extender (EE) connections with local endpoints on your z/OS system.	
zERT Network Analyzer Plug-In		*Saf-prefix* ZOSMF.ZERT_NETWORK_ANALYZER

7 z/OSMF Tasks

7.1 Task – Consoles

The Consoles task currently contains only the z/OS Operator Consoles task.

DESCRIPTION

The z/OS Operator Consoles task allows you to work with z/OS consoles, view system messages, and issue system commands, for systems that are defined with the Systems task of the z/OSMF settings category.

Key features include the ability to:

- select a console from a list of systems in the sysplex
- see a system activity summary
- work with system messages
- enter system commands
- search and Filter system messages
- automatically retrieve and display message help
- retrieve messages from OPERLOG or SYSLOG
- allow REST APIs for client programs to issue system commands and retrieve command responses.

SECURITY SETUP

RACF Profiles ZMFAPLA Class

Saf-prefix.ZOSMF.CONSOLES.ZOSOPER

In order to use a z/OS console with the z/OS Operator Consoles task, additional setup is required. Please review the following areas:

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” in the z/OSMF Configuration Guide.

7.2 Task – Jobs and Resources - SDSF

The Jobs and Resources task currently contains only the SDSF task.

DESCRIPTION

The z/OSMF provides a framework for managing various aspects of the z/OS system through a web browser interface. The SDSF task of z/OSMF lets you see key summary information about your sysplex in a graphical form, work with jobs and checks for the IBM z/OS Health Checker. It includes the functions you would normally see in SDSF on TSO. Access to the views in SDSF is protected in the same way as the corresponding panel command in z/OS SDSF.

SECURITY SETUP

RACF Profiles ZMFAPLA Class

Saf-prefix.ZOSMF.IBMSDSF.JOBS
Saf-prefix.ZOSMF.IBMSDSF.SETTINGS

In order to use a z/OS console with the z/OS Operator Consoles task, additional setup is required. Please review the following areas:

- This is the area that describes the tasks to manage jobs, job output, system resources
- This tasks communicates with z/OS SDSF and provide information about your sysplex
- Provides the capabilities to configure the values used for SDSF task

7.3 Task – z/OSMF Diagnostic Assistant

This task is used by z/OSMF to collect diagnostic data.

DESCRIPTION

This task is used by z/OSMF to collect diagnostic data about z/OSMF and download it as a compressed file package.

SECURITY SETUP

RACF Profiles ZMFAPLA Class

Saf-prefix.ZOSMF.ADMINTASKS.DIAGNOSTIC_ASSISTANT

8 z/OSMF Plug-Ins — by Category

In this section, we will discuss some of the security permissions required for setting up z/OSMF Plug-ins.

8.1 Category: Cloud Provisioning - Cloud Provisioning Plug-in

NOTE: Cloud Provisioning uses the services of the following plug-ins:

- Network Configuration Assistant
- Resource Monitoring
- Workload Management

Therefore, we recommend you configure and enable these plug-ins before you enable Cloud Provisioning.

DESCRIPTION

From within the Cloud Provisioning plug-in, you can perform software provision for z/OS middleware. This work includes creating instances of CICS, Db2, IMS, MQ, and Websphere Application Server (WAS).

Under the Cloud Provisioning Category are the following functions:

- Marketplace - A sample of a software services marketplace for consumers. It can be used with Marketplace Administration as a model for developing you own consumer marketplace for software services.
- Marketplace Administration - A sample that offers administrative function for a software services marketplace.
- Resource Management - Define resources such as the domain of the systems and the classes of users (tenants) that will participate in Cloud on z/OS

SECURITY SETUP

RACF Profiles ZMFAPLA Class

Saf-prefix.ZOSMF.PROVISIONING.SOFTWARE_SERVICES
Saf-prefix.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT
Saf-prefix.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.ENWRP
Saf-prefix.ZOSMF.WORKFLOW.EDITOR
Saf-prefix.ZOSMF.VARIABLES.SYSTEM.ADMIN
Saf-prefix.ZOSMF.SECURITY.ADMIN

- Software Services - Provision z/OS software and manage the provisioned software, including deprovisioning.

z/OS Cloud Provisioning added several new RACF definitions to z/OSMF. The profiles that must be defined when you plan to use Cloud Provisioning are defined to the following RACF classes:

- ZMFAPLA: For z/OS Cloud Provisioning, this class consists of several profiles that are related to navigation tasks.
- ZMFCLOUD: This class was created when z/OS Cloud Provisioning was introduced in z/OSMF V2R2. It includes all resource profiles that are related to Cloud Provisioning.

z/OS Cloud Provisioning also added the following new RACF groups to z/OSMF:

- IYU: For z/OS Cloud Provisioning, this prefix is the default group name prefix. It can be used as is, or another name can be used. However, it must match the

parameter CLOUD_SAF_PREFIX in SYS1.PARMLIB(IZUPRMxx).

- IYU0: This name is the default group name for the domain administrator. It includes group IYU as its superior RACF group.
- IYU0RPAW: This name is the default group name for the WLM resource pool administrator group. It includes group IYU as its superior RACF group.
- IYU0RPAN: This name is the default group name for the networking resource pool administrator group. It includes group IYU as its superior RACF group.
- IYU000: This name is the default group name for tenant consumers. It includes group IYU0 as its superior RACF group.

PRE-REQUISITE SETUP:

z/OSMF Core: The Core z/OSMF security setup (IZUSEC) is required to be completed before running this Cloud Provisioning and Management security setup job.

Network Configuration Assistant: If you plan to support provisioning with templates that require being able to dynamically provision networking resources from a network resource pool, the Network Configuration Assistant plug-in must be configured. The Network Configuration Assistant plug-in's security setup or Cloud Provisioning and Management is part of this job.

Workload Management: If you plan to support provisioning with templates that require being able to dynamically provision workload management report classes from a workload management resource pool, the Workload Management plug-in must be configured. The Workload Management plug-in's security setup for Cloud Provisioning and Management is part of this job.

z/OSMF for z/OS Operator Consoles (REST Consoles): If you plan to support provisioning with templates that require issuing z/OS operator commands, the z/OSMF support for z/OS Operator Consoles must be configured. This will activate required resource classes. This job contains commented RACF commands that can be used to setup a specific ID to issue z/OS operator commands. That ID can then be used when running provisioning templates. A CP&M IVP template is available that can be used to verify if the REST Consoles configuration for a given ID works correctly when issuing operator commands that expect solicited and unsolicited command responses.

SECURITY SETUP

The IZUPRSEC job, found in SYS1.SAMPLIB contains sample RACF commands that may be used to create the security authorizations necessary to enable the Cloud Provisioning functions.

Your Security Administrator will need to review this and tailor it to fit your site-specific requirements.

Running this job defines required SAF resource profiles, creates corresponding SAF security groups, and grants appropriate authorizations.

RACF Profiles ZMFCLOUD Class

Saf-prefix.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT
Saf-prefix.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT
Saf-prefix.ZOSMF.PROVISIONING.RESOURCE_POOL.WLM
Saf-prefix.ZOSMF.PROVISIONING.RESOURCE_POOL.NETWORK
Saf-prefix.ZOSMF.TEMPLATE.APPROVERS
Saf-prefix.ZOSMF.SECURITY.ADMIN

8.2 Category: Configuration - Network Configuration Assistant Plug-in

DESCRIPTION

The Network Configuration Assistant plug-in simplifies and optimizes the configuration of policy-based networking of the z/OS Communications Server. It can generate and maintain policy files for the following technologies:

- AT-TLS (Application Transparent Transport Layer Security),
- DMD (Defense Manager Daemon),
- IDS (Intrusion Detection Services),
- IPSec (IP security), NSS (Network security services),
- PBR (Policy Based Routing), and QoS (Quality of service).

SECURITY SETUP

RACF Profiles ZMFAPLA Class

Saf-prefix.ZOSMF.CONFIGURATION_ASSISTANT
Saf-prefix.ZOSMF.CONFIGURATION_ASSISTANT.CONFIGURATION_ASSISTANT

The Policy Agent must be correctly configured to allow policy files to be exported if the import policy data function of the Configuration Assistant is used. The user must have the correct security access permissions to import the policy file. For more information about the required security settings, see the Configuration Assistant Help topic that is titled, “Policy Data Import” (specifically, the section titled “Policy Agent Preparation”).

When policy files are installed, the user must have adequate permissions to save the policy file in the specified location. If FTP is used, a valid user ID and password are required.

Note: 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.

When you plan to set up the Network Configuration Assistant plug-in, ensure that you apply the RACF commands that are found in the IZUCASEC job located in SYS1.SAMPLIB the contents of which is listed below:

8.3 Category: Performance

8.3.1 Capacity Provisioning Plug-in

DESCRIPTION

The Capacity Provisioning plug-in manages domain configurations and provisioning policies and can request reports of the status of the Capacity Provisioning Manager.

SECURITY SETUP

RACF Profiles ZMFAPLA Class

Saf-prefix.ZOSMF.CAPACITY_PROVISIONING
Saf-prefix.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT
Saf-prefix.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT.DOMAIN
Saf-prefix.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT.POLICY
Saf-prefix.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.VIEW

The IZUCPSEC job, found in SYS1.SAMPLIB contains sample RACF commands

that may be used to create the security authorizations necessary to enable the Capacity Provisioning functions.

Your Security Administrator will need to review this and tailor it to fit your site-specific requirements.

The Capacity Provisioning plug-in may require system customizations in order to run. This is to ensure that the users of the Capacity Provisioning task have access to the Capacity Provisioning domain.

8.3.2 Resource Monitoring Plug-in

DESCRIPTION

The Resource Monitoring plug-in monitors the performance of the z/OS, AIX, Linux, and Windows systems in your enterprise.

SECURITY SETUP

RACF Profiles ZMFAPLA Class

Saf-prefix.ZOSMF.RESOURCE_MONITORING
Saf-prefix.ZOSMF.RESOURCE_MONITORING.OVERVIEW
Saf-prefix.ZOSMF.RESOURCE_MONITORING.PERFDESKS

System Status Task

Quickly assess the workload performance on the systems in your enterprise and define the systems to be monitored.

This task is installed as part of the Resource Monitoring plug-in. No other configuration is required to use it. Connections to DDS servers to monitor z/OS or other systems are defined by using this task.

z/OSMF security for Resource Monitoring

If you plan to use the Resource Monitoring plug-in, you must make the SAF definitions for z/OSMF that are shown below. The defaults are documented in the IZURMSEC job found in SYS1.SAMPLIB.

8.3.3 Workload Management – Plug-in

DESCRIPTION

The Workload Management plug-in administers and operates Workload Management and manages WLM services definitions and policies.

SECURITY SETUP

RACF Profiles ZMFAPLA Class

Saf-prefix.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.VIEW
Saf-prefix.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.MODIFY
Saf-prefix.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.INSTALL
Saf-prefix.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.ENWRP

The defaults are documented in the IZUWMSEC job located in SYS1.SAMPLIB.

If you plan to use z/OS Cloud Provisioning, you must prepare more SAF definitions for WLM, which can be found documented in the IZURMSEC job found in SYS1.SAMPLIB.

8.4 Category: Problem Determination

8.4.1 Incident Log Plug-in

DESCRIPTION

The Incident Log plug-in can diagnose system problems and send diagnostic data to IBM or other vendors for further diagnostics.

SECURITY SETUP

RACF Profiles ZMFAPLA Class

Saf-prefix.ZOSMF.INCIDENT_LOG
Saf-prefix.ZOSMF.INCIDENT_LOG.INCIDENT_LOG

The default security definitions are documented in the IZUILSEC job located in SYS1.SAMPLIB. It contains sample RACF commands used to customize the z/OS host system so that it can run the Incident Log plug-in.

This task requires that specific z/OS components and facilities be enabled. Many of these components may already be configured on your system. Your Security Administrator will need to pay particular attention to the contents of this sample job in order to customize it to suit your site-specific standards.

8.5 Category: Software – Software Management Plug-in

DESCRIPTION

The Software Management plug-in manages z/OS software inventory, deploys SMP/E packaged and installed software, and generates reports about your software.

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.
- 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.

SECURITY SETUP

RACF Profiles 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
Saf-prefix.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT
Saf-prefix.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT

The IZUDMSEC job, found in SYS1.SAMPLIB contains sample RACF commands that may be used to create the security authorizations necessary to enable the Software Deployment plug-in.

Your Security Administrator will need to review this and tailor it to fit your site-specific requirements.

In order to use the Software Deployment plug-in, additional system customization may be required.

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.

8.6 Category: Sysplex – Sysplex Management Plug-in

DESCRIPTION

The Sysplex Management plug-in allows you to view sysplex resources graphically as well as view the systems in a sysplex. You can view physical configurations, such as coupling facilities and LPARs.

SECURITY SETUP

RACF Profiles ZMFAPLA Class

Saf-prefix `ZOSMF.SYSPLEX`
Saf-prefix `ZOSMF.SYSPLEX.LOG`
Saf-prefix `ZOSMF.SYSPLEXMODIFY`

The IZUSPECC job, found in SYS1.SAMPLIB contains sample RACF commands that may be used to create the security authorizations necessary to enable the Sysplex Management Plug-in.

8.7 Category: z/OS Classic Interface – ISPF Plug-in

DESCRIPTION

The ISPF plug-in feature of z/OSMF provides access to traditional ISPF applications within a browser-based environment.

When you log on to z/OSMF, this will show up on the z/OSMF welcome page under the z/OS Classic Interfaces task on the left tool bar.

This is brought up to aid in determining where security function will reside. z/OSMF uses tasks and plug-ins and it can be confusing to determine what belongs to which feature.

When configuring the ISPF plug-in, ensure that each user of the ISPF task is an existing TSO/E user that fits the following specific criteria:

Each user ID must be authorized to:

- TSO/E on the z/OS host system, have a valid password,
- a valid logon procedure and TSO/E account number,
- the JES spool.

Additionally, as required for access to z/OSMF, they must:

- Have an OMVS segment defined,
- Have a home directory defined.

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.

SECURITY SETUP

RACF Profiles ZMFAPLA Class

Saf-prefix `ZOSMF.ISPF.ISPF`

The IZUISSEC job, found in SYS1.SAMPLIB contains sample RACF commands that may be used to create the security authorizations necessary to enable the ISPF plug-in.

Your Security Administrator will need to review this and tailor it to fit your site-specific requirements.

8.8 Category: z/ERT – zERT Network Analyzer Plug-in

DESCRIPTION

The z/OS Encryption Readiness (zERT) Network Analyzer Plug-in provides the capability to analyze SMF data to identify the cryptographic protection characteristics of TCP and Enterprise Extender (EE) connections with local endpoints on your z/OS system.

Because the zERT Network Analyzer plug-in provides access to sensitive network security information, only users authorized to manage this data should be allowed to access to it. The IZUNASEC job includes sample RACF commands to create

Your Security Administrator may need to review this and tailor it to fit your site-specific requirements in order to:

- 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.

SECURITY SETUP

RACF Profiles ZMFAPLA Class

Saf-prefix `ZOSMF.ZERT_NETWORK_ANALYZER`

Your z/OS security administrator must perform additional steps to create the necessary authorizations which are detailed below.

The IZUNASEC job, found in SYS1.SAMPLIB contains sample RACF commands that may be used to create the group IZUZNA. The IZUZNA group is used to control access to this plug-in.

9 Sample Jobs in SYS1.SAMPLIB

These are the Sample Jobs provided in SYS1.SAMPLIB and a description of their purpose.

IZUAUTH	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).
IZUCASEC	Configuration Assistant - **plug-in**
IZUCPSEC	Capacity Provisioning - **plug-in**
IZUDELFN	The purpose of this job is to DELETE previous levels of z/OSMF FMIDs before installing the new FMIDs shipped in z/OSMF V2R2.
IZUDMSEC	Software Management - **plug-in**
IZUDWFVR	Software Management Workflow definition sample - plug-in
IZUDXEXP	Another new function is designed to provide a RESTful programming interface that allows a portable software instance to be created, by exporting a previously defined software instance. This function can be used to automate the creation of a software instance using a program. A sample REXX exec that can be used in a batch job is also provided in the IZUDXEXP member of the samplib data set; it is intended to create a software instance and then export it to create a portable software instance. This function is also available for z/OS V2.2 with the PTF for APAR PI72283.
IZUGCSEC	The job contains RACF commands for creating the required security authorizations for the z/OS Operator Consoles task. – **plug-in**
IZUILSEC	Incident Log - **plug-in**
IZUISALC	Allocates target and distribution libraries for z/OSMF.
IZUISDDD	Creates DDDEF entries for z/OSMF.
IZUISHFS	Allocates the HFS data set for z/OSMF. If you choose not to allocate a separate file system for the installation of z/OSM, then you can skip this sample job.
IZUISMKD	Executes the IZUMKDIR exec for z/OSMF.
IZUISSEC	ISPF - **plug-in**
IZUISZFS	This JCL will: a) Allocate the zFS data set for z/OS MF, and b) Execute IZUMNTFS EXEC to mount the ZFS data set at a given mountpoint. If you choose not to allocate a separate filesystem for z/OSMF install, then you can skip this sample job.
IZUMKDIR	This REXX exec will create the necessary directories for z/OSMF.
IZUMKFS	Initializes the z/OSMF user file system, which contains configuration settings and persistence information for z/OSMF.

IZUMNTFS This REXX EXEC will create product mount point and will mount the product HFS or ZFS data set at the newly created mountpoint.

IZUNASEC IBM z/OS Encryption Readiness Technology (zERT) Network Analyzer. – **plug-in**

IZUPRM00 Optional Parmlib member for z/OSMF. If your z/OSMF set-up requires customization, you can provide a customized member, IZUPRMxx, with installation-specific values for your configuration. IBM provides a sample member, IZUPRM00, which you can use as a model.

IZUPRSEC Security authorizations for IBM Cloud Provisioning and Management for z/OS environment which includes a default domain and default tenant to help you quickly get started. – **plug-in**

IZURMSEC Resource Monitoring - **plug-in**

IZUSEC Establishes security for z/OSMF by creating SAF-based authorizations. Contains RACF commands for creating the security definitions.

IZUSPSEC Contains RACF commands for creating the required security authorizations for the Sysplex Management task. – **plug-in**

IZUSVR2 This procedure can be used for starting the z/OSMF server manually.

IZUWMSEC Workload Management - **plug-in**

IZUZUNDAG REXX exec to create a customizes set of DDL directives for a set of zERT Network Analyzer database objects.

IZUDZNADI REXX exec for zERT Network Analyzer

IZUDZNAD REXX exec for zERT Network Analyzer

10 APPENDIX A: z/OSMF User Experiences — Survey Results

Between August of 2018 and February of 2019, we conducted two surveys of z/OSMF usage within the zExchange community. The first survey, which ran from August 3 – 16, 2018, had 73 respondents. The second survey, which ran from February 13 – March 13, 2019, had 67 respondents.

These surveys coincided with our SHARE presentations which were given at both SHARE – St. Louis in August of 2018 and SHARE – Phoenix in March of 2019. The survey responses, and the lively discussion prompted by the attendees at both SHARE sessions provided insight into those who may be using, or not using, z/OSMF and what successes and/or difficulties they may have experienced.

Of the respondents, almost half had implemented z/OSMF and were using it, with another 25% in the process of planning its implementation. About a fifth of respondents had no plans to implement z/OSMF and a small percentage, less than 10% had implemented it but were not using it.

Implementation and Use of z/OSMF

46% Implemented and in use

8% Implemented but not in use

25% Planning or in process

21% had no plans to implement or use

Most of those who responded have RACF running as their External Security Manager (60%). CA-ACF2 and CA-Top Secret were present in 20% of shops.

External Security Managers

60% RACF

20% ACF2

20% Top Secret

Overwhelmingly, most respondents categorized themselves as Novices with regard to their skill level with z/OSMF. A few added comments stating they were more involved with setting up z/OSMF rather than working with the applications or plug-ins, themselves.

Skill Level of Respondent

74% Novice

6% Intermediate

6% Expert

14% Other

Almost 75% of respondents who said they were using z/OSMF said they had been using it for two years or more.

Implementation time

10% <1 year

17% 1 year

24% 2 years

49% >2 years

When asked “Are you concerned about security issues surrounding z/OSMF?”, the respondents to the August 2018 survey given only a YES/NO option reported a close split leaning slightly towards not being concerned.

Concerns about security, Aug-2018

42% YES

58% NO

However, when we re-worded the question to “How concerned are you about security issues surrounding z/OSMF?” and provided more answer options, we got a more granular response.

Concerns about security issues, Feb-2019

10% Primary concern

40% Moderate concern

21% Some concern

29% No concern

Some Good, Some Bad, and Some Ugly – User Comments

When putting together a survey of simple multiple choice or option selections, you get purely quantitative data. Adding a comment box to each question allows respondents to a provide valuable insight into their personal experience. Below is a sampling of what our respondents had to say.

First, the good...

When asked if using z/OSMF had improved productivity and efficiency compared to before using it, about 40% of respondents reported replied that these areas had improved “somewhat” or “greatly”. About an equal number said things were “about the same”.

A sampling of positive comments are:

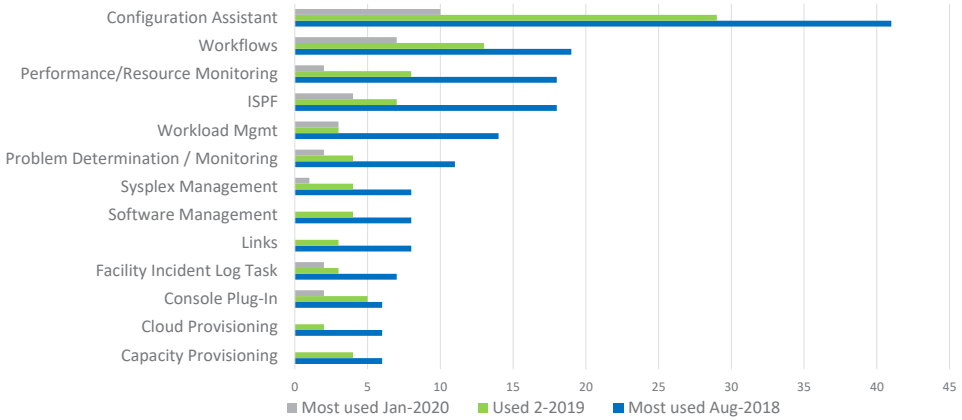
”Just started using and appears that going forward it should improve our process.”

”Not much productivity enhancement for experiences Systems Programmers. The Workflow becomes self-documenting for work that is done and that is a help.”

“If ZERT can provide the information we think it can, use of z/OSMF will increase as we use it to monitor network traffic and encryption methods.”

“Specifically in the area of AT-TLS set up and implementation.”

Asked what parts of z/OSMF were actually being used, the most popular function was the Network Configuration Assistant. This was followed by Workflows, Performance / Resource Monitoring, and ISPF.



On the topic of the Network Configuration Assistant and AT-TLS, we received the most positive comments. From the statistics of who is using what z/OSMF plug-ins, Network Configuration Assistant was the most used. Users said:

"We had never implemented AT-TLS (or IP-Sec) although we needed to do so. ***The Config Assistant is wonderful for getting that done*** *ONCE you UNDERSTAND how to use it."*

"The network team finds configuration assistance a useful tool. "

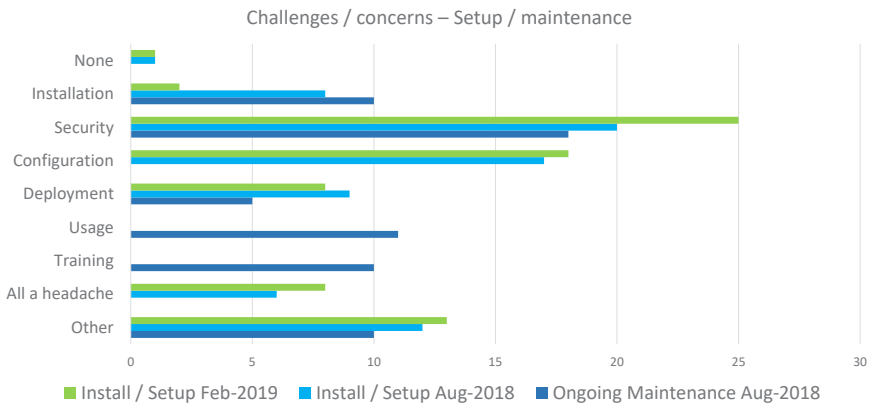
"Main motivation: Access to the Configuration Assistant (AT-TLS implementation) "

"For Config Assist, great!!!"

"It's great for creating and managing the Policy Agent configurations."

Not everyone had something positive to say.

When asked "What were the biggest challenges or concerns with its installation, setup, configuration and ongoing maintenance?", most cited security as the biggest headaches. This was also a common theme across the comments sections of the surveys.



Considering the comments from the questions about security, the concerns seems to be centered on that of configuring security properly so that functions work

properly rather than whether the environment was secure from hacking or misuse:

"It seemed very awkward to figure what was needed for a lot due to the number of RACF changes needed to get it up and running."

"Am not aware of any security issues."

"Any time we research a plug-in for any functionality or want to start z/OSMF on other systems we run into numerous security issues."

Some negative comments in general give insight into the types of trouble users experienced. Most of these concerned implementing z/OSMF or its plug-ins:

*"It was a **very ugly/hard experience** the first time I tried to implement and setup TCPIP using z/OSMF. Since then I never used."*

"Still fighting issues after 3 years."

"None of these are in use on a consistent basis due to issues using them."

"Plugins are a nightmare."

*"tried to implement basic functions but **never got it to work.**"*

"Leave the toys to the boys."

A few respondents provided details surrounding the complexity of configuring security for z/OSMF:

"**Security issues** *have kept it from being deployed in our shop."*

*"Since **security is a separate group** getting the appropriate paperwork submitted requesting their setup made it a **long and tedious install.** "*

"Any time we research a plug-in for any functionality or want to start z/OSMF on other systems we run into numerous security issues."

*"In the process of getting it installed but setting up the **security rules has been extremely challenging.**"*

11 APPENDIX B: Configuring z/OSMF to Work with CA-ACF2 or CA-Top Secret

If your environment has an External Security Manager other than RACF you will need to create equivalent commands for your security product. See IBM's **z/OSMF Configuration Guide, Appendix A** for a list of resources, groups, IDs, and authorizations that need to be defined to your security product.

Broadcom has announced the following PTFs that include sample JCL for both CA ACF2 and CA Top Secret and also sample REXX code for configuring z/OSMF Cloud Provisioning in a CA Top Secret environment.

For more details, we recommend searching (Google, or your search engine of choice) for the latest information on these PTF(s):

PTF(s) for CA ACF2:

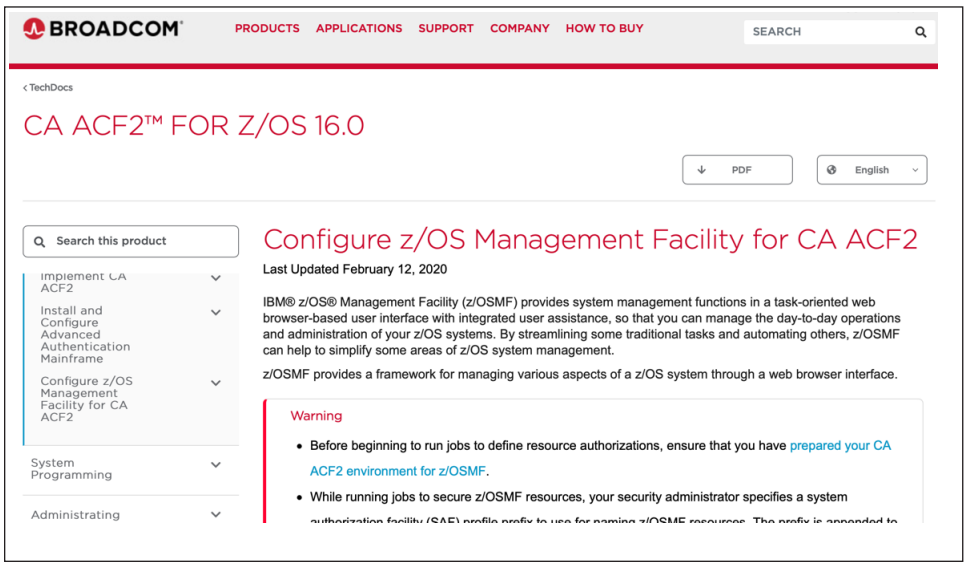
SO04537 Sample JCL for z/OSMF Security Configuration
SO04740 z/OSMF Cloud Provisioning REXX

PTF for CA Top Secret:

SO03835 – Sample JCL for z/OSMF Security Configuration and Cloud Provisioning REXX

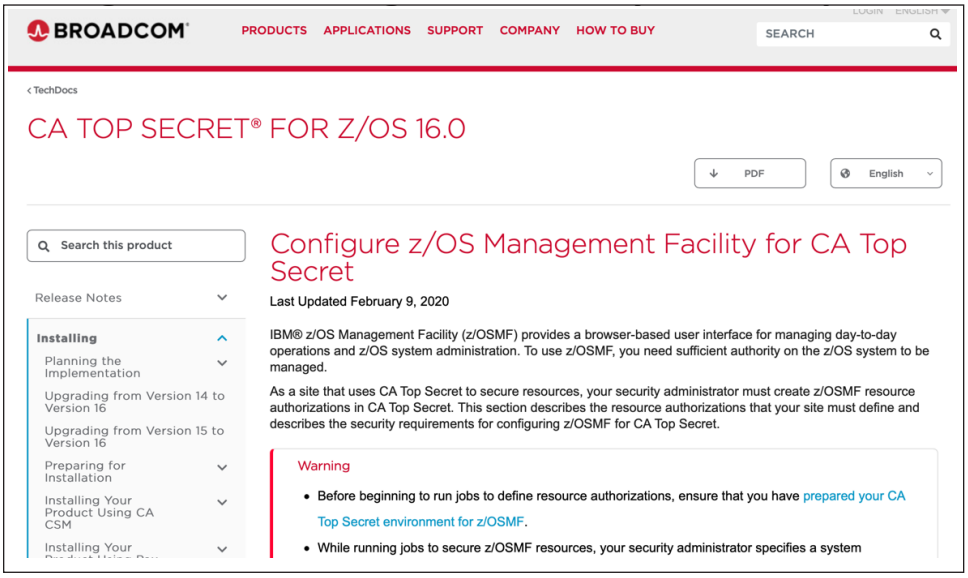
You may also find the information at these links useful, **though the information is subject to change.**

Configure z/OS Management Facility for CA ACF2:
Last Updated February 12, 2020
https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-mainframe-software/security/ca-acf2-for-z-os/16-0/installing-and-implementing/configure-z-os-management-facility-for-ca-acf2.html#toccontentbroadcom-techdocsusencamainframesoftwaresecuritycaacf2forzos160installingandimplementinginstallandconfigureadvancedauthenticationmainframehtmlInstallandConfigureAdvancedAuthenticationMainframe



Configure z/OS Management Facility for CA Top Secret:
Last Updated February 9, 2020
https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-mainframe-software/security/ca-top-secret-for-z-os/16-0/installing/configure-z-os-management-facility-for-ca-top-secret.html#toccontentbroadcomtechdocsusencamainframesoftwaresecuritycatopsecretforzos160installinghtmlInstalling

Configure z/OS Management Facility for CA Top Secret:
Last Updated February 9, 2020



12 APPENDIX C: Reference material

12.1 IBM Documentation

IBM has, in the past, frequently changed where to find its documentation. Please search for these documents with your preferred search engine:

z/OS Management Facility Redbook,

z/OS Management Facility Configuration Guide,

z/OS Management Facility Programming Guide.

12.2 z/OSMF IBM Blog

Please search for this page with your preferred search engine:

z/OSMF One Stop Hub

12.3 ListServs

Sign up for these two ListServs which occasionally include some lively discussion of z/OSMF topics:

IBM-MAIN ListServ: https://listserv.ua.edu/

Search for and subscribe to IBM-MAIN

RACF-L ListServ: https://listserv.uga.edu/

Search for and subscribe to RACF-L

12.4 Other References

Interest in z/OSMF is abounding – Marna's Musings (Marna Walle of IBM)

See a proof of concept Workflow-Driven Installation presented by Phoenix Software: Presentation on z/OSMF Workflow-Driven Installation

www.terminaltalk.net

13 APPENDIX D: RACF Security Configuration Requirements

In order to use z/OSMF, users will need to be granted sufficient authority within the z/OS system. These authorities must be created within the external security manager, on the z/OS system being managed. Sample jobs are included within SYS1.SAMPLIB which may be used to create user IDs, groups and resource profiles for the z/OSMF configuration.

13.1 Class Activations Required by z/OSMF

The following RACF security classes must be active when configuring z/OSMF. Your security administrator may enter the commands directly, as shown below. The commands for activating the classes – with generic profile checking active - may also be found within the comment sections of the IZUxxSEC jobs.

ACCTNUM - *Controls access to the account number used for the procedure for the z/OSMF REST interfaces.*

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.

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.*

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.*

JESSPOOL - *Allows the user to retrieve messages from the system log (SYSLOG).*

LOGSTRM – Allows the user to retrieve messages from the operations log (OPERLOG).

OPERCMDS – *Allows the user to issue system commands when using an EMCS console by using the z/OS Operator Consoles task.*

SERVAUTH – Is used to control access to various TCP/IP functions. In z/OSMF it 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.*

SERVER – This class is used to control the server's ability to register with the daemon. It is used to allow *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.*

STARTED – This class is used to define an identity during the process of an MFS START command *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.*

TSOAUTH – Is used for user authorities such as OPER and MOUNT. *Allows the user to create an EMCS console by using the z/OS Operator Consoles task.*

TSOPROC – TSO logon procedures. *Controls access to the procedure for the z/OSMF REST interfaces.*

ZMFALPA - *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*.

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.*

The ZMFCLOUD class requires the RACLIST option.

14 APPENDIX E: Table with all sample basic profiles

MENU ITEM	MENU - SUB-ITEM (TASK)	CORE FUNC-TION	PLUG-IN	RACF Profiles -
Welcome		Y		
Notifications		Y		*Saf-prefix*.ZOSMF.NOTIFICATION *Saf-prefix*.ZOSMF.NOTIFICATION.MODIFY *Saf-prefix*.ZOSMF.NOTIFICATION.SETTINGS *Saf-prefix*.ZOSMF.NOTIFICATION.SETTINGS.ADMIN
Workflow Editor		Y		*Saf-prefix*.ZOSMF.WORKFLOW *Saf-prefix*.ZOSMF.WORKFLOW.ADMIN *Saf-prefix*.ZOSMF.WORKFLOW.EDITOR
Workflows		Y		*Saf-prefix*.ZOSMF.WORKFLOW.WORKFLOWS
Cloud Provisioning			YES	*Saf-prefix*.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT *Saf-prefix*.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT *Saf-prefix*.ZOSMF.PROVISIONING.RESOURCE_POOL.WLM *Saf-prefix*.ZOSMF.PROVISIONING.RESOURCE_POOL.NETWORK *Saf-prefix*.ZOSMF.TEMPLATE.APPROVERS *Saf-prefix*.ZOSMF.SECURITY.ADMIN
	Marketplace			
	Marketplace Administration			
	Resource Management			*Saf-prefix*.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT
	Software Services			*Saf-prefix*.ZOSMF.PROVISIONING.SOFTWARE_SERVICES
Configuration				*Saf-prefix*.ZOSMF.CONFIGURATION_ASSISTANT
	Network Configuration Assistant		COMM SERVER _CFG	*Saf-prefix*.ZOSMF.CONFIGURATION_ASSISTANT.CONFIGURATION_ASSISTANT
Consoles				
	z/OS Operator Consoles			*Saf-prefix*.ZOSMF.CONSOLES.ZOSOPER
Jobs and Resources				
	SDSF			See SDSF section in administration tasks for details
Links		Y		*Saf-prefix*.ZOSMF.ADMINTASKS.LINK.linkname
	Shopz			*Saf-prefix*.ZOSMF.LINK.SHOPZSERIES

MENU ITEM	MENU - SUB-ITEM (TASK)	CORE FUNC-TION	PLUG-IN	RACF Profiles -
	Support for z/OS			*Saf-prefix*.ZOSMF.LINK.SUPPORT_FOR_Z_OS
	WSC Flashes & Techdocs			*Saf-prefix*.ZOSMF.LINK.WAS_FLASHES_ TECHDOCS
	z Systems			*Saf-prefix*.ZOSMF.LINK.SYSTEM_Z_ REDBOOKS
	z/OS Basics Information Center			*Saf-prefix*.ZOSMF.LINK.Z_OS_BASICS_ INFORMATION_CENTER
	z/OS Home Page			*Saf-prefix*.ZOSMF.LINK.Z_OS_HOME_PAGE
	z/OS Internet Library			*Saf-prefix*.ZOSMF.LINK.Z_OS_INTERNET_ LIBRARY
Performance				
	Capacity Provisioning		CAPA CITY_ PROV	*Saf-prefix*.ZOSMF.CAPACITY_PROVISIONING *Saf-prefix*.ZOSMF.CAPACITY_PROVISIONING. CAPACITY_PROVISIONING.EDIT *Saf-prefix*.ZOSMF.CAPACITY_PROVISIONING. CAPACITY_PROVISIONING.EDIT.DOMAIN *Saf-prefix*.ZOSMF.CAPACITY_PROVISIONING. CAPACITY_PROVISIONING.EDIT.POLICY *Saf-prefix*.ZOSMF.CAPACITY_PROVISIONING. CAPACITY_PROVISIONING.VIEW
	Resource Monitoring		RESO URCE_ MON	*Saf-prefix*.ZOSMF.RESOURCE_MONITORING *Saf-prefix*.ZOSMF.RESOURCE_MONITORING. OVERVIEW *Saf-prefix*.ZOSMF.RESOURCE_MONITORING .PERFDESKS
	System Status			
	Workload Management		WORK LOAD_ MGMT	*Saf-prefix*.ZOSMF.WORKLOAD_ MANAGEMENT *Saf-prefix*.ZOSMF.WORKLOAD_ MANAGEMENT.WORKLOAD_MANAGEMENT. ENWRP *Saf-prefix*.ZOSMF.WORKLOAD_ MANAGEMENT.WORKLOAD_MANAGEMENT. INSTALL *Saf-prefix*.ZOSMF.WORKLOAD_ MANAGEMENT.WORKLOAD_MANAGEMENT. MODIFY *Saf-prefix*.ZOSMF.WORKLOAD_ MANAGEMENT.WORKLOAD_MANAGEMENT. VIEW
Problem Determination				

MENU ITEM	MENU - SUB-ITEM (TASK)	CORE FUNC-TION	PLUG-IN	RACF Profiles -
	Incident Log		INCI DENT _LOG	*Saf-prefix*.ZOSMF.INCIDENT_LOG. *Saf-prefix*.ZOSMF.INCIDENT_LOG.INCIDENT_ LOG
Software				*Saf-prefix*.ZOSMF.SOFTWARE_DEPLOYMENT
	Software Management		SOFT WARE _MGMT	*Saf-prefix*.ZOSMF.SOFTWARE_DEPLOYMENT. DATA *Saf-prefix*.ZOSMF.SOFTWARE_DEPLOYMENT. SOFTWARE_MAMANGEMENT *Saf-prefix*.ZOSMF.SOFTWARE_DEPLOYMENT. SOFTWARE_MANAGEMENT.CATEGORIES. MODIFY *Saf-prefix*.ZOSMF.SOFTWARE_DEPLOYMENT. SOFTWARE_MANAGEMENT.CATEGORIES. PRODUCT_INFO_FILERETRIEVE
Sysplex				*Saf-prefix*.ZOSMF.SYSPLEX *Saf-prefix*.ZOSMF.SYSPLEX.LOG *Saf-prefix*.ZOSMF.SYSPLEX.MODIFY
	Sysplex Management		SYSP LEX_ MGMT	
z/OS Classic Interfaces				
	ISPF		ISPF	*Saf-prefix*.ZOSMF.ISPF.ISPF A valid account number that is defined in ACCTNUM class A valid TSOPROC defined to your system. z/ OSMF provide a default of IZUFPROC.
z/OSMF Administration				*Saf-prefix*.ZOSMF.ADMINTASKS *Saf-prefix*.ZOSMF.ADMINTASKS.LOGGER *Saf-prefix*.ZOSMF.ADMINTASKS.UI_LOG_ MANAGMENT
	Application Linking Manager	Y		*Saf-prefix*.ZOSMF.ADMINTASKS.APPLINKING
	Import Manager	Y		*Saf-prefix*.ZOSMF.ADMINTASKS. IMPORTMANAGER
	Links	Y		*Saf-prefix*.ZOSMF.ADMINTASKS.LINKSTASK
	Usage Statistics	Y		*Saf-prefix*.ZOSMF.ADMINTASKS. USAGESTATISTICS
z/OSMF Settings				*Saf-prefix*.ZOSMF *Saf-prefix*.ZOSMF.SETTINGS

MENU ITEM	MENU - SUB-ITEM (TASK)	CORE FUNC-TION	PLUG-IN	RACF Profiles -
	FTP Servers	Y		*Saf-prefix*.ZOSMF.SETTINGS.FTP_SERVERS *Saf-prefix*.ZOSMF.SETTINGS.FTP_SERVERS.MODIFY *Saf-prefix*.ZOSMF.SETTINGS.FTP_SERVERS.VIEW
	General Settings	Y		*Saf-prefix*.ZOSMF.SETTINGS.SYSTEMS *Saf-prefix*.ZOSMF.SETTINGS.SYSTEMS.MODIFY *Saf-prefix*.ZOSMF.SETTINGS.SYSTEMS.VIEW
	Notification Settings	Y		*Saf-prefix*.ZOSMF.SETTINGS.SYSTEMS *Saf-prefix*.ZOSMF.SETTINGS.SYSTEMS.MODIFY *Saf-prefix*.ZOSMF.SETTINGS.SYSTEMS.VIEW
	SDSF			*Saf-prefix*.ZOSMF.IBMSDSF.JOBS *Saf-prefix*.ZOSMF.IBMSDSF.SETTINGS
	Systems			*Saf-prefix*.ZOSMF.SETTINGS.SYSTEMS *Saf-prefix*.ZOSMF.SETTINGS.SYSTEMS.MODIFY *Saf-prefix*.ZOSMF.SETTINGS.SYSTEMS.VIEW
z/OSMF Diagnostic Assistant				
	z/OSMF Diagnostic Assistant			*Saf-prefix*.ZOSMF.ADMINTASKS.DIAGNOSTIC_ASSISTANT
z/ERT	zERT Network Analyzer Plug-In		ZERT_ANALYZER	
				Saf-prefix ZOSMF.ZERT_NETWORK_ANALYZER

15 APPENDIX F: IZUSEC (complete JCL listing)

```
//IZUCORE JOB MSGCLASS=C,MSGLEVEL=(1,1),USER=XXXXXXX,NOTIFY=XXXXXXX
//*****************************************************************
//* PROPRIETARY STATEMENT:                                        *
//*    Licensed Materials - Property of IBM                       *
//*    5650-ZOS Copyright IBM Corp. 2015, 2018                    *
//*                                                               *
//*    STATUS=HSMA230                                             *
//*                                                               *
//* DESCRIPTIVE NAME:                                             *
//*    z/OSMF SERVER default security setup                       *
//*                                                               *
//*    The JCL contains the security setup for z/OSMF server.     *
//*    You can customize this JCL to create a security setup      *
//*    for the z/OSMF Server as you wish.                         *
//*                                                               *
//*    NOTE: The V2R3 and CLOUD steps are added to job IZUSEC in  *
//*    this release. The V2R3 step contains the profiles which are *
//*    new in z/OS V2R3. The CLOUD step connects the started task *
//*    ID to the IZUSECAD group, which is required as part of z/OSMF  *
//*    initialization in z/OS V2R3. If you have previously installed  *
//*    and configured z/OSMF, steps V2R3 and CLOUD are the only    *
//*    steps you need to run.                                     *
//*                                                               *
//*****************************************************************
//*                                                               *
//* This job must be run using a user ID that has the RACF SPECIAL   *
//* attribute.                                                    *
//*                                                               *
//* This job assumes that the BPX.NEXT.USER profile has been       *
//* defined in the FACILITY class to enable the use of AUTOUID     *
//* and AUTOGID.  See the topic "Automatically assigning unique   *
//* IDs through UNIX services" in z/OS Security Server RACF       *
//* Security Administrator's Guide for additional information     *
//* about automatic UID and GID assignment.  If this function has *
//* not been enabled, you must assign unique UIDs to the IZUSVR   *
//* and IZUGUEST user IDs, and unique GIDs to the groups          *
//* IZUADMIN, IZUSECAD, IZUUSER, and IZUUNGRP.                    *
//*                                                               *
//*****************************************************************
//*
//* This step sets up z/OSMF core security settings.
//*
//STEP1  EXEC PGM=IKJEFT01
//SYSPRINT DD SYSOUT=*
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *

 /* Begin "Core" Setup                                           */
 /*                                                              */
 /* This commented section contains the CLASS activation commands.  */
 /* Ensure the following classes are active before executing this   */
 /* script or creating profiles in these classes.                */
 /*                                                              */
 /* Activate and RACLIST the APPL class                          */
 /*SETROPTS CLASSACT(APPL)                                       */
 /*SETROPTS RACLIST(APPL) GENERIC(APPL)                          */
 /*                                                              */
 /* Activate and RACLIST the EJBROLE class                       */
 /*SETROPTS CLASSACT(EJBROLE)                                    */
```

```
/*SETROPTS RACLIST(EJBROLE) GENERIC(EJBROLE)                    */
/*                                                              */
/* Activate and RACLIST the FACILITY class                      */
/*SETROPTS CLASSACT(FACILITY)                                   */
/*SETROPTS RACLIST(FACILITY)                                    */
/*                                                              */
/* Activate and RACLIST the SERVER class                        */
/*SETROPTS CLASSACT(SERVER)                                     */
/*SETROPTS RACLIST(SERVER)                                      */
/*                                                              */
/* Activate and RACLIST the SERVAUTH class                      */
/*SETROPTS CLASSACT(SERVAUTH)                                   */
/*SETROPTS RACLIST(SERVAUTH) GENERIC(SERVAUTH)                  */
/*                                                              */
/* Activate and RACLIST the STARTED class                       */
/*SETROPTS CLASSACT(STARTED)                                    */
/*SETROPTS RACLIST(STARTED) GENERIC(STARTED)                    */
/*                                                              */
/* Activate and RACLIST the ZMFAPLA class                       */
/*SETROPTS CLASSACT(ZMFAPLA)                                    */
/*SETROPTS RACLIST(ZMFAPLA) GENERIC(ZMFAPLA)                    */
/*                                                              */
/* Activate the ACCTNUM class                                   */
/*SETROPTS CLASSACT(ACCTNUM)                                    */
/* Activate the TSOPROC class                                   */
/*SETROPTS CLASSACT(TSOPROC)                                    */
/* Refresh the ACCTNUM class                                    */
/* SETROPTS RACLIST(ACCTNUM) REFRESH                            */
/* Refresh the TSOPROC class                                    */
/* SETROPTS RACLIST(TSOPROC) REFRESH                            */
/*                                                              */
/* Activate the TSOAUTH class                                   */
SETROPTS CLASSACT(TSOAUTH)
/* Refresh the TSOAUTH class                                    */
SETROPTS RACLIST(TSOAUTH)
/*                                                              */
/* Activate the OPERCMDS class                                  */
SETROPTS CLASSACT(OPERCMDS)
/* Refresh the OPERCMDS class                                   */
SETROPTS RACLIST(OPERCMDS)

/* Create the z/OSMF Administrators group                       */
ADDGROUP IZUADMIN OMVS(AUTOGID)

/* Create the z/OSMF Users group                                */
ADDGROUP IZUUSER OMVS(AUTOGID)

/* Create the z/OSMF Unauthenticated group                      */
ADDGROUP IZUUNGRP OMVS(AUTOGID)

/* Create the started task USERID for the z/OSMF Server         */
/* Note: The HOME directory will be created by the IZUMKFS      */
/* sample job.                                                  */
ADDUSER IZUSVR DFLTGRP(IZUADMIN) OMVS(AUTOUID   +
  HOME(/global/zosmf/data/home/izusvr) +
  PROGRAM(/bin/sh)) NAME('zOSMF Started Task USERID')  +
  NOPASSWORD

/* Change concurrent open file number for started task USERID    */
ALTUSER IZUSVR OMVS(FILEPROC(10000))

/* Create the z/OSMF unauthenticated USERID                     */
ADDUSER IZUGUEST RESTRICTED DFLTGRP(IZUUNGRP) OMVS(AUTOUID)   +
  NAME('zOSMF Unauthenticated USERID') NOPASSWORD

/* 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))

/* Define the APPL profile for the z/OSMF server                  */
RDEFINE APPL IZUDFLT UACC(NONE)

/* Define the SERVER profiles for the z/OSMF server               */
RDEFINE SERVER BBG.SECPFX.IZUDFLT UACC(NONE)
RDEFINE SERVER BBG.ANGEL UACC(NONE)
RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM UACC(NONE)
RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM.SAFCRED UACC(NONE)
RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM.ZOSWLM UACC(NONE)
RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM.TXRRS UACC(NONE)
RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM.ZOSDUMP UACC(NONE)

/* Permit the z/OSMF unauthenticated USERID access               */
PERMIT IZUDFLT CLASS(APPL)    ID(IZUGUEST) ACCESS(READ)

/* Permit the started task USERID access                         */
PERMIT BBG.SECPFX.IZUDFLT CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.ANGEL CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.AUTHMOD.BBGZSAFM CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.AUTHMOD.BBGZSAFM.SAFCRED CLASS(SERVER) ACCESS(READ) +
  ID(IZUSVR)
PERMIT BBG.AUTHMOD.BBGZSAFM.ZOSWLM CLASS(SERVER) ACCESS(READ) +
  ID(IZUSVR)
PERMIT BBG.AUTHMOD.BBGZSAFM.TXRRS CLASS(SERVER) ACCESS(READ) +
  ID(IZUSVR)
PERMIT BBG.AUTHMOD.BBGZSAFM.ZOSDUMP CLASS(SERVER) ACCESS(READ) +
  ID(IZUSVR)

/* Define the BPX.CONSOLE profile to supress the BPXM023I message */
/* prefix for console messages                                   */
RDEFINE FACILITY BPX.CONSOLE UACC(NONE)

/* Permit the started task USERID access                         */
PERMIT  BPX.CONSOLE CLASS(FACILITY) ID(IZUSVR) ACCESS(READ)

/* Define the Sync-to-OS-thread FACILITY profile                 */
RDEFINE FACILITY BBG.SYNC.IZUDFLT UACC(NONE)

/* Permit the started task USERID access                         */
PERMIT  BBG.SYNC.IZUDFLT CLASS(FACILITY) ID(IZUSVR) ACCESS(CONTROL)

/* Define the FACILITY class profiles for working with digital   */
/* certificates                                                  */
RDEFINE FACILITY IRR.DIGTCERT.LIST UACC(NONE)
RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE)

/* 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 started task USERID access                         */
PERMIT IRR.DIGTCERT.LIST CLASS(FACILITY) ID(IZUSVR) ACCESS(READ)
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(IZUSVR) +
  ACCESS(READ)

/* 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           */
/* 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
RACDCERT ID( IZUSVR ) CONNECT (LABEL('DefaultzOSMFCert.IZUDFLT') +
  RING(IZUKeyring.IZUDFLT) DEFAULT)
RACDCERT ID( IZUSVR ) CONNECT (LABEL('zOSMFCA') +
  RING(IZUKeyring.IZUDFLT) CERTAUTH)

/* Assumption: SERVAUTH class is active                          */
/* SETROPTS GENERIC(SERVAUTH)                                    */

/* Define the CEA resource profile required for z/OSMF server    */
RDEFINE SERVAUTH CEA.CEATSO.* UACC(NONE)

/* Define the Account Number resource profile for REST File API  */
RDEFINE ACCTNUM IZUACCT UACC(NONE)

/* Define the TSO Procedure resource profile for REST File API   */
RDEFINE TSOPROC IZUFPROC UACC(NONE)

/* List-of-groups authority checking supplements the normal RACF  */
/* access authority checking by allowing all groups of which a    */
/* user ID is a member to enter into the access list checking      */
/* process. Uncomment the following line to activate this.        */
/* SETROPTS GRPLIST                                               */

/* Create the z/OS Security Administrators group                  */
ADDGROUP IZUSECAD OMVS(AUTOGID)

/* Define the ZMFAPLA profile for the z/OSMF server               */
RDEFINE ZMFAPLA IZUDFLT.ZOSMF UACC(NONE)

/* The EJBROLE definitions are case-sensitive in RACF.  Insure you */
/* preserve case for these commands                               */
/* Assumption: EJBROLE is defined, activated, and raclisted.      */
RDEFINE EJBROLE IZUDFLT.*.izuUsers UACC(NONE)

/* Define the z/OSMF Server profile                               */
RDEFINE SERVER BBG.SECCLASS.ZMFAPLA UACC(NONE)

/* Permit the started task USERID access                          */
PERMIT BBG.SECCLASS.ZMFAPLA CLASS(SERVER) ID(IZUSVR) ACCESS(READ)

/* Roles processing will permit the z/OSMF Server groups to the   */
/* Application Server resources                                   */
/* Assumption: APPL class has been defined, activated, raclisted. */

/* Permit the Administrators group to this profile                */
PERMIT CEA.CEATSO.* CLASS(SERVAUTH) ID(IZUADMIN) ACCESS(READ)

/* Permit the Users group to this profile                         */
PERMIT CEA.CEATSO.* CLASS(SERVAUTH) ID(IZUUSER) ACCESS(READ)

/* Permit the started task USERID to this profile                 */
PERMIT CEA.CEATSO.* CLASS(SERVAUTH) ID(IZUSVR) ACCESS(READ)

/* Make changes effective                                         */
SETROPTS RACLIST(SERVAUTH) REFRESH

/* Permit the Administrators group to these profiles              */
PERMIT IZUACCT CLASS(ACCTNUM) ID(IZUADMIN) ACCESS(READ)
PERMIT IZUFPROC CLASS(TSOPROC) ID(IZUADMIN) ACCESS(READ)

/* Permit the Users group to these profiles                       */
```

```
PERMIT IZUACCT CLASS(ACCTNUM) ID(IZUUSER) ACCESS(READ)
PERMIT IZUFPROC CLASS(TSOPROC) ID(IZUUSER) ACCESS(READ)

/* Define console profile in class TSOAUTH to issue MVS commands  */
/* via EMCS consoles                                              */
RDEFINE TSOAUTH CONSOLE UACC(NONE)

/* Permit the Administrators group to these profiles              */
PERMIT CONSOLE CLASS(TSOAUTH) ID(IZUADMIN) ACCESS(READ)

/* Permit the Users group to these profiles                       */
PERMIT CONSOLE CLASS(TSOAUTH) ID(IZUUSER) ACCESS(READ)

/* Make changes effective                                         */
SETROPTS RACLIST(TSOAUTH) REFRESH

/* Define MCS operator profile starting with prefix IZU@          */
RDEFINE OPERCMDS MVS.MCSOPER.IZU@* UACC(NONE)

/* Permit the Administrators group to these profiles              */
PERMIT MVS.MCSOPER.IZU@* CLASS(OPERCMDS) ID(IZUADMIN) ACCESS(READ)

/* Permit the Users group to these profiles                       */
PERMIT MVS.MCSOPER.IZU@* CLASS(OPERCMDS) ID(IZUUSER) ACCESS(READ)

/* Make changes effective                                         */
SETROPTS RACLIST(OPERCMDS) REFRESH

/*If your installation uses hardware crypto in combination with */
/*ICSF, the use of various ICSF services might be restricted by */
/*your security policy. Some z/OSMF functions use these services.  */
/*To use those functions if their use has been restricted by    */
/*profiles in the CSFSERV class, the user ID assigned to the     */
/*z/OSMF started task will need to be granted access to those   */
/*profiles.  The commands below will permit the started task user*/
/*ID to use the necessary ICSF services.                         */
/*PERMIT CSFIQF  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)         */
/*encipher callable service                                      */
/*PERMIT CSFENC  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)         */
/*cryptographic variable encipher callable                       */
/*PERMIT CSFCVE  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)         */
/*decipher callable service                                      */
/*PERMIT CSFDEC  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)         */
/*symmetric algorithm encipher callable service                  */
/*PERMIT CSFSAE  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)         */
/*symmetric algorithm decipher callable service                  */
/*PERMIT CSFSAD  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)         */
/*one-way hash generate callable service                         */
/*PERMIT CSFOWH  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)         */
/*random number generate callable service                        */
/*PERMIT CSFRNG  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)         */
/*random number generate long callable service                   */
/*PERMIT CSFRNGL CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)         */
/*PKA key generate callable service                              */
/*PERMIT CSFPKG  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)         */
/*digital signature generate service                             */
/*PERMIT CSFDSG  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)         */
/*digital signature verify callable service                      */
/*PERMIT CSFDSV  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)         */
/*PKA key token change callable service                          */
/*PERMIT CSFPKT  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)         */
/*retained key list callable service                             */
/*PERMIT CSFRKL  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)         */
/*PKA Public Key Extract callable service                        */
/*PERMIT CSFPKX  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)         */
/*PKA encrypt callable service                                   */
/*PERMIT CSFPKE  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)         */
```

```
/*PKA decrypt callable service                                    */
/*PERMIT CSFPKD  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)           */
/*PKA key import callable service                                 */
/*PERMIT CSFPKI  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)           */
/*multiple clear key import callable service                      */
/*PERMIT CSFCKM  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)           */
/*key generate callable service                                   */
/*PERMIT CSFKGN  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)           */
/*ECC Diffie-Hellman callable service                             */
/*PERMIT CSFEDH  CLASS(CSFSERV) ACCESS(READ) ID(IZUSVR)           */
/*SETROPTS RACLIST(CSFSERV) REFRESH                               */
/*                                                               */

/*   Profile Definitions for Core                                */
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.ADMINTASKS.APPLINKING UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.ADMINTASKS.IMPORTMANAGER UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.ADMINTASKS.LINKSTASK UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.ADMINTASKS.LOGGER UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.ADMINTASKS.UI_LOG_MANAGEMENT +
  UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.ADMINTASKS.USAGESTATISTICS +
  UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.LINK.** UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SETTINGS.SYSTEMS.VIEW UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SETTINGS.SYSTEMS.MODIFY UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SETTINGS.SYSTEMS UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS.VIEW UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS.MODIFY +
  UACC(NONE)

/*   Profile Definitions for “Workflow”                          */
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.WORKFLOW.WORKFLOWS UACC(NONE)

/* Profile Definitions for “Workflow administrator role” */
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.WORKFLOW.ADMIN UACC(NONE)

/* Profile Definitions for “z/OSMF notification” */
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.NOTIFICATION.SETTINGS UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.NOTIFICATION.SETTINGS.ADMIN UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.NOTIFICATION.MODIFY UACC(NONE)

/*  End Core Setup                                               */
/*                                                               */
/*   Begin zOSMF User Role Setup                                 */
/*                                                               */
PERMIT IZUDFLT             CLASS(APPL)    ID(IZUUSER) ACCESS(READ)
PERMIT IZUDFLT.*.izuUsers  CLASS(EJBROLE) ID(IZUUSER) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF       CLASS(ZMFAPLA) ID(IZUUSER) ACCESS(READ)

/*   Permit definitions for Core                                 */
PERMIT IZUDFLT.ZOSMF.LINK.** CLASS(ZMFAPLA) ID(IZUUSER) +
  ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.SYSTEMS.VIEW CLASS(ZMFAPLA) +
  ID(IZUUSER) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.SYSTEMS CLASS(ZMFAPLA) ID(IZUUSER) +
  ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS CLASS(ZMFAPLA) +
  ID(IZUUSER) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS.VIEW CLASS(ZMFAPLA) +
  ID(IZUUSER) ACCESS(READ)

/*   Permit definitions for Workflow                             */
PERMIT IZUDFLT.ZOSMF.WORKFLOW.WORKFLOWS CLASS(ZMFAPLA) +
  ID(IZUUSER) ACCESS(READ)
/*   Permit definitions for notification                         */
```

```
PERMIT IZUDFLT.ZOSMF.NOTIFICATION.SETTINGS CLASS(ZMFAPLA) +
  ID(IZUUSER) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.NOTIFICATION.MODIFY CLASS(ZMFAPLA) +
  ID(IZUUSER) ACCESS(READ)

/*                                                              */
/*  End zOSMF User Role Setup                                   */
/*                                                              */

/*                                                              */
/*   Begin zOSMF Administrator Role Setup                       */
/*                                                              */
PERMIT IZUDFLT            CLASS(APPL)    ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF      CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)

/*   Permit definitions for Core                                */
PERMIT IZUDFLT.ZOSMF.ADMINTASKS.APPLINKING CLASS(ZMFAPLA) +
  ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.ADMINTASKS.IMPORTMANAGER   CLASS(ZMFAPLA) +
  ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.ADMINTASKS.LINKSTASK  CLASS(ZMFAPLA) +
  ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.ADMINTASKS.LOGGER   CLASS(ZMFAPLA) +
  ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.ADMINTASKS.UI_LOG_MANAGEMENT  CLASS(ZMFAPLA) +
  ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.ADMINTASKS.USAGESTATISTICS   +
  CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.LINK.** CLASS(ZMFAPLA) ID(IZUADMIN) +
  ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.SYSTEMS.VIEW CLASS(ZMFAPLA) +
  ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.SYSTEMS.MODIFY CLASS(ZMFAPLA) +
  ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.SYSTEMS CLASS(ZMFAPLA) ID(IZUADMIN) +
  ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS CLASS(ZMFAPLA) +
  ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS.VIEW CLASS(ZMFAPLA) +
  ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.SETTINGS.FTP_SERVERS.MODIFY CLASS(ZMFAPLA) +
  ID(IZUADMIN) ACCESS(READ)

/*   Permit definitions for Workflow                            */
PERMIT IZUDFLT.ZOSMF.WORKFLOW.WORKFLOWS CLASS(ZMFAPLA) +
  ID(IZUADMIN) ACCESS(READ)

/* Permit definitions for “Workflow administrator role”  */
PERMIT IZUDFLT.ZOSMF.WORKFLOW.ADMIN CLASS(ZMFAPLA) +
  ID(IZUADMIN) ACCESS(READ)
/* Permit definitions for “z/OSMF notification”  */
PERMIT IZUDFLT.ZOSMF.NOTIFICATION.SETTINGS CLASS(ZMFAPLA) +
  ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.NOTIFICATION.SETTINGS.ADMIN CLASS(ZMFAPLA) +
  ID(IZUADMIN) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF.NOTIFICATION.MODIFY CLASS(ZMFAPLA) +
  ID(IZUADMIN) ACCESS(READ)

/* 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)

/*                                                              */
/*  End zOSMF Administrator Role Setup                          */
/*                                                              */
/*                                                              */
/*   Begin zOS Security Administrator Role Setup                */
/*                                                              */

PERMIT IZUDFLT            CLASS(APPL)    ID(IZUSECAD) ACCESS(READ)
PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ID(IZUSECAD) ACCESS(READ)
PERMIT IZUDFLT.ZOSMF      CLASS(ZMFAPLA) ID(IZUSECAD) ACCESS(READ)

/*   Permit definitions for Workflow                            */
PERMIT IZUDFLT.ZOSMF.WORKFLOW.WORKFLOWS CLASS(ZMFAPLA) +
  ID(IZUSECAD) ACCESS(READ)

/*                                                              */
/*  End zOS Security Administrator Role Setup                   */
/*                                                              */

/*--------------------------------------------------------------*/
/* Begin Setup for API Discovery Swagger User Interface         */
/*--------------------------------------------------------------*/
/* The API Discovery feature lets you view z/OSMF REST APIs in  */
/* a Swagger User Interface. That feature uses the Liberty REST */
/* handler framework, which requires the following RACF resource */
/* permissions to allow all z/OSMF users to access the Swagger  */
/* User Interface.                                              */
RDEFINE EJBROLE +
 IZUDFLT.com.ibm.ws.management.security.resource.+
 allAuthenticatedUsers UACC(NONE)
PERMIT IZUDFLT.com.ibm.ws.management.security.resource.+
 allAuthenticatedUsers CLASS(EJBROLE) ID(IZUUSER) ACCESS(READ)
PERMIT IZUDFLT.com.ibm.ws.management.security.resource.+
 allAuthenticatedUsers CLASS(EJBROLE) ID(IZUADMIN) ACCESS(READ)
/*--------------------------------------------------------------*/
/* End Setup for API Discovery Swagger User Interface           */
/*--------------------------------------------------------------*/

/* Need to REFRESH these classes for Roles                      */
SETROPTS RACLIST(APPL) REFRESH
SETROPTS RACLIST(EJBROLE) REFRESH
SETROPTS RACLIST(ZMFAPLA) REFRESH
SETROPTS RACLIST(SERVER) REFRESH
SETROPTS RACLIST(STARTED) REFRESH
SETROPTS RACLIST(FACILITY) REFRESH

/* Connect the started task USERID to the CIM USER group        */
CONNECT (IZUSVR) GROUP(CFZUSRGP)

/*
//V2R3   EXEC PGM=IKJEFT01
//SYSPRINT DD SYSOUT=*
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
 /* */
 /*  The V2R3 step contains the profiles which are added in V2R3  */
 /*  release                                                     */

 /* Define the STARTED profiles for auto start function         */
 RDEFINE STARTED IZUINSTP.* UACC(NONE) STDATA(USER(IZUSVR) +
   GROUP(IZUADMIN) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))

 /* Define the CEA resource profile required for auto start     */
 /* function                                                    */
 RDEFINE SERVAUTH CEA.SIGNAL.* UACC(NONE)
```

```
/* Permit the started task USERID to this profile                */
PERMIT CEA.SIGNAL.* CLASS(SERVAUTH) ID(IZUSVR) ACCESS(READ)

/* Profile for general setting                                   */
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.GENERAL.SETTINGS UACC(NONE)

/* Permit the Administrators group to this profile               */
PERMIT IZUDFLT.ZOSMF.GENERAL.SETTINGS CLASS(ZMFAPLA) +
  ID(IZUADMIN) ACCESS(READ)

/* Profile Definitions for "z/OSMF email function" */
RDEFINE FACILITY IRR.RUSERMAP UACC(NONE)

/* Permit the started task USERID to this profile                */
PERMIT IRR.RUSERMAP CLASS(FACILITY) ID(IZUSVR) ACC(READ)

/*---------------------------------------------------------------*/
/* Begin Setup for Discovery CPC function in Systems task        */
/*---------------------------------------------------------------*/
/* Replace the <netid.nau> with the 3-17 character SNA name of   */
/* the particular CPC.                                           */
/* Replace the <uppercasecommunityname> with the SNMP community */
/* name that is associated with the CPC.                         */
/* Replace the <imagename> with the 1-8 character which          */
/* represents LPAR name.                                         */
/*                                                               */
/* RDEFINE FACILITY HWI.APPLNAME.HWISERV UACC(NONE)              */
/* PERMIT HWI.APPLNAME.HWISERV CLASS(FACILITY) ID(IZUADMIN) +    */
/*   ACCESS(READ)                                                */
/* RDEFINE FACILITY HWI.TARGET.<netid.nau> UACC(NONE) +          */
/*   APPLDATA('<uppercasecommunityname>')                        */
/* RDEFINE FACILITY HWI.TARGET.<netid.nau>.<imagename> UACC(NONE)  */
/* PERMIT HWI.TARGET.<netid.nau> CLASS(FACILITY) ID(IZUADMIN) + */
/*   ACCESS(READ)                                                */
/* PERMIT HWI.TARGET.<netid.nau>.<imagename> CLASS(FACILITY) +   */
/*   ID(IZUADMIN) ACCESS(READ)                                   */
/*---------------------------------------------------------------*/
/* End Setup for Discovery CPC function in Systems task          */
/*---------------------------------------------------------------*/

/* If AT_TLS is enabled, the z/OSMF started task userid needs to   */
/* be permitted on resource EZB.INITSTACK.sysname.tcpname        */
/*                                                               */
/* PERMIT EZB.INITSTACK.sysname.tcpname CLASS(SERVAUTH)  +       */
/*   ID(IZUSVR) ACCESS(READ)                                     */

/* Profile Definitions for "zOS Operator Consoles" task */
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.CONSOLES.ZOSOPER UACC(NONE)
/* Permit definitions for "zOS Operator Consoles" task */
PERMIT IZUDFLT.ZOSMF.CONSOLES.ZOSOPER CLASS(ZMFAPLA) +
  ID(IZUUSER) ACCESS(READ)
/* Permit definitions for "zOS Operator Consoles" task */
PERMIT IZUDFLT.ZOSMF.CONSOLES.ZOSOPER CLASS(ZMFAPLA) +
  ID(IZUADMIN) ACCESS(READ)

/* Profile definitions for Named Angel Support                   */
RDEFINE SERVER BBG.ANGEL.IZUANG1 UACC(NONE)
PERMIT BBG.ANGEL.IZUANG1 CLASS(SERVER) ID(IZUSVR) ACCESS(READ)

/* Define security setup to permit Authorized WLM Service(ZOSWLM )  */
RDEFINE FACILITY BPX.WLMSERVER UACC(NONE)

/* Profile for TSO RESTful API remote support */
RDEFINE SERVAUTH CEA.CEATSO.FLOW.* UACC(NONE)
PERMIT CEA.CEATSO.FLOW.* CLASS(SERVAUTH) ID(IZUSVR) ACCESS(READ)
PERMIT CEA.CEATSO.FLOW.* CLASS(SERVAUTH) ID(IZUADMIN) ACCESS(READ)
PERMIT CEA.CEATSO.FLOW.* CLASS(SERVAUTH) ID(IZUUSER) ACCESS(READ)
```

```
/* Make changes effective                                          */
SETROPTS RACLIST(SERVER) REFRESH
SETROPTS RACLIST(SERVAUTH) REFRESH
SETROPTS RACLIST(ZMFAPLA) REFRESH
SETROPTS RACLIST(FACILITY) REFRESH
/*                                                                 */
/*  End V2R3 step Setup                                            */
/*                                                                 */
```