Auditing Essentials

VOLUME
3.1

SECURING z/OSMF

Updates Specific to

z/OS 2.4

Julie Bergh – J & S Consulting, LLC.

09/25/2020

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.

Table of Contents

1 Recommendations

As was mentioned in the original z/OSMF document, these are all still valid \ comments for z/OSMF 2.4

Some recommendations are as follows:

- RACF commands provided **do not** always include fields like OWNER and
  - 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.
  - If some of the 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.
- 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.
- 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.
- 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.
- The CSFCERV class does not deny access by default. If you define the profiles listed, other areas may not work. Be cautious on what id defined and granted in the areas.

2 Security Settings z/OSMF 2.4

What it is and What it isn't

This document discusses the security settings / changes of z/OSMF from a z/OS 2.4 perspective.

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 to get z/OSMF up and running securely in your organization.

In z/OS 2.3 some of the key terms that described z/OSMF were:

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.

With z/OS 2.4, some new terms to describe functions were added. They are:

Nucleus - This is really for the first-time setup of z/OSMF. It is what is called the z/OSMF Lite. If you have z/OSMF already active in your system, this is not needed. This 'nucleus' includes only the following functions, which are enabled when the z/OSMF server is started.

- WebSphere Liberty profile runtime
- z/OSMF desktop user interface (UI)
- z/OSMF online help system.

Core Service – This relates to the core functions that are described above.

Optional Service – This relates to the Plug-ins in z/OS 2.3.

Advanced Configuration – This includes such areas as the autostart, ICSF setup, AT-TLS. Some of which was included in other areas of z/OS 2.3.

In the z/OSMF 2.4 Configuration manual, there is detail describing the above functions and where they are applicable. This document will not recreate that information here. For example, it mentions that the TSO/E address space services is considered a core service and provides the sample JCL is in SYS1.SAMPLIB(IZUTSSEC) for configuration of it. It then describes if there are any dependencies on those services you may want to install. For example, going back to the TSO/E address space, it mentions this should be a relatively easy to implement and will describe any dependencies. TSO/E address space is considered low complexity to implement. It has requirements of having the CEA (Common Event Adapter) address space active. Another example of a dependency is Sysplex Management. It requires the following to set up successfully; CEA, z/OSMF settings, z/OS dataset and file REST services, TSO/E address space, and console services. This make it a lot easier to determine the level of effort that is required to set up these optional services.

It is discussed the set up with IZUPRMxx member in PARMLIB. There is also showing a MVS modify command to display the active parameters. The command is F IZUSVR1,DISPLAY IZU. This command is also available in z/OS 2.3.

3 Getting Started with Securing z/OSMF

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.

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.

4 SYS1.SAMPLIB IZUxxxxx Members

SYS1.SAMPLIB member that contain RACF commands.

JOBNAME	z/OS 2.3	Approximate number of RACF commands	z/OS 2.4	Approximate number of RACF commands	DESCRIPTION
IZUASSEC			**YES**	**4**	**Use the autostart capability**
IZUATSEC			**YES**	**36**	**Administrator tasks and web site links**
IZUAUTH	Yes	5	YES	5	Connects
IZUCASEC	Yes	4	YES	4	Configuration Assistant
IZUCPSEC	Yes	10	YES	10	Capacity Provisioning
IZUDCSEC			**YES**	**7**	**Discover CPC function**
IZUDMSEC	Yes	13	YES	15	Software Management
IZUGCSEC	Yes	22	YES	17	Consoles
IZUICSEC			**YES**	**23**	**ICSF**
IZUILSEC	Yes	21	YES	21	Incident Log -
IZUISSEC	Yes	4	YES	4	ISPF
IZUNASEC	Yes		YES	12	zERT
IZUNFSEC			**YES**	**13**	**Notifications**
IZUNUSEC			**YES**	**60**	**Nucleus basic**
IZUPRSEC	Yes	30	YES	42	IBM Cloud Provisioning
IZURFSEC			**YES**	**15**	**Dataset and files REST services**
IZURJSEC			**YES**	**1**	**jobs REST services**
IZURMSEC	Yes	1	YES	1	Resource Monitoring
IZUSASEC			**YES**	**39**	**Security Configuration Assistant**
IZUSEC	Yes	170	YES	195	z/OSMF nucleus and core
IZUSKSEC			**YES**	**8**	**Cert and keyring**
IZUSPSEC	Yes	20	YES	15	Sysplex Management
IZUSTSEC			**YES**	**21**	**Settings Services**
IZUSWSEC			**YES**	**7**	**Swagger Service**
IZUTLSEC			**YES**	**2**	**AT-TLS security**
IZUTSSEC			**YES**	**9**	**TSO/E address space service**
IZUWFSEC			**YES**	**8**	**Workflows**
IZUWMSEC	Yes	13	YES	11	Workload Management

5 Sample Jobs in SYS1.SAMPLIB

These are the Sample Jobs provided in SYS1.SAMPLIB and a description of their purpose. It also talks to which ones are z/OS 2.3 and z/OS 2.4

JOBNAME	z/OS 2.3	z/OS 2.4	DESCRIPTION
IZUASSEC		**YES**	**Security Setup for z/OSMF AUTOSTART function**
IZUATSEC		**YES**	**Security setup for z/OSMF Administrator tasks and web site links Some of this was in IZUSEC in z/OS 2.3. Links definitions are new for this release.**
IZUAUTH	Yes	YES	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	Yes	YES	Configuration Assistant - plug-in. z/OS 2.4 version contains more specific profiles and has comments for cloud provisioning.
IZUCPSEC	Yes	YES	Capacity Provisioning - plug-in. Members appear to be basically the same.
IZUDCSEC		**YES**	**This sample JCL intends to help with security setup required per user of Discover CPC function**
IZUDELFN	Yes	YES	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	Yes	YES	Software Management - plug-in. Basically, the same commands between releases
IZUDWFVR	Yes	YES	Software Management Workflow definition sample - plug-in
IZUDXEXP	Yes	YES	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	Yes	YES	The job contains RACF commands for creating the required security authorizations for the z/OS Operator Consoles task. – plug-in Basically the same commands between releases

JOBNAME	z/OS 2.3	z/OS 2.4	DESCRIPTION
IZUILSEC	Yes	YES	Incident Log - plug-in Basically, the same commands between releases
IZUISALC	Yes	YES	Allocates target and distribution libraries for z/OSMF.
IZUISDDD	Yes	YES	Creates DDDEF entries for z/OSMF.
IZUISHFS	Yes	YES	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. No longer there with z/os 2.4
IZUISMKD	Yes	YES	Executes the IZUMKDIR exec for z/OSMF.
IZUISSEC	Yes	YES	ISPF - plug-in Basically, the same commands between releases
IZUISZFS	Yes		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. **Member not there in z/OS 2.4**
IZUMKDIR	Yes	YES	This REXX exec will create the necessary directories for z/OSMF.
IZUMKFS	Yes	YES	Initializes the z/OSMF user file system, which contains configuration settings and persistence information for z/OSMF.
IZUMNTFS	Yes	YES	This REXX EXEC will create product mount point and will mount the product HFS or ZFS data set at the newly created mountpoint.
IZUNASEC	Yes	YES	IBM z/OS Encryption Readiness Technology (zERT) Network Analyzer. – plug-in Basically, the same commands between releases
IZUNFSEC		**YES**	**Security setup for z/OSMF Notifications. Most of this was in IZUSEC in z/OS 2.3**
IZUNUSEC		**YES**	**Security setup for z/OSMF Nucleus basic**
IZUPRM00	Yes	YES	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	Yes	YES	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
IZURFSEC		**YES**	**Security Setup for z/OS data set and file REST interface Most of this was in IZUSEC in z/OS 2.3**
IZURJSEC		**YES**	**Security Setup for z/OS Jobs REST interface**

JOBNAME	z/OS 2.3	z/OS 2.4	DESCRIPTION
IZURMSEC	Yes	YES	Resource Monitoring - plug-in Basically, the same commands between releases
IZUSASEC		**YES**	**Security Setup for z/OSMF Security Configuration Assistant**
IZUSEC	Yes	YES	Establishes security for z/OSMF by creating SAF-based authorizations. Contains RACF commands for creating the security definitions.
IZUSKSEC		**YES**	**Setup shared key ring and certificate for the z/OSMF server. These commands were in IZUSEC in z/OS 2.3**
IZUSPSEC	Yes	YES	Contains RACF commands for creating the required security authorizations for the Sysplex Management task. – **plug-in** Basically, the same commands between releases
IZUSTSEC		**YES**	**This sample JCL intends to help with security setup required per user of z/OSMF settings**
IZUSVR2	Yes	YES	This procedure can be used for starting the z/OSMF server manually.
IZUSWSEC		**YES**	**This sample JCL intends to help with security setup required for z/OSMF Support Swagger Document Profile for Liberty API Discovery support**
IZUTLSEC		**YES**	**Setup AT-TLS security for z/OSMF server**
IZUTSSEC		**YES**	**This sample JCL intends to help with security setup required per user of z/OSMF TSO/E address space service. These commands were in IZUSEC in z/OS 2.3**
IZUWFSEC		**YES**	**z/OSMF work flows These commands were in IZUSEC in z/OS 2.3**
IZUWMSEC	Yes	YES	Workload Management - plug-in
IZUZUNDAG	Yes	YES	REXX exec to create a customizes set of DDL directives for a set of zERT Network Analyzer database objects.
IZUDZNADI	Yes	YES	REXX exec for zERT Network Analyzer
IZUZNADT	yes	YES	zERT Network Analyzer

Prepared for publication by The z Exchange – https://zexchange.info

Other eBooks can be downloaded free of charge at www.newera-info.com/eBooks.html

Titles include:

What's New in z/OS V2R1
What's New in z/OS V2R2
What's New in z/O V2R3
What's new in z/OS V2R4

AE1 – zAuditing Essentials – Volume 1 – zEnterprise Hardware

AE2 – zAuditing Essentials – Volume 2 – Taming RACF - SETROPTS
AE2 – zAuditing Essentials – Volume 2 – Mastering CA ACF2 - GSO
AE2 – zAuditing Essentials – Volume 2 – Controlling CA Top Secret

AE3 – Securing z/OSMF
AE3.1 – Securing z/OSMF – Updated for z/OSMF 2.4

AE4 – Are Your Ports Safe?

NewEra Software, Inc.
www.newera.com