

# z/OSMF Security Setup Overview V2R4

1

JULIE BERGH  
SEPTEMBER 2020

# Abstract

- ▶ In August, Julie presented and demoed z/OSMF on a z/OS 2.4. She briefly talked about some of the changes in security in this release. The primary focus in the August call was on the security assistant. This session will provide more detail on the setup for z/OSMF security from user experiences



# NewEra – Link to eBook

3



<https://www.newera-info.com/eBooks.html>

**AE3 - Securing z/OSMF** - 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. 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.

[AE3 - Securing z/OSMF](#)

# z/OSMF Components – Classic Interface



IBM z/OS Management Facility

[LEARN MORE](#) [NEED HELP?](#)

## Welcome to z/OS

The highly secure, scalable and resilient enterprise operating system for the IBM z Systems mainframe.

**z/OS USER ID**

**z/OS PASSWORD**

**LOG IN**

# z/OSMF Components – Classic Interface

IBM z/OS Management Facility

Welcome adcdmst

- Welcome
- Notifications
- Workflow Editor
- Workflows
- Cloud Provisioning
- Configuration
- Consoles
- Jobs and Resources
- Links
- Performance
- Problem Determination
- Software
- Sysplex
- z/OS Classic Interfaces
- z/OSMF Administration
- z/OSMF Settings
- z/OSMF Diagnostic Assistant

Refresh

## Welcome to IBM z/OS Management Facility

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

To learn more about z/OSMF, visit the links in the Learn More section.

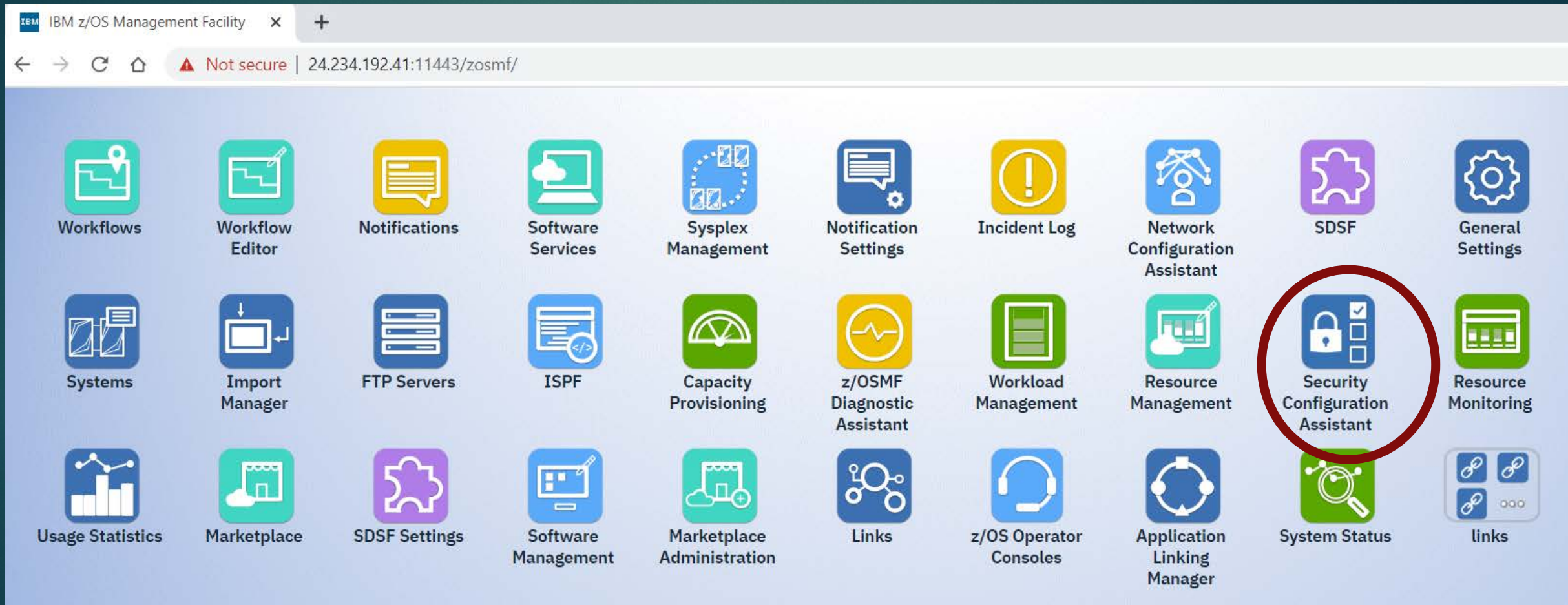
To start managing your z/OS systems, select a task from the navigation area.

### Learn More:

- [What's New](#)
- [z/OSMF tasks at a glance](#)
- [Getting started with z/OSMF](#)



# z/OSMF Components – Desktop Interface



# z/OSMF – From a Security Perspective

## z/OSMF - Security:

- z/OSMF uses your **Enterprise Security Management** (e.g., RACF, CA ACF2, CA Top Secret) product for **user authentication and authorization**.
- The z/OSMF SAF-based authorization support brings tighter integration with z/OS SAF-based authorization with the introduction of the resource class ZMFAPLA for z/OSMF task-based resources.
- All z/OSMF tasks and links are associated with resource names and resource class profiles under this resource class, and SAF groups are used to represent Roles.
- SAF-based authorization also allows for custom roles via creation of SAF groups at your discretion.



# z/OSMF Lite configuration

- What's "z/OSMF Lite configuration"
- "z/OSMF Lite configuration" provides a new approach of z/OSMF configuration which allows user to bring up a minimum z/OSMF as quick as possible and then configure only for z/OSMF services that user require.
- To achieve the goal, z/OSMF Configuration Guide and security sample jobs are both restructured
  - A minimum z/OSMF is defined and referred as z/OSMF nucleus.
    - IZUNUSEC sample job is provided for security configuration of z/OSMF nucleus.
    - Typically, the z/OSMF nucleus can be setup and bring up in 90 minutes\*.
  - About 20 z/OSMF services are identified and can be added on top of z/OSMF nucleus per user's need.
    - Setup complexity of each z/OSMF service is provided to help you determine which service to setup first.
    - Dependency list is clearly documented in each z/OSMF service's chapter
    - Configuration required by z/OSMF REST services are also documented in the same structure with plugins in z/OSMF Configuration Guide.
  - Advanced configuration are consolidated in the later chapter so that user can focus on common configuration and bring z/OSMF up quickly.



# z/OSMF Terms Previous Release

- ▶ 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.



# z/OSMF Terms Previous Release

- ▶ 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.



# z/OSMF Terms

- ▶ Nucleus – first time user and using IZUNUSEC – minimal configuration
- ▶ Core Service – workflow tasks, REST API
- ▶ Optional Service – Plug-ins
- ▶ Advanced Configuration – autostart, Links, ICSF

# z/OSMF Lite configuration

- What's “z/OSMF Lite configuration”

## Previous z/OSMF configuration

z/OSMF Core	z/OSMF Optional Services
Liberty Profile	Capacity Provisioning
Core Navigation	Network Configuration Assistant
Online Help	Incident Log
Notification	ISPF
Notification settings	Resource Monitoring
App linking	Software Management
Import Manager	Sysplex Management
Links	Workload Management
FTP Servers	zERT
Usage Statistics	Cloud Provisioning
Systems	z/OS Operator Consoles
Workflow Editor	
API Discovery Swagger	
REST Job API	
REST File API	
REST TSO API	
Workflows	



## z/OSMF Lite configuration

z/OSMF Nucleus	z/OSMF Core Services	z/OSMF Optional Services
Liberty Profile	Notification	Capacity Provisioning
Core Navigation	Settings	Network Configuration Assistant
Online Help	Administration Tasks	Incident Log
	Workflow Editor	ISPF
	Swagger support for REST APIs	Resource Monitoring
	REST Job API	Software Management
	REST File API	Sysplex Management
	REST TSO API	Workload Management
	Workflows	zERT
		Cloud Provisioning
		z/OS Operator Consoles



# z/OSMF

- ▶ IZUNUSEC - represents the authorizations that are needed to set up z/OSMF in a minimal configuration called the *nucleus*.
- ▶ IZUSEC - represents the authorizations that are needed to set up z/OSMF in a full configuration: Nucleus, plus the core services.
- ▶ IZUxxSEC - jobs is associated with a particular z/OSMF service or an advanced configuration setup.
- ▶ To create user authorizations for the services, your security administrator can use the IZUAUTH job in SYS1.SAMPLIB

# z/OSMF

- ▶ ADDGROUP IZUADMIN OMVS(AUTOGID) - Security group to be used for the z/OSMF administrator role. The user IDs that are connected to this group are considered to be z/OSMF administrators
- ▶ ADDGROUP IZUUSER OMVS(AUTOGID) - Security group to be used for the z/OSMF user role. The user IDs that are connected to this group are considered to be z/OSMF users.
- ▶ ADDGROUP IZUUNGRP OMVS(AUTOGID) – undefined users
- ▶ ADDGROUP IZUSECAD OMVS(AUTOGID) - Group name to be used for the z/OS Security Administrator role. This group is permitted to the Workflows task. Job IZUAUTH. Basically CONNECT commands to connect to other groups.



# IZUNUSEC

```
ADDGROUP IZUADMIN OMVS(AUTOGID)
ADDGROUP IZUUSER OMVS(AUTOGID)
ADDGROUP IZUUNGRP OMVS(AUTOGID)
ADDGROUP IZUSECAD OMVS(AUTOGID)

ADDUSER IZUSVR DFLTGRP(IZUADMIN) NOPASSWORD OMVS(AUTOUID) +
  HOME(/global/zosmf/data/home/izusvr) +
  PROGRAM(/bin/sh)) NAME('zOSMF Started Task USERID')

ALTUSER IZUSVR OMVS(FILEPROC(10000))
CONNECT IZUSVR GROUP(IZUSECAD)

ADDUSER IZUGUEST RESTRICTED DFLTGRP(IZUUNGRP) OMVS(AUTOUID) +
  NAME('zOSMF Unauthenticated USERID') NOPASSWORD
```

# IZUNUSEC

```
RDEFINE SERVER BBG.ANGEL.IZUANG1 UACC(NONE)
PERMIT BBG.ANGEL.IZUANG1 CLASS(SERVER) ACCESS(READ) ID(IZUSVR)

RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM CLASS(SERVER) ACCESS(READ) ID(IZUSVR)

RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM.SAFCRED UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM.SAFCRED CLASS(SERVER) ACCESS(READ) +
  ID(IZUSVR)

RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM.ZOSWLM UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM.ZOSWLM CLASS(SERVER) ACCESS(READ) ID(IZUSVR)

RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM.TXRRS UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM.TXRRS CLASS(SERVER) ACCESS(READ) ID(IZUSVR)

RDEFINE SERVER BBG.AUTHMOD.BBGZSAFM.ZOSDUMP UACC(NONE)
PERMIT BBG.AUTHMOD.BBGZSAFM.ZOSDUMP CLASS(SERVER) ACCESS(READ) +
  ID(IZUSVR)

RDEFINE SERVER BBG.SECPFIX.IZUDFLT UACC(NONE)
PERMIT BBG.SECPFIX.IZUDFLT CLASS(SERVER) ACCESS(READ) ID(IZUSVR)

RDEFINE SERVER BBG.SECCLASS.ZMFAPLA UACC(NONE)
PERMIT BBG.SECCLASS.ZMFAPLA CLASS(SERVER) ID(IZUSVR) ACCESS(READ)

SETROPTS RACLIST(SERVER) REFRESH
```



# IZUNUSEC

```
RDEFINE FACILITY BBG.SYNC.IZUDFLT UACC(NONE)
PERMIT BBG.SYNC.IZUDFLT CLASS(FACILITY) ID(IZUSVR) ACCESS(CONTROL)

/* RDEFINE FACILITY BPX.WLMSEVER UACC(NONE) */
PERMIT BPX.WLMSEVER CLASS(FACILITY) ID(IZUSVR) ACCESS(READ)
/* RDEFINE FACILITY BPX.CONSOLE UACC(NONE) */
PERMIT BPX.CONSOLE CLASS(FACILITY) ID(IZUSVR) ACCESS(READ)
SETROPTS RACLIST(FACILITY) REFRESH

RDEFINE APPL IZUDFLT UACC(NONE)
PERMIT IZUDFLT CLASS(APPL) ACCESS(READ) ID(IZUADMIN IZUUSER IZUGUEST)
SETROPTS RACLIST(APPL) REFRESH

RDEFINE EJBROLE IZUDFLT.*.izuUsers UACC(NONE)
PERMIT IZUDFLT.*.izuUsers CLASS(EJBROLE) ACCESS(READ) +
ID(IZUADMIN IZUUSER)
SETROPTS RACLIST(EJBROLE) REFRESH

/* By default, no users are allowed to perform z/OSMF tasks. Users */
/* will only have access to z/OSMF tasks if it's specified explicitly.*/
RDEFINE ZMFAPLA IZUDFLT.** UACC(NONE)
RDEFINE ZMFAPLA IZUDFLT.ZOSMF UACC(NONE)
PERMIT IZUDFLT.ZOSMF CLASS(ZMFAPLA) ACCESS(READ) ID(IZUADMIN IZUUSER)
SETROPTS RACLIST(ZMFAPLA) REFRESH

/* RDEFINE SERVAUTH CEA.SIGNAL.ENF83 UACC(NONE) */
PERMIT CEA.SIGNAL.ENF83 CLASS(SERVAUTH) ID(IZUSVR) ACCESS(READ)
SETROPTS RACLIST(SERVAUTH ) REFRESH
```



# IZUNUSEC

```
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))  
SETROPTS RACLIST(STARTED) REFRESH  
@@
```



# RC = 0

```
-
-STEPNAME PROCSTEP      RC      EXCP      CONN      -----TIMINGS (MINS.)-----
-          TCB          SRB      CLOCK
-BASIC01      00      791      0      .01      .00      .0
ICH408I USER(ADCDMST ) GROUP(SYS1      ) NAME(ADCD MASTER      )
  IZUSVR1.* CL(STARTED )
  DEFINE - RESOURCE ALREADY DEFINED
ICH408I USER(ADCDMST ) GROUP(SYS1      ) NAME(ADCD MASTER      )
  IZUANG1.* CL(STARTED )
  DEFINE - RESOURCE ALREADY DEFINED
-STCPROFS      00      113      0      .00      .00      .0
IEF404I ADCDMST1 - ENDED - TIME=09.04.02
-ADCDMST1 ENDED.  NAME-      TOTAL TCB CPU TIME=
$HASP395 ADCDMST1 ENDED - RC=0000
STATISTICS -----
EXECUTION DATE
```

IKJ56702I INVALID GROUP, IZUSECAD

READY

READY

ADDUSER IZUSVR DFLTGRP(IZUADMIN) NOPASSWORD OMVS(AUTOUID HOME(/global/zosmf/d  
d Task USERID')

IKJ56702I INVALID USERID, IZUSVR

IKJ56701I MISSING HOME DIRECTORY+

IKJ56701I MISSING OMVS USER'S INITIAL WORKING DIRECTORY

READY

# z/OSMF

z/OSMF area to be configured	Description <ul style="list-style-type: none"><li>• Nucleus</li><li>• Core service</li><li>• Optional service</li><li>• Advanced configuration</li></ul>	Security job in SYS1.SAMPLIB
Nucleus	Nucleus	IZUNUSEC
Notifications task	Core service	IZUNFSEC
z/OS data set and file REST services	Core service	IZURFSEC
z/OS jobs REST services	Core service	IZURJSEC
Swagger service	Core service	IZUSWSEC
TSO/E address space services	Core service	IZUTSSEC
z/OSMF administrative tasks	Core service	IZUATSEC
z/OSMF settings service	Core service	IZUSTSEC
z/OSMF Workflows task	Core service	IZUWFSEC
All of the above	Nucleus, plus all core services	IZUSEC



# z/OSMF

- Some z/OSMF services require other z/OSMF services to be enabled. Therefore, you might need to configure more services than just the ones you plan to use.

To use this z/OSMF service...	... Configure these required services	You might also need to configure these optional services, depending on your intended use.
<b>Cloud Provisioning</b>	<ul style="list-style-type: none"><li>• Console services (UI and API)</li><li>• Network Configuration Assistant</li><li>• Notifications</li><li>• Swagger (API Discovery)</li><li>• z/OSMF Settings</li><li>• z/OSMF Workflows</li></ul>	<ul style="list-style-type: none"><li>• Common Information Model (CIM) server, which is used by Resource Monitoring and Workload Management.</li><li>• z/OS data set and file REST services because these services are used by z/OSMF Workflows.</li><li>• TSO/E address space services because these services are used by the console services.</li><li>• Resource Monitoring because it is used by Cloud Provisioning to obtain CPU and memory metering data.</li><li>• Workload Management because it is used by Cloud Provisioning to set CPU and memory capping.</li></ul>
<b>Console services</b>	<ul style="list-style-type: none"><li>• Common event adapter (CEA)</li><li>• TSO/E address space services</li><li>• z/OSMF Settings</li></ul>	<ul style="list-style-type: none"><li>• None.</li></ul>
<b>Incident Log</b>	<ul style="list-style-type: none"><li>• Common event adapter (CEA)</li><li>• z/OSMF Settings</li><li>• Common Information Model (CIM) server</li></ul>	<ul style="list-style-type: none"><li>• None.</li></ul>

# IZUPRMxx

```
HOSTNAME('s0wl.dal-ebis.ihost.com')
HTTP_SSL_PORT(10443)
INCIDENT_LOG UNIT('SYSALLDA')
JAVA_HOME('/usr/lpp/java/J8.0_64')
KEYRING_NAME('IZUKeyring.IZUDFLT')
LOGGING('*=warning:com.ibm.zosmf.*=info:com.ibm.zosmf.environment.ui=
finer')
RESTAPI_FILE ACCT(IZUACCT) REGION(32768) PROC(IZUFPROC)
COMMON_TSO ACCT(IZUACCT) REGION(50000) PROC(IZUFPROC)
SAF_PREFIX('IZUDFLT')
CLOUD_SAF_PREFIX('IYU')
SEC_GROUPS USER(IZUUSER),ADMIN(IZUADMIN),SECADMIN(IZUSECAD)
SESSION_EXPIRE(495)
TEMP_DIR('/tmp')
CSRF_SWITCH(ON)
SERVER_PROC('IZUSVR1')
ANGEL_PROC('IZUANG1')
AUTOSTART('LOCAL')
```



# IZUPRMxx

```
Command ==> _SCROLL ==> CSR
/* AUTOSTART_GROUP('IZUDFLT') */
/* AUTOSTART_GROUP('NONE') */
USER_DIR('/var/zosmf')
UNAUTH_USER(IZUGUEST)
/* WLM_CLASSES DEFAULT(IZUGHTTP)
   LONG_WORK(IZUGWORK) */
CSRF_SWITCH(OFF)

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

# F IZUSVR1,DISPLAY IZU

```
F IZUSVR1,DISPLAY IZU
+CWWKBO004I: z/OSMF PARMLIBs DISPLAY 397
  IZUG013I The home page of z/OSMF server in SYSTEM(SOW1)
  in AUTOSTART_GROUP(IZUDEFLT) can be accessed at :
  https://SOW1.DAL-EBIS.IHOST.COM:11443/zosmf
  IZUG014I The server started at 08/20/2020 12:30:36
  and has been running for 0004(hhhh):761(mm):02(ss)

Current z/OSMF settings
```

	Source
HOSTNAME(SOW1.DAL-EBIS.IHOST.COM)	IZUPRMAS
+CWWKBO0061I CONTINUATION 1 FOR MESSAGE IDENTIFIER 14397	398
HTTP_SSL_PORT(11443)	IZUPRMAS
LOGGING('*=warning:com.ibm.zoszmf.*=info:com.ibm.zoszm	
f.environment.ui=finer')	IZUPRMAS
UNAUTH_USER(IZUGUEST)	IZUPRMAS
SEC_GROUPS	
ADMIN(IZUADMIN)	IZUPRMAS
USER(IZUUSER)	IZUPRMAS
SECADMIN(IZUSECAD)	IZUPRMAS
SAF_PREFIX(IZUDEFLT)	IZUPRMAS
+CWWKBO0061I CONTINUATION 2 FOR MESSAGE IDENTIFIER 14397	399
CLOUD_SAF_PREFIX(IYU)	IZUPRMAS
KEYRING_NAME(IZUKeyring.IZUDEFLT)	IZUPRMAS
SESSION_EXPIRE(495)	IZUPRMAS
WLM_CLASSES	
LONG_WORK(IZUGWORK)	DEFAULT
DEFAULT(IZUGHTTP)	DEFAULT
JAVA_HOME(/usr/lpp/java/J8.0_64)	IZUPRMAS
TEMP_DIR(/tmp)	IZUPRMAS
INCIDENT_LOG_UNIT(SYSALLDA)	IZUPRMAS



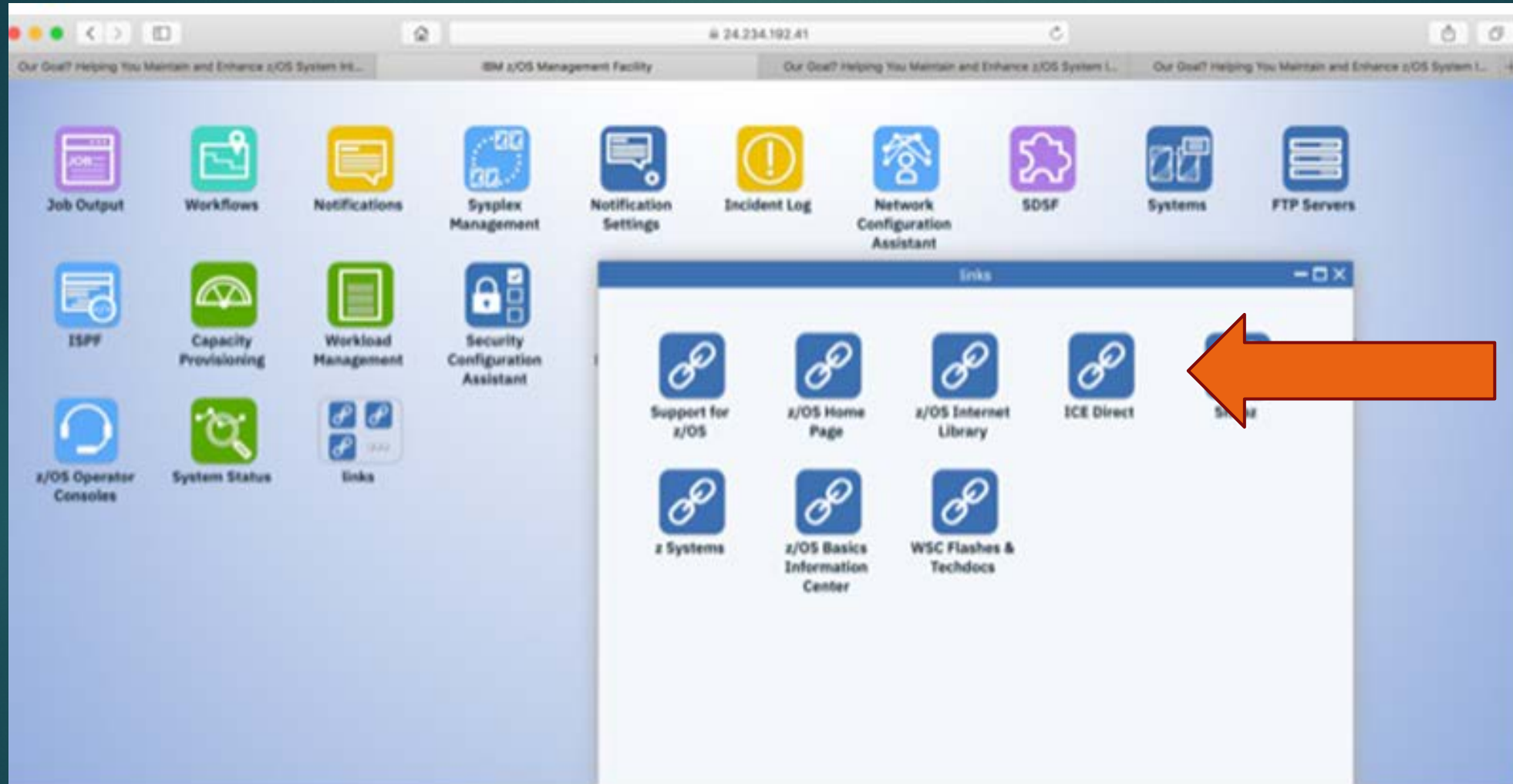
# F IZUSVR1,DISPLAY IZU

```
+CWWKBO061I CONTINUATION 3 FOR MESSAGE IDENTIFIER 14397 400
  RESTAPI_FILE
    ACCT(IZUACCT) IZUPRMAS
    PROC(IZUFFPROC) IZUPRMAS
    REGION(65536) IZUPRMAS
  COMMON_TSO
    ACCT(IZUACCT) IZUPRMAS
    PROC(IZUFFPROC) IZUPRMAS
    REGION(65536) IZUPRMAS
  AUTOSTART_GROUP(IZUDFLT) DEFAULT
+CWWKBO061I CONTINUATION 4 FOR MESSAGE IDENTIFIER 14397 401
  AUTOSTART(LOCAL) IZUPRMAS
  SERVER_PROC(IZUSVR1) IZUPRMAS
  ANGEL_PROC(IZUANG1) IZUPRMAS
  USER_DIR(/var/zosmf) IZUPRMAS
  CSRF_SWITCH(OFF) IZUPRMAS

  Status of z/OSMF plugins

  Configuration Assistant(STARTED) IZUPRMAS
+CWWKBO061I CONTINUATION 5 FOR MESSAGE IDENTIFIER 14397 402
  Capacity Provisioning(STARTED) IZUPRMAS
  Workload Management(STARTED) IZUPRMAS
  Resource Monitoring(STARTED) IZUPRMAS
  Incident Log(STARTED) IZUPRMAS
  Software Management(STARTED) IZUPRMAS
  WebISPF(STARTED) IZUPRMAS
  ZERT(UNSPECIFIED) DEFAULT
  Sysplex Management(STARTED) IZUPRMAS
+CWWKBO005I: COMMAND RESPONSES COMPLETED SUCCESSFULLY FROM display 403
  izu|d izu Command Handler.
+CWWKBO002I: MODIFY COMMAND DISPLAY IZU COMPLETED SUCCESSFULLY.
```

# Links





# NEW Security Configuration Assistant task

- What's Security Configuration Assistant

Security Configuration Assistant task is built for simplifying the user experience of security configuration and validation. It starts with help z/OSMF security configuration by providing

- Automatic validation of security configuration by user
  - Graphic views for validation result
  - Filter by validation result, service enablement status, etc.
  - Description for each security requirement
  - Support both RACF and non-RACF security products
- Security Configuration Assistant can be used in the following scenarios
    - Security planning for z/OSMF
    - Validation of z/OSMF security configuration
    - Trouble shooting for function failures

# Security Configuration Assistant task

- Security Configuration Assistant – Graphic view to display automatic validation result

Validation is done per user

- Validation can be done against
- All z/OSMF security configuration
  - Selected services
  - One specific security requirement

Description is included for each security requirement

Security Configuration Assistant


Validate for user ID: debug1 Validate all

Security Configuration Assistant | Nucleus | Services 31 | Advanced Configuration 24

Align with z/OSMF Lite configuration

Show enabled services only

Passed Failed Unknown



z/OSMF Sysplex Management

z/OSMF Settings

z/OSMF Notifications

Automated

Resources for z/OSMF Notifications	Description	Class	Who needs the access	Required Access	Validated User ID	Validation Result	Action
IZUP03SF.ZOSMF.NOTIFICATION.SETTINGS	Allows the user to view the Notification Settings task.	ZMFAPLA	IZUUSER IZUADMIN	READ	debug1	Passed	
IZUP03SF.ZOSMF.NOTIFICATION.SETTINGS.ADMIN	Allows the user to modify the notification settings.	ZMFAPLA	IZUADMIN	READ	debug1	Passed	
IZUP03SF.ZOSMF.NOTIFICATION.MODIFY	Allows the user to send a notification.	ZMFAPLA	IZUUSER IZUADMIN	READ	debug1	Passed	
IRR.RUSERMAP	Allows notification settings task to get the user's email address configured to RACF.	FACILITY	IZUUSER IZUADMIN	READ	debug1	Failed	



# NEW Security Configuration Assistant task

- Security Configuration Assistant – Manual checks

The screenshot displays the Security Configuration Assistant interface. At the top, there's a header with the title "Security Configuration Assistant" and a "debug1" status. Below the header, there's a "Validate for user ID" field with "debug1" entered and a "Validate all" button. To the right, there's a "Filters" button. Below this, there are tabs for "Security Configuration Assistant", "Nucleus", "Services 31", and "Advanced Configuration 24". A "Show enabled services only" checkbox is also present.

The main content area shows a list of services. The "z/OSMF Administration" service is expanded, showing "Passed 6", "Automated Checks Failed 0", "Unknown 0", and "Manual Checks 0". Below it, the "TSO/E Address Space Services" service is expanded, showing "Passed 2", "Automated Checks Failed 0", "Unknown 0", and "Manual Checks 3".

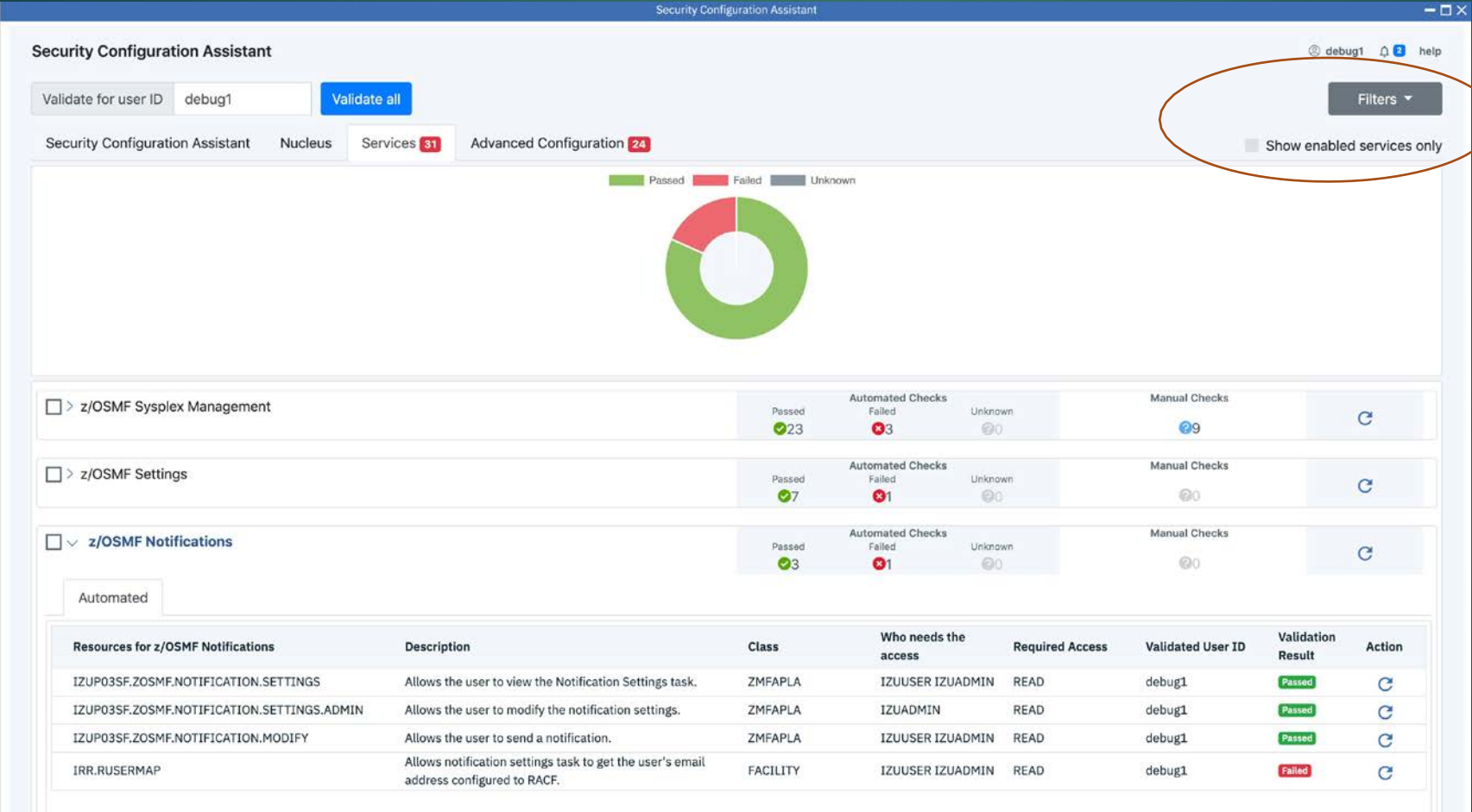
Under "TSO/E Address Space Services", there are two tabs: "Automated" and "Manual". The "Manual" tab is selected, showing a table of resources for TSO/E Address Space Services. The table has five columns: "Resources for TSO/E Address Space Services", "Description", "Class", "Who needs the access", and "Required Access".

Resources for TSO/E Address Space Services	Description	Class	Who needs the access	Required Access
<account>	Allows the user to use TSO account.	ACCTNUM	<User of the Service>	READ
<proc>	Allows the user to use TSO proc.	TSOPROC	<User of the Service>	READ
CEA.CEATSO.FLOW.<systemname>	Allows the user to use TSO/E address space services remote support.	SERVAUTH	<User of the Service>	READ

Below the table, there are more services listed: "z/OS Jobs REST Interface" (Passed 0, Automated Checks Failed 0, Unknown 0, Manual Checks 2), "z/OS Operator Consoles" (Passed 14, Automated Checks Failed 1, Unknown 0, Manual Checks 7), and "IBM Cloud Provisioning and Management for z/OS" (Passed 11, Automated Checks Failed 11, Unknown 0, Manual Checks 5).

# NEW Security Configuration Assistant task

- Security Configuration Assistant – Filter support



Filters ▾

- ☐ Failed
- ☐ Unknown
- ☐ Manual



# NEW Security Configuration Assistant task

- Security Configuration Assistant – Dependencies are included

The screenshot displays the Security Configuration Assistant interface. At the top, there's a header bar with the title "Security Configuration Assistant" and a "debug1" button. Below the header, there's a navigation bar with tabs: "Security Configuration Assistant", "Nucleus", "Services 31", and "Advanced Configuration 24". A "Validate all" button is visible. The main content area shows a list of services with their validation status. The "z/OS Operator Consoles" service is expanded, showing a table of resources for z/OS Operator Consoles. The table has columns: Resources for z/OS Operator Consoles, Description, Class, Who needs the access, Required Access, Validated User ID, Validation Result, and Action. The resources listed are CONSOLE, IZUP03SF.ZOSMF.CONSOLES.ZOSOPER, IZUP03SF.IzuManagementFacilityRestConsoles.izuUsers, and SYSPLEX.OPERLOG. All resources show a "Passed" validation result. Below this, there's another table for "Resources for TSO/E Address Space Services" with resources IZUACCT, IZUFPROC, CEA.CEATSO.\*, and CEA.CEATSO.FLOW.\*. All these resources also show a "Passed" validation result. A red circle highlights the "Resources for TSO/E Address Space Services" table.

Resources for z/OS Operator Consoles	Description	Class	Who needs the access	Required Access	Validated User ID	Validation Result	Action
CONSOLE	Allows the user to create an EMCS console through TSO Console command.	TSOAUTH	<User of the Service>	READ	debug1	Passed	⌂
IZUP03SF.ZOSMF.CONSOLES.ZOSOPER	Allows the user to view and access the z/OS Operator Consoles task in the z/OSMF navigation tree.	ZMFAPLA	IZUUSER IZUADMIN	READ	debug1	Passed	⌂
IZUP03SF.IzuManagementFacilityRestConsoles.izuUsers	Allows the user to connect to the z/OS Operator Consoles task.	EJBROLE	<User of the Service>	READ	debug1	Passed	⌂
SYSPLEX.OPERLOG	Allows user to retrieve OPERLOG.	LOGSTRM	<User of the Service>	READ	debug1	Passed	⌂

Resources for TSO/E Address Space Services	Description	Class	Who needs the access	Required Access	Validated User ID	Validation Result	Action
IZUACCT	Allows the user to use TSO account.	ACCTNUM	IZUUSER IZUADMIN	READ	debug1	Passed	⌂
IZUFPROC	Allows the user to use TSO proc.	TSOPROC	IZUUSER IZUADMIN	READ	debug1	Passed	⌂
CEA.CEATSO.*	Allows the user to use CEA.	SERVAUTH	<User of the Service>	READ	debug1	Passed	⌂
CEA.CEATSO.FLOW.*	Allows the user to use TSO/E address space services remote support.	SERVAUTH	<User of the Service>	READ	debug1	Passed	⌂

# RACF Classes Used in Various Definitions

- ▶ ACCTNUM
- ▶ APPL
- ▶ CSFSERV
- ▶ DATASET
- ▶ DIGTCERT
- ▶ DIGTRING
- ▶ EJBROLE
- ▶ FACILITY
- ▶ JESSPOOL
- ▶ LOGSTRM
- ▶ OPERCMDS
- ▶ PROGRAM
- ▶ PTKTDATA
- ▶ RDATA LIB – for certificates
- ▶ REALM
- ▶ SERVAUTH
- ▶ SERVER
- ▶ STARTED
- ▶ SURROGAT
- ▶ TSOAUTH
- ▶ TSOPROC
- ▶ ZMFAPLA
- ▶ ZMFCLOUD
- ▶ UNIXPRIV



# Security Configuration Assistant task



# Security Configuration Assistant task

```
ADCDMST.SYST.SAMPLIB(IZUSASEC) - 01.00 Columns 00001 00072
==> Scroll ==> CSR
/* Profile Definitions for z/OSMF Security Configuration Assistant */
RDEFINE ZMFAPLA IZUDFLT.ZOSMF.CONFIGURATION.SECURITY_ASSISTANT +
        UACC(NONE)

RDEFINE SERVER BBG.SECCLASS.SERVER UACC(NONE)
RDEFINE SERVER BBG.SECCLASS.APPL UACC(NONE)
RDEFINE SERVER BBG.SECCLASS.FACILITY UACC(NONE)
RDEFINE SERVER BBG.SECCLASS.EJBROLE UACC(NONE)
RDEFINE SERVER BBG.SECCLASS.SERVAUTH UACC(NONE)
RDEFINE SERVER BBG.SECCLASS.STARTED UACC(NONE)
RDEFINE SERVER BBG.SECCLASS.ZMFCLOUD UACC(NONE)
RDEFINE SERVER BBG.SECCLASS.ACCTNUM UACC(NONE)
RDEFINE SERVER BBG.SECCLASS.TSOPROC UACC(NONE)
RDEFINE SERVER BBG.SECCLASS.TSOAUTH UACC(NONE)
RDEFINE SERVER BBG.SECCLASS.OPERCMDS UACC(NONE)
RDEFINE SERVER BBG.SECCLASS.CSFSERV UACC(NONE)
RDEFINE SERVER BBG.SECCLASS.JESSPOOL UACC(NONE)
RDEFINE SERVER BBG.SECCLASS.LOGSTRM UACC(NONE)
RDEFINE SERVER BBG.SECCLASS.UNIXPRIV UACC(NONE)
RDEFINE SERVER BBG.SECCLASS.RDATA LIB UACC(NONE)
```



# Security Configuration Assistant task

```
/* **** */
/* Permit definitions for  z/OSMF Security Configuration Assistant */
/* **** */
/* Begin zOSMF Administrator Role Setup */
/* **** */
PERMIT IZUFLT.ZOSMF.CONFIGURATION.SECURITY_ASSISTANT +
      CLASS(ZMFAPLA) ACCESS(READ) ID(IZUADMIN)

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

# Security Configuration Assistant task

```
/* **** */
/*  Permit the started task USERID access  */
/* **** */
PERMIT BBG.SECCLASS.SERVER CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.SECCLASS.APPL CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.SECCLASS.FACILITY CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.SECCLASS.EJBROLE CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.SECCLASS.SERVAUTH CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.SECCLASS.STARTED CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.SECCLASS.ZMFAPLA CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.SECCLASS.ZMFCLOUD CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.SECCLASS.ACCTNUM CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.SECCLASS.TSOPROC CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.SECCLASS.TSOAUTH CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.SECCLASS.OPERCMDS CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.SECCLASS.CSFSESV CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.SECCLASS.JESSPOOL CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.SECCLASS.LOGSTRM CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.SECCLASS.UNIXPRIV CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
PERMIT BBG.SECCLASS.RDATALIB CLASS(SERVER) ACCESS(READ) ID(IZUSVR)
```



# Security Configuration Assistant task

```
1READY
```

```
  RL SERVER BBG.SECCLASS.SERVER ALL  
  ICH13003I BBG.SECCLASS.SERVER NOT FOUND  
  READY  
  END
```

```
  SR CLASS(SERVER) MASK(BBG)  
  BBG.ANGEL  
  BBG.ANGEL.IZUANG1  
  BBG.AUTHMOD.BBGZSCFM  
  BBG.AUTHMOD.BBGZSCFM.WOLA  
  BBG.SECCLASS.ZMFAPLA  
  BBG.SECCLASS.ZMFCLOUD  
  BBG.SECPFEX.BBGZDFLT  
  BBG.SECPFEX.IZUDFLT  
  READY  
  END
```

# Security Configuration Security Setup

## – Some Statistics – New Jobs

- ▶ In z/OS 2.3 there were approximately 336 RACF commands in the IZUxx members in SYS1.SAMPLIB
- ▶ In z/OS 2.4 there are approximately 642 RACF commands in the IZUxx members in SYS1.SAMPLIB
- ▶ The primary member in SYS1.SAMPLIB is IZUSEC. In z/OS 2.3 it contained 658 lines. In z/OS 2.4 this member has 751 lines.



# Security Configuration Security Setup

## – Some Statistics – New Jobs

JOBNAME	DESCRIPTION
IZUASSEC	Security Setup for z/OSMF AUTOSTART function
IZUATSEC	Security setup for z/OSMF Administrator tasks and web site links
IZUDCSEC	This sample JCL intends to help with security setup required per user of Discover CPC function
IZUICSEC	Setup hardware crypto(ICSF) for z/OSMF server
IZUNFSEC	Security setup for z/OSMF Notifications
IZUNUSEC	Security setup for z/OSMF Nucleus basic
IZURFSEC	Security Setup for z/OS data set and file REST interface
IZURJSEC	Security Setup for z/OS Jobs REST interface
IZUSASEC	Security Setup for z/OSMF Security Configuration Assistant
IZUSKSEC	Setup shared key ring and certificate for the z/OSMF server
IZUSTSEC	This sample JCL intends to help with security setup required per user of z/OSMF settings
IZUSWSEC	This sample JCL intends to help with security setup required for z/OSMF Support Swagger Document Profile for Liberty API Discovery support
IZUTLSEC	Setup AT-TLS security for z/OSMF server
IZUTSSEC	This sample JCL intends to help with security setup required per user of z/OSMF TSO/E address space service
IZUWFSEC	z/OSMF work flows

# Security Configuration Security Setup

## – Summary

- ▶ Major improvements in RACF commands
- ▶ Security Assistant great improvement and contains lots of detail



# Security Configuration Security Setup

## – Summary

- ▶ Some RACF profiles have changed and some have been removed.
  - ▶ Note RACF commands provide do not always include fields like OWNER, SUPERIOGROUP
    - ▶ This is applicable for ADDGROUP, ADDUSER, RDEFINE, CONNECT
    - ▶ Did not provide all the instances, one should review the commands before executing
- ▶ Activates classes sometimes before profiles are created
  - ▶ Adds groups IZUADMIN, IZUUSER, IZUUNGRP
    - ▶ This corresponds to what is defined in IZUPRMxx in SYS1.PARMLIB
    - ▶ Assumes AUTOGID

# z/OSMF – From a Security Perspective

- ▶ Sample JCL is SYS1.SAMPLIB – IZUSEC is the primary one for setting up the base configuration
  - ▶ Adds user IZUSVR – this will be userid for the 2 started tasks
    - ▶ DEFAULTGROUP(IZUADMIN)
    - ▶ Assumes AUTOUID
  - ▶ Adds user IZUGUEST – this is unauthenticated user
    - ▶ Makes user RESTRICTED
    - ▶ This corresponds to what is defined in IZUPRMxx in SYS1.PARMLIB
    - ▶ DEFAULTGROUP(IZUUNGRP)



# z/OSMF – From a Security Perspective

- ▶ RACF commands are fully qualified generics
- ▶ Review commands as they may undercut what is already defined in your system.
- ▶ Review commands as an example of CSFSERV as this will define more profiles that may cause other areas to stop working.
- ▶ Recommend put in 'back stop' entries to protect other areas
- ▶ Recommend putting in generic profiles versus fully qualified generics
- ▶ As the JCL states, review the JCL for you company standards and completeness.
- ▶ Still need to RACF CONNECT people to the appropriate groups
- ▶ The initial product needs to be up and running before you can configure / use the security assistant



# QUESTIONS



# z/OSMF Security Setup Overview V2R4

JULIE BERGH