2013
IBM Systems

z/OSMF V2.1 Implementation and Configuration

z/OSMF V2.1 became available on 30 September 2013.

Greg Daynes
z/OS Installation and Deployment Architect

IBM

Agenda

- **Overview of z/OS Management Facility V2.1**
- **Ordering and Installing z/OS Management Facility V2.1**
  - Via ServerPac or SMP/E
- **New user setup and configure z/OSMF "base"**
  - Using z/OSMF scripts
  - Using ServerPac jobs
- **Existing user migrating to z/OSMF V2.1**
- **Adding additional "plug-ins"**
  - Configuring the z/OS requisites
    - Note: Due to time constraints, identifying and configuring the z/OS requisites for each of the z/OSMF plug-ins will not be discussed, but information is included in the handout (.pdf file).
  - Configuring z/OSMF to include the "plug-ins"
- **Authorizing users to z/OSMF**

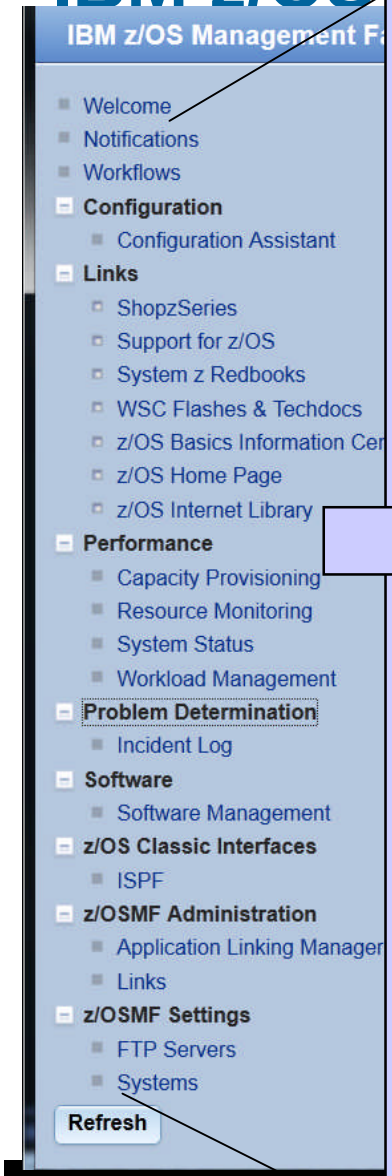
Agenda

- **Overview of z/OS Management Facility V2.1**
- **Ordering and Installing z/OS Management Facility V2.1**
  - Via ServerPac or SMP/E
- **New user setup and configure z/OSMF "base"**
  - Using z/OSMF scripts
  - Using ServerPac jobs
- **Existing user migrating to z/OSMF V2.1**
- **Adding additional "plug-ins"**
  - Configuring the z/OS requisites
  - Configuring z/OSMF to include the "plug-ins"
- **Authorizing users to z/OSMF**

IBM z/OS Management Facility

- **The IBM z/OS Management Facility is a separate product for z/OS that provides support for a modern, Web-browser based management console for z/OS.**
- **It helps system programmers more easily manage and administer a mainframe system by simplifying day to day operations and administration of a z/OS system.**
- **More than just a graphical user interface, the z/OS Management Facility is intelligent, addressing the needs of a diversified skilled workforce and maximizing their productivity.**
  - Automated tasks can help reduce the learning curve and improve productivity.
  - Embedded active user assistance (such as wizards) guide you through tasks and helps provide simplified operations.

IBM z/OS Management Facility



- **Notifications (V2.1)** - View and act on the z/OSMF notifications that have been assigned to you
- **Workflow (V2.1)** - Perform a guided set of steps, for example, to configure components or products in your installation.
- **Configuration** category
  - **Configuration Assistant for z/OS Communication Server** application - simplified configuration and setup of TCP/IP policy-based networking functions
- **Links** category
  - Links to resources - provide common launch point for accessing resources beyond z/OSMF
- **Performance** category
  - **Capacity Provisioning** application - manage connections to CPMs, view reports for domain status, active configuration and active policy.
  - **Resource Monitoring, System Status** - provide integrated performance monitoring of customer's enterprise
  - **Workload Manager Policy Editor** application (updated) - Facilitate the creation and editing of WLM service definitions, installation of WLM service definitions, and activation of WLM service policies
- **Problem Determination** category
  - **Incident Log** application (updated) **-** provide a consolidated list of SVC Dump related problems, along with details and diagnostic data captured with each incident; facilitate sending the data for further diagnostics.
- **Software** category
  - **Management** application (updated) **-** deployment of installed software simpler and safer, manage service levels and product levels
- **z/OS classic Interface** category
  - **ISPF Task -** integrate existing ISPF into z/OSMF to enable tasks from single interface and ability to launch to ISPF functions directly
- **z/OSMF Administration** category
  - z/OSMF authorization services for administrator:- dynamically add links to non-z/OSMF resources; application linking manager
- **z/OSMF Settings** category (V2.1)
  - Manage FTP destinations and systems

z/OS Management Facility

Problem Management & Analysis	Installation, Migration, and Maintenance	Configuration
Monitoring z/OS system health; identifying real and potential problems; Analyzing and resolving problems	*Planning, installing, and upgrading z/OS systems and products that run on z/OS*	*Adding or changing z/OS system components; enabling new features; defining and updating policies that affect system behavior*

Simplify and modernize the user experience and programming requirements
Task-oriented browser based user-interface; end-to-end task simplification ; eliminating opportunity for error

Incident Log (z/OSMF V1.11)
The Incident Log provides a consolidated list of SVC Dump related problems, along with details and diagnostic data captured with each incident. It also facilitates sending the data for further diagnostics.

Software Management (z/OSMF V1.13) The z/OSMF Software Management provides a simple, structured approach to deploying SMP/E installed software, In addition, it allows for inspection of a software instance to view the product, feature, FMID content, SYSMODS, as well as the physical datasets that comprise a particular software instance. It also enables you to perform actions to analyze and report on software instances (such as identifying installed products with an announced end of service date).

Configuration Assistant for z/OS Communications Server (z/OSMF V1.11) Simplified configuration and setup of TCP/IP policy-based networking functions

WLM Policy Editor (z/OSMF V1.12)
Simplified management of WLM service definitions and policies. Facilitate the creation and editing of WLM service definitions, installation of WLM service definitions, and activation of WLM service policies

Resource Monitoring (z/OSMF V1.12) Provides dynamic real time metrics for system performance

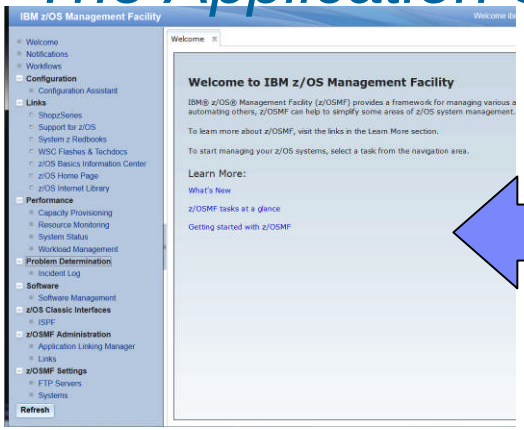
Capacity Provisioning (z/OSMF V1.13) simplify the work of a z/OS CP administrator to manage connections to CPMs, view reports for domain status, active configuration and active policy.

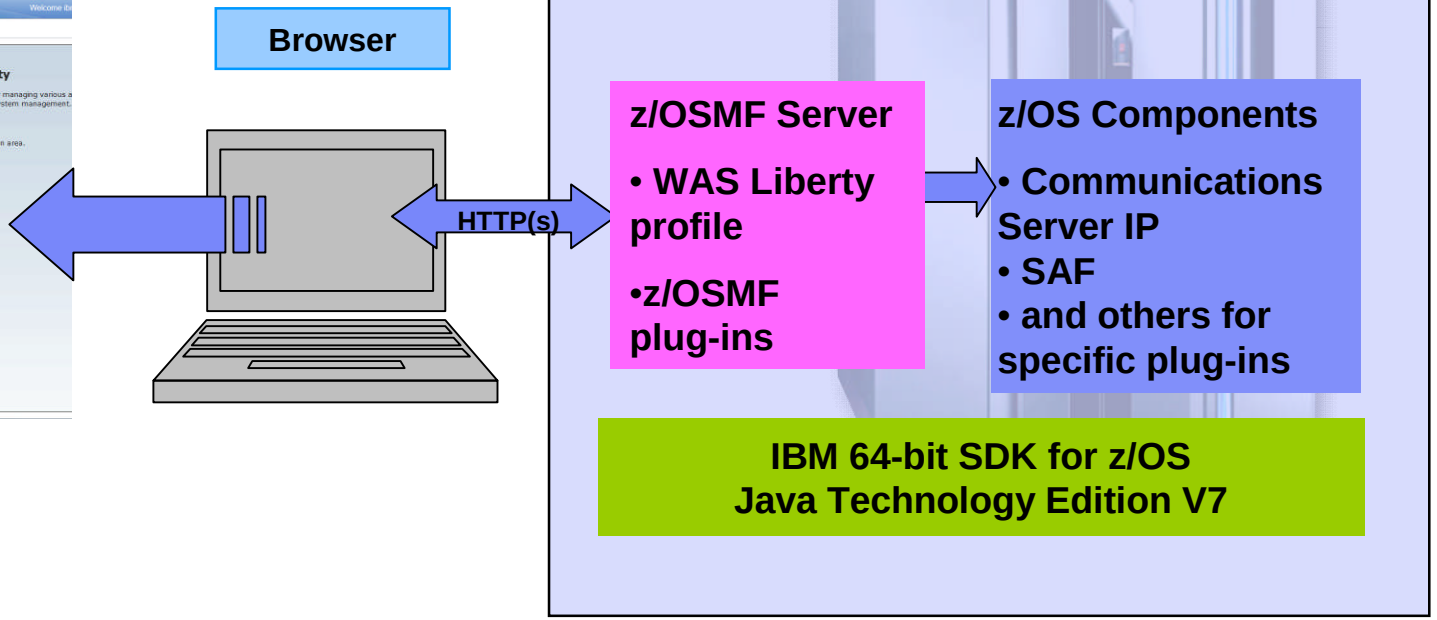
z/OSMF Base Services:

- **Notifications (z/OSMF V2.1)** View and act on the z/OSMF notifications that have been assigned to you
- **Workflow (z/OSMF V2.1)** Perform a guided set of steps, for example, to configure components or products in your installation
- The ability to add non-z/OSMF launch points and links to any category in the navigation tree allows a central tool for effective information and knowledge sharing.
- **Security integration with SAF (z/OSMF V1.13)**
- **ISPF Web UI (z/OSMF V1.13)**
- **REST API for Jobs (z/OSMF V1.13)**

IBM z/OS Management Facility

The Application Stack





- **The z/OS Management Facility applications run on the z/OS enabling you to manage z/OS from z/OS**
  - Information is presented on a PC using a browser
- **The z/OS Management Facility requires:**
  - z/OS Communications Server
  - Security definitions (SAF)
  - Other components are required for specific z/OSMF plug-ins
  - IBM 64-bit SDK for z/OS Java Technology Edition V7

Agenda

- Overview of z/OS Management Facility V2.1
- **Ordering and Installing z/OS Management Facility V2.1**
  - Via ServerPac or SMP/E
- New user setup and configure z/OSMF “base”
  - Using z/OSMF scripts
  - Using ServerPac jobs
- Existing user migrating to z/OSMF V2.1
- Adding additional “plug-ins”
  - Configuring the z/OS requisites
  - Configuring z/OSMF to include the “plug-ins”
- Authorizing users to z/OSMF

IBM z/OS Management Facility

- The IBM z/OS Management Facility is ... licensed program product
  - z/OS Management Fa... (5610-A01)
  - z/OS Manag... ...ity Subscription and Support (5655-S29)
- The IBM z/OS ...anagement Facility product consists of :
  - WebSphere Liberty Profile V8.5
  - z/OSMF core infrastructure
  - z/OSMF plug-ins
- z/OSMF V2.1 requires
  - z/OS V2.1
  - IBM 64-bit SDK for z/OS Java Technology Edition V7
- You can include z/OSMF in:
  - A ServerPac that also includes z/OS V2.1 and IBM 64-bit SDK for z/OS Java Technology Edition V7
  - A CBPDO (comes in SMP/E format) with or without other products
  - A Product ServerPac (comes in its own target, DLIB, and global zones)

No Additional Charge = Free

IBM z/OS Management Facility

- z/OSMF V2.1 consists of nine (9) FMIDs:
  - HSMA210 - z/OS Management Facility core
  - HSMA211 - z/OSMF ISPF
  - HSMA212 - z/OSMF Resource Monitoring
  - HSMA213 - z/OSMF WLM
  - HSMA214 – z/OSMF Software Deployment (really Software Management)
  - HSMA215 - z/OSMF Incident Log
  - HSMA216 - z/OSMF Capacity Provisioning
  - HSMA217 – z/OSMF Workflow
  - HSMA21A - z/OSMF Configuration Assistant

z/OSMF Installation

- **Installing the software (code) done via ServerPac or SMP/E**
  - Product file system
    - Described by Program Directory
    - 401 CYLs
      - 4x bigger than the z/OSMF V1.12 default size
      - 2.6x bigger than z/OSMF V1.13 default size
    - Allocated via sample job IZUISHFS as CYL(300 30)
      - May want to override HFSPRIM from “300” to “415”
    - Can be HFS or zFS
  - Note: You no longer need the WAS OEM product file system that was allocated as CYL(2400 50)

Agenda

- **Overview of z/OS Management Facility V2.1**
- **Ordering and Installing z/OS Management Facility V2.1**
  - Via ServerPac or SMP/E
- **New user setup and configure z/OSMF "base"**
  - **Using z/OSMF scripts**
  - Using ServerPac jobs
- **Existing user migrating to z/OSMF V2.1**
- **Adding additional "plug-ins"**
  - Configuring the z/OS requisites
  - Configuring z/OSMF to include the "plug-ins"
- **Authorizing users to z/OSMF**

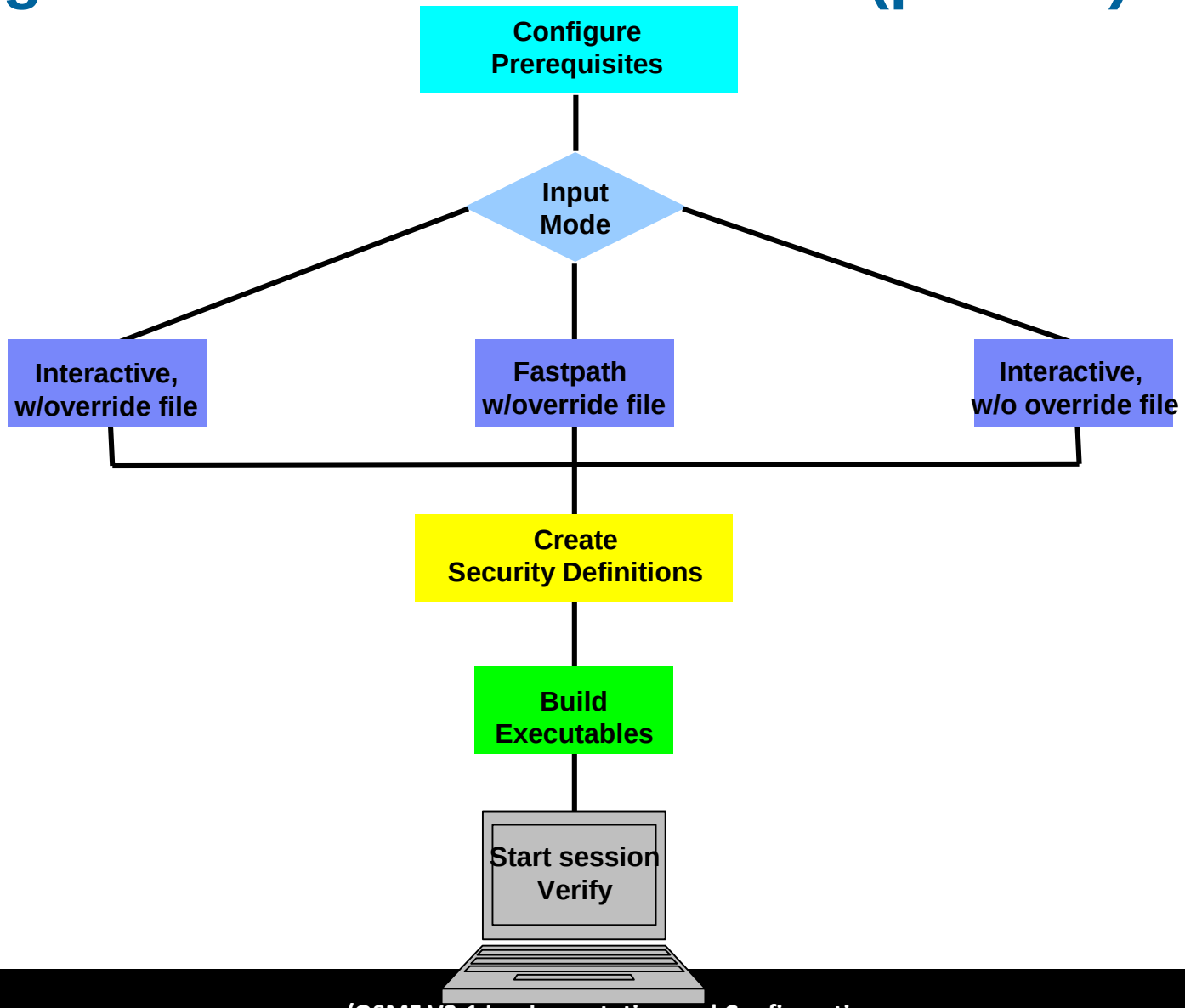
z/OSMF Configuration Process

- **The z/OSMF Configuration Guide**
  - The configuration guide has been restructured to reflect a change in the recommended sequence for configuring z/OSMF.
    - In previous releases, we recommended that new customers create a functionally robust instance of z/OSMF in the initial pass through the configuration scripts, with all or most of the optional plug-ins selected. That approach required you to complete all host system customization for the optional plug-ins during the initial setup of the product.
    - **The new recommended approach for a new or first time installation is now a two-phase sequence:**
      1. **Create a base configuration (that is, with no optional plug-ins selected)**
      2. **Add plug-ins, users, and host system customizations later, when you choose to do so.**

Configuration Process Overview

- **z/OSMF has four basic stages for configuration**
  1. **Configure prerequisites**
  2. **Setup the configuration file**
  3. **Create security definitions**
  4. **Build the executables (run-time files)**

Configuration Process Overview (picture)



Prerequisites

- **Client machine (no client machine install requirements)**
  - **The client browser can run in the following operating systems:**
    - Microsoft Windows XP 32-bit
    - Windows 7 32-bit
    - Windows 7 64-bit
  - **For a complete list of supported browsers see:**
    - http://www-03.ibm.com/systems/z/os/zos/zosmf/browser_notes.html

Prerequisites …

- **Client machine (no client machine install requirements)**
  - **The z/OSMF interface supports a minimum screen resolution of 1024 by 768 pixels.**
    - If your workstation is set to a lesser resolution, you might experience some clipping of content.
  - **Ensure that your browser is enabled for JavaScript.**
  - **z/OSMF uses session cookies to track which users are logged in from a specific browser.**
    - If you want to allow multiple users to log in from a single location, or if you want the ability to log in to multiple servers from the same workstation, you might need to either launch another browser instance (as with Internet Explorer), or, configure another browser profile (as with Firefox).
  - **If you plan to use the Internet Explorer browser to work with WLM service definitions, ensure that the browser is enabled for automatic prompting for file downloads.**
    - This setting prevents the file download blocker from being invoked when you download service definitions to your workstation. Otherwise, if automatic prompting is disabled (the default setting), the download blocker prompts you to accept these file downloads, causing your session to be reloaded and your active tabs to be closed. To avoid this disruption, enable automatic prompting for file downloads.

Prerequisites

- **Host system**
  - **IBM System z9 Enterprise Class (z9 EC) or IBM System z9 Business Class (z9 BC) or higher**
  - **Ensure that your target system has the following:**
    - **Available CPU resource equivalent to a processor with a processor capacity index (PCI) of at least 45.**
    - **One gigabyte (1 GB) of central storage. This amount is in addition to your existing storage allocation for other applications running in the same z/OS system.**

Notes:

1. These are significantly reduced from z/OSMF V1.13
2. It may be possible to execute some z/OSMF applications and scenarios on systems that do not meet the requirements above, depending upon the number of objects to be retrieved and/or displayed by z/OSMF. However, under these circumstances, z/OSMF may sometimes exhibit behaviors such as long response times, time outs, blank response screens, or abnormal terminations (ABENDs).

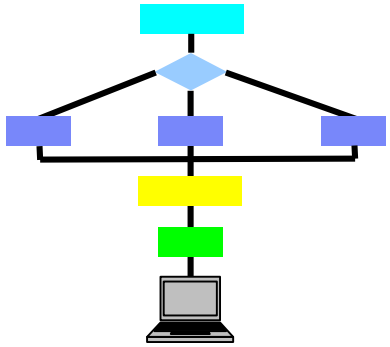
Prerequisites …

- **z/OS V2.1 (5650-ZOS) with the following PTFs**
  - UA68211
  - UA65303
  - UA67499
- **IBM 64-bit SDK for z/OS, Java Technology Edition, Version 7 (5655-W44) with PTFs**
  - UK83228
  - UK83229
- **A userid with sufficient (“superuser”) authority**
  - Using UNIXPRIV class profiles (which is the recommended way)
    - CONTROL access to SUPERUSER.FILESYS
    - UPDATE access to SUPERUSER.FILESYS.MOUNT
    - READ access to SUPERUSER.FILESYS.CHOWN
    - READ access to SUPERUSER.FILESYS.CHANGEPERMS
    - READ access to SUPERUSER.FILESYS.PFSCTL
  - Using the BPX.SUPERUSER resource in the FACILITY class.
  - Assigning a UID of 0 (which is the least desirable way)

z/OSMF Configuration Process

- **The configuration process occurs in three stages, and in the following order:**
  1. **Stage 1 – Configuration**
     - **izusetup.sh -file *etc/zosmf/izuconfig1*.cfg -config**

     a. **Interactive mode (with an override file)**
     b. **Fastpath mode**
     c. **Interactive mode (without an override file)**
  2. **Stage 2 - Security setup**
     - **Invoke Security REXX EXEC**
       - ***/etc/zosmf*/izuconfig1.cfg.rexx**
       - ***/etc/zomf*/izuconfig1.cfg.**<z/OSMF Installer USERID>**.rexx**
     - **Verify the RACF Security Setup**
       - **izusetup.sh -file */etc/zosmf/izuconfig1*.cfg –verify racf**
  3. **Stage 3 – Build the executables – deploy the z/OSMF apps**
     - **Complete the setup (configure and verify z/OSMF)**
       - **izusetup.sh -file */etc/zosmf/izuconfig1*.cfg -finish**



z/OSMF Configuration Roles and Authorities

Action to perform	Script invocation	Performed by
Step N1: Create the initial configuration	izusetup.sh -file <*pathname/filename*>.cfg -config *[...other options...]*	z/OSMF installer (Superuser)
Step N2: Run the security commands for z/OSMF resources	<*IZU_CONFIG_DIR*>/izuconfig1.cfg.rexx	Security Administrator
Step N3: Run the security commands for the z/OSMF installer	<*IZU_CONFIG_DIR*>/izuconfig1.cfg. <z/OSMF-Installer-USERID>.rexx	Security Administrator
Step N4: Verify the RACF security setup	izusetup.sh -file <*pathname/filename*>.cfg -verify racf	Security Administrator
Step N5: Complete the setup	izusetup.sh -file <*pathname/filename*>.cfg -finish	z/OSMF installer (Superuser)
Step N6: Start the z/OSMF server	START IZUANG1 START IZUSVR1	System Operator
Step N7: Access the z/OSMF Welcome task	You can verify the success of your configuration changes by opening your browser to the z/OSMF Welcome task.	Any authorized z/OSMF user (z/OSMF installer)

z/OSMF Configuration Scripts and Files

- **Following are the main components of the z/OSMF configuration process:**
  - **izusetup.sh**
    - The shell script, with several options, that is used to configure z/OSMF.
    - You can run this script interactively or "quietly" (the *fastpath* mode), as you prefer.
    - This script is located in the /bin subdirectory of the product file system: <IZU_CODE_ROOT>/bin.
  - **izudflt.cfg**
    - The configuration file that is shipped with z/OSMF.
    - This file contains IBM-supplied configuration values that can be used as input to a base configuration.
    - This file is located in the /defaults subdirectory of the product file system, by default: <IZU_CODE_ROOT>/defaults.
    - Do not edit the IBM-supplied configuration file.
  - **izudflt.ovr**
    - The optional override file that is used to replace any of the settings found in the configuration file.
    - A default copy of this file is located in the /defaults subdirectory of the product file system, by default: <IZU_CODE_ROOT>/defaults**.**
  - **izu_env.sh**
    - The optional environment variables file that can be used to modify the session defaults that are in effect when you run the shell script.
    - A default copy of this file is located in the /defaults subdirectory of the product file system, by default: <IZU_CODE_ROOT>/defaults.

Modes for Running the z/OSMF Configuration Script

Resulting behavior	Resulting behavior	When to use this mode
Interactive mode (with an override file)	Script prompts you for configuration values, displaying the values from your override file as defaults. Values not found in the override file are taken from the specified configuration file. In response to each prompt, you must either press Enter to accept your installation-specific value, or type a new value.	You want the configuration session to be preset with your installation-specific values. This method saves you from having to enter your values interactively in response to script prompts. Instead, you need only review each value displayed by the script and press Enter to accept it.
Interactive mode (without an override file)	Script prompts you for configuration values, displaying the values from the configuration file as defaults. In response to each prompt, you must either press Enter to use the configuration file value, or type your installation specific value.	You have determined that most of the IBM-supplied defaults are appropriate for your installation, and you would prefer to supply the few needed modifications interactively in response to script prompts.
Fastpath mode (with an override file)	Script runs to completion without any interactive prompting. Values are used as supplied in the specified override file. Any values not found in the override file are taken from the configuration file. If a value is not found in either location, the script ends with an error message indicating the first value that could not be found.	You prefer to supply your data in a standalone file, and have no need to review the values interactively. You have verified that all of the necessary configuration data is supplied through the configuration file, or the optional override file, or a combination of both files. Or, you need to re-run the configuration process to update an erroneous value in an existing configuration file, and do not want to repeat the prompts.

Before You Begin Configuration

- **Consider using AUTOUID/AUTOGID instead of manually providing UID/GID values**
  - –You can specify to have RACF automatically generate a unique ID values.
    - RACF must be able to automatically select an unused UID or GID value for z/OSMF user IDs and groups.
      - oTherefore the SHARED.IDS and BPX.NEXT.USER RACF profiles must be defined, and the BPX.NEXT.USER RACF profile must be used to indicate the ranges from which UID and GID values are selected.
      - oRefer to the *z/OS Security Server RACF Security Administrator's Guide* for your z/OS system for more information on how to use these operands.

Before You Begin Configuration …

- **Use the configuration worksheet as a guide, determine the appropriate value that should be specified for that system.**
  - Fill in the information on the worksheet to help ensure that you know the correct values to enter for the prompts prior to starting the izusetup script.
- **Use an override file if the default value does not suffice for the system onto which z/OSMF is being configured.**

Before You Begin Configuration …

- **z/OSMF by default uses standard port numbers**
  - 443 is the Port number for SSL encrypted traffic from the active instance of z/OSMF on your system. This follows the Internet Engineering Task Force (IETF) standard.
  - 80 is the Port number for non-encrypted traffic from the active instance of z/OSMF on your system.
- **You can change the port numbers as part of z/OSMF Configuration**
- **Whatever port numbers you choose to use, you should reserve them in your TCP/IP profile setting**
  - For example, if you take the z/OSMF default values include the following in your TCP/IP profile configuration settings

```
80 TCP IZUSVR1            ; HTTPTRANSPORTPORT
443 TCP IZUSVR1 NODELAYACKS ; HTTPSSLPORT
```

z/OSMF Prompts and Override File

- **The following prompts are the ones that are most likely to require changes:**
  - GID and UID defaults (I use AUTOUID/AUTOGID)
  - z/OSMF data filesystem data set name
  - Volume serial numbers for file system data set
  - z/OSMF R/W directories
  - Port numbers
  - Hostname
- **However, you should review ALL of the other prompts to determine if any additional configuration variables need to be updated.**
  - You can either in respond to the prompts, or update the override file with the changed values

Example of a z/OSMF V2.1 Override File

```
# Licensed Materials - Property of IBM
# 5610-A01
# Copyright IBM Corp. 2013
#
# Status = HSMA210
#
# Information:
#
# SID=1.1.1.46
# Delta Date=3/17/13
# Delta Time=11:43:01
#
# The izudflt.ovr file does not contain every variable=value pair that i
# Those variables that are least likely to be modifed do not appear in t
# If your installation requires a change to a variable that isn't in thi
# to configure it in your override file, simply add it with the modified
#
# Do not update or remove variable IZU_OVERRIDE_FILE_VERSION.  The infor
# is required for the configuration processing.
IZU_OVERRIDE_FILE_VERSION=2.1.0
IZU_DATA_DIR=/var/zosmf/data
IZU_CONFIG_DIR=/etc/zosmf
IZU_LOGFILE_DIR=/var/zosmf/configuration/logs
IZU_STARTED_TASK_USERID_HOME=/var/zosmf/data/home/izusvr
IZU_DATA_FS_NAME=C90BUILD.ZR21ESP.SIZUDATA
IZU_DATA_FS_VOLUME='C90ES4'
IZU_AUTOUID_OVERRIDE=Y
IZU_AUTOGID_OVERRIDE=Y
IZU_HTTP_SSL_PORT=443
IZU_HTTP_PORT=80
IZU_APPSERVER_HOSTNAME=@HOSTNAME
```

Complete override file used

You may want to override for High Availability Environments

AUTOUID and AUTOGID used for simplification

The default override file has many additional entries

By default NO plug-ins are configured

Step N1: Create the initial configuration

- The **izusetup.sh -config** script uses the input you supply, based on your environment. The script saves your input in the configuration file, which is used as input to subsequent script invocations.
- **Regardless of which mode you use, the script does the following:**
  - Creates a configuration file as output.
  - As an aid to your security administrator, the script creates a set of REXX EXEC programs with sample RACF commands that your security administrator can review and run. If your installation uses another security management product, you can create equivalent SAF commands. The commands are tailored based on your configuration settings.
- **Sample command:**
  - izusetup.sh -file /etc/zosmf/izuconfig1.cfg -config -overridefile /etc/zosmf/izudflt.ovr

Remember the name of the configuration file

Steps N2 and N3: Run the Security Commands

- **Two EXECs need to be run:**
  1. **izuconfig1.cfg.rexx**
     - This EXEC contains the complete set of RACF commands that your security administrator can use to secure the z/OSMF functions and tasks.
     - The exec also contains commented sections for additional authorizations that might be useful for your installation.
  2. **izuconfig1.cfg.<z/OSMF Installer USERID>.rexx**
     - This EXEC contains the RACF commands for authorizing your user ID to:
       - Complete the z/OSMF configuration process
       - Log in to the Welcome page at the end of the configuration process
       - Perform other post-configuration tasks, as needed.
- If your installation uses a security management product other than RACF, do not perform this step. Instead, your installation must create equivalent commands for your security product.

Step N2: Run the Security Commands

- **This EXEC is run by your installation's security administrator.**
- **Prior to running the REXX EXEC review the RACF commands and comments making any necessary changes**
  - If you provided the proper User ID and Group names during the configuration process, you shouldn't have to edit those commands
  - If you need to make any changes, copy the REXX EXEC to another file and make changes to the copied file
- **Sample invocation of REXX EXEC**
  - From the /etc/zosmf/ directory
    - ./izuconfig1.cfg.rexx | tee /var/zosmf/configuration/logs/izuconfig1_cfg_rexx.log

Captures command output in a file

Step N3: Run the Security Commands

- **This EXEC is run by your installation's security administrator.**
- **Prior to running the REXX EXEC review the RACF commands and comments making any necessary changes**
  - If you need to make any changes, copy the REXX EXEC to another file and make changes to the copied file
- **Sample invocation of REXX EXEC**
  - From the /etc/zosmf/ directory
    - ./izuconfig1.cfg**.<z/OSMF Installer USERID>.**rexx | tee /var/zosmf/configuration/logs/izuconfig1_cfg_ **<z/OSMF Installer USERID>.** rexx.log

Captures command output in a file

Step N4: Verify the RACF Security Setup

- **This exec is run by your installation's security administrator.**
- The **izusetup.sh** script verifies the RACF security setup actions that were performed in the previous steps.
- If your installation uses a security management product other than RACF, do not perform this step. Instead, take the appropriate steps to verify your security setup.
- **Sample command**
  - izusetup.sh -file /etc/zosmf/izuconfig1.cfg -verify racf
- On completion, the script creates a report file called **izuracfverify.report**, which by default is stored in the following location:
  - /var/zosmf/configuration/logs/izuracfverify.report

Step N5: Complete the Setup

- The **izusetup.sh** script creates an instance of z/OSMF, using the values you supplied earlier.
- Specifically, the script:
  - Initializes the z/OSMF data file system and creates the necessary directories and files. This work includes:
    - Allocating the z/OSMF data file system and mounting it, by default, at /var/zosmf/data.
    - Mounting the filesystem with the option UNMOUNT to ensure that it is unmounted if the z/OS system becomes unavailable. Also, for a zFS filesystem, the script mounts the filesystem with the option PARM('AGGRGROW') to allow the filesystem to grow dynamically, as needed.
    - Setting the permissions and ownership of the directories and files in the z/OSMF data file system.
  - Creates the home directory for the z/OSMF started task, if this directory does not exist already. By default, the directory is /var/zosmf/data/home/izusvr.
  - Changes ownership and permissions for the other directories that z/OSMF uses.
  - Performs other data set allocations, as needed for z/OSMF processing.
  - Verifies the setup for the z/OSMF functions and tasks.

Step N5: Complete the Setup …

- **The script is intended to be run by the z/OSMF Installer (Superuser)**

Same configuration file as prior command

- **Sample command:**
  - izusetup.sh -file /etc/zosmf/izuconfig1.cfg -finish
- On completion, the script displays message IZUG349I, which provides the link for accessing z/OSMF.
  - This message is also written to the script log file: I*ZU_LOGFILE_DIR*>/izusetup_finish.*mm.dd.yy.hh.mm.ss.tt*.log where *<IZU_LOGFILE_DIR>* is the log file directory for your installation.
    - By default, this directory is /var/zosmf/configuration/logs/.

Step N6: Start the z/OSMF server

- **To start the z/OSMF server manually, you can enter the MVS START command from the operator console.**
  - The START command specifies the member name to start and, optionally, the job name to use, for example:
    - **START IZUANG1**, JOBNAME=*jobname*
    - **START IZUSVR1**, JOBNAME=*jobname*
  - Start the tasks in the following sequence: IZUANG1 followed by IZUSVR1.
    - Otherwise, z/OSMF users might encounter authorization errors later when logging in to the z/OSMF Welcome page.
  - On server start-up, a number of messages are written to SYSLOG:

    $HASP100 IZUANG1 ON STCINRDR
    $HASP373 IZUANG1 STARTED
    CWWKB0056I INITIALIZATION COMPLETE FOR ANGEL
    $HASP100 IZUSVR1 ON STCINRDR
    $HASP373 IZUSVR1 STARTED
    IZUG400I: The z/OSMF Web application services are initialized.
    +CWWKF0011I: The server zosmfServer is ready to run a smarter planet.
  - Consider having the server start automatically at system IPL time by
    - Adding the commands to a COMMNDxx PARMLIB member, and
    - Updating BPXPRMxx to mount (or automount) the z/OSMF file systems

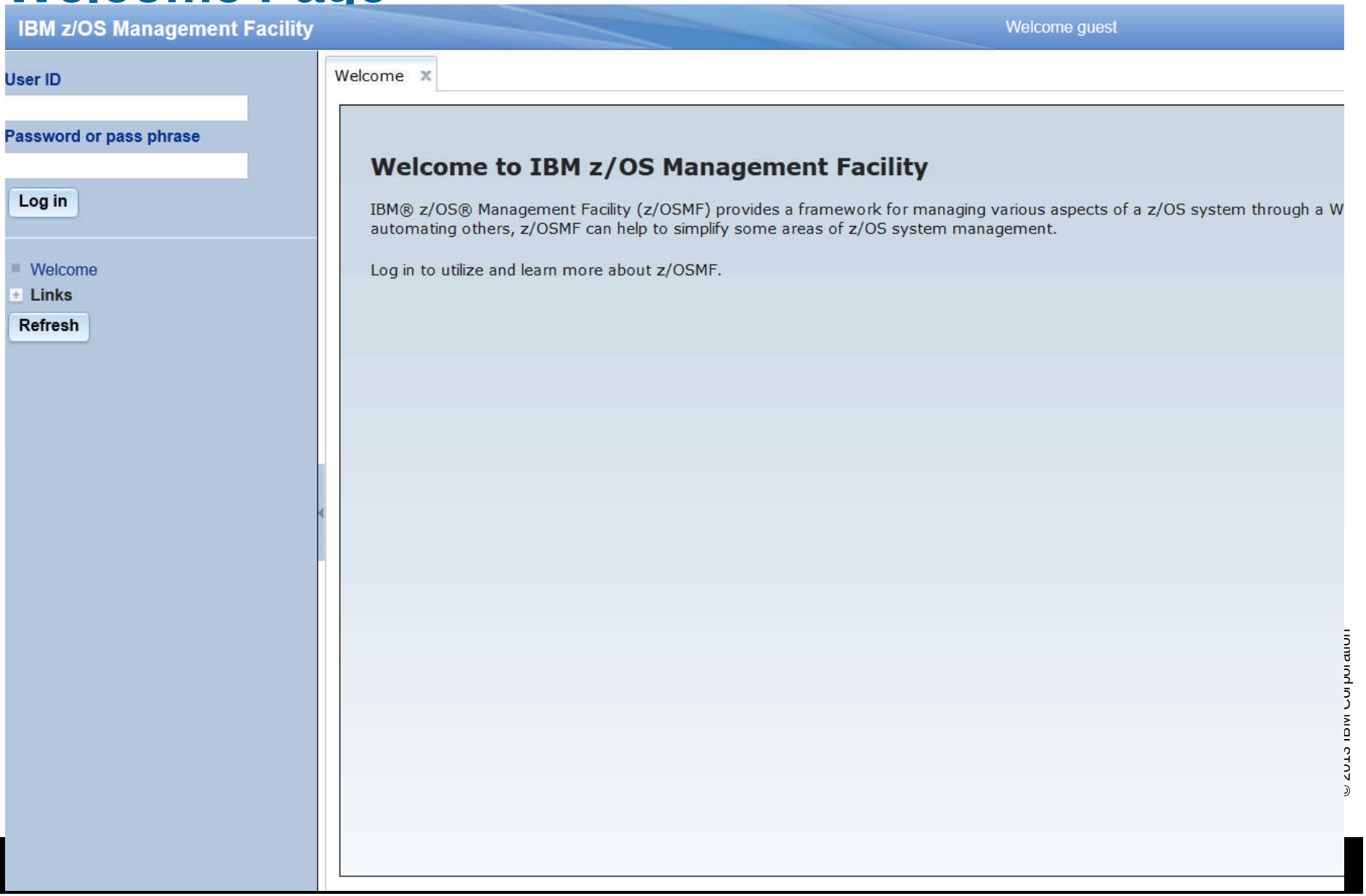
Step N7: Access the z/OSMF Welcome page

- At the end of the z/OSMF configuration process, you can verify the results of your work by opening a web browser to the Welcome page.
- The URL for the Welcome page has the following format:
  - https://hostname:port/zosmf/

  where:
    - *hostname* is the hostname or IP address of the system in which z/OSMF is installed
    - *port* is the secure application port for the z/OSMF configuration. *port* is optional. If you specified a secure port for SSL encrypted traffic during the configuration process (through variable IZU_HTTP_SSL_PORT), that value is required to log in. Otherwise, it is assumed that you are using port 443, the default.
- To find the URL, see message IZUG349I, which was written to the log file that was created when you ran the **izusetup.sh** script.
  - This log file is in the format:
    - *<IZU_LOGFILE_DIR>*/izusetup_finish.*mm.dd.yy.hh.mm.ss.tt*.log

    where *<IZU_LOGFILE_DIR>* is the log file directory for your installation. By default, this directory is /var/zosmf/configuration/logs/.
- Open a web browser to the Welcome page

Welcome Page



Next Steps

- **Adding additional “plug-ins”**
  - Configuring the z/OS requisites
  - Configuring z/OSMF to include the “plug-ins”
- **Authorizing users to z/OSMF**

Agenda

- Overview of z/OS Management Facility V2.1
- Ordering and Installing z/OS Management Facility V2.1
  - Via ServerPac or SMP/E
- **New user setup and configure z/OSMF "base"**
  - Using z/OSMF scripts
  - **Using ServerPac jobs**
- Existing user migrating to z/OSMF V2.1
- Adding additional "plug-ins"
  - Configuring the z/OS requisites
  - Configuring z/OSMF to include the "plug-ins"
- Authorizing users to z/OSMF

New user using ServerPac Jobs

- **Use the CustomPac Installation dialogs to install your ServerPac**
  - z/OSMF can be part of a z/OS ServerPac or in its own “product” ServerPac
- **The ServerPac jobs will create a default base z/OSMF configuration with the data set names and paths that you defined during Modify System Layout**
  - For z/OS ServerPac’s, the “Full System Replace” install method must be used
- **If you choose not to run the ServerPac jobs, or want to override additional defaults then you should configure z/OSMF using the scripts (as previously described)**
  - Note: All jobs listed on the next page must be run to configure z/OSMF

New user using ServerPac Jobs …

- **As part of the installation process, several jobs are created. The following jobs configure the z/OSMF "base"**
  - **RACFTGT** – Defines security definitions for the target system, including required z/OSMF definitions
    - Only used if your security product is RACF
  - **HSMA210B** – Defines ports to TCP/IP for use with z/OSMF
  - **HSMA210D** - Updates the /etc/zosmf/izudflt.ovr with product variables taken from installation dialogs and with product defaults.
    - This job **must** be run from the target system

    Note: After this job, you could edit /etc/zosmf/izudflt.ovr to customize your initial z/OSMF configuration
  - **HSMA210E** - Invokes the izusetup.sh shell script in -config mode
    - This job **must** be run from the target system
  - **HSMA210F** - Verifies the results of the RACF security setup performed previously (via RACFTGT)
    - Only used if your security product is RACF
    - This job **must** be run from the target system
  - **HSMA210G** - Invokes the izusetup.sh shell script in –finish mode which will complete the configuration of the z/OSMF.
    - This job **must** be run from the target system
- Once these jobs are run, you can start IZUANG1 and IZUSVR1, and then (by default) IBMUSER can log on to z/OSMF
  - You then have to add the plug-ins that you want to use, configure their z/OS requisites and optionally authorize additional users

Agenda

- **Overview of z/OS Management Facility V2.1**
- **Ordering and Installing z/OS Management Facility V2.1**
  - Via ServerPac or SMP/E
- **New user setup and configure z/OSMF "base"**
  - Using z/OSMF scripts
  - Using ServerPac jobs
- **Existing user migrating to z/OSMF V2.1**
- **Adding additional "plug-ins"**
  - Configuring the z/OS requisites
  - Configuring z/OSMF to include the "plug-ins"
- **Authorizing users to z/OSMF**

Existing user migrating to z/OSMF V2.1

- **Migrating to a new release of z/OSMF involves the following steps:**
  1. Perform actions you can perform before installing z/OSMF V2.1
     - These are migration actions that you perform on your current (old) system before you install or configure z/OSMF V2.1.
  2. Perform actions you perform before configuring z/OSMF V2.1
     - These are migration actions that you perform after you have SMP/E installed z/OSMF V2.1 on a z/OS V2.1 system, but before you have configured or activated the product.
  3. Configure the new release of z/OSMF, using migrated configuration and override files
     – You must follow all of the phases of the configuration process to set up and verify the new release of z/OSMF on your system.
  4. Prepare for fallback (in case you have to revert back to a prior release of z/OSMF)
  5. Activate z/OSMF V2.1 by starting the z/OSMF server
  6. Perform actions you perform after activating z/OSMF V2.1
     - These are migration actions that you can perform only after you have started the z/OSMF server.
  7. When you are certain that you will not need to fallback to your current (old) release, you can perform the post-migration actions to:
     – Clean-up actions to perform when satisfied with the new release
     – Exploit new capabilities

z/OSMF Migration Details

Step	Description
Step M1: Actions you can perform before installing z/OSMF V2.1	Migrate from Repository mode
Step M2: Actions you perform before configuring z/OSMF V2.1	a. Continue to use ZOSMFAD as a z/OSMF Administrator user ID b. Authorize the z/OSMF server to create PassTickets c. Setting up the z/OSMF started procedures d. Migrating your configuration file and override file
Step M3: Configure the new release of z/OSMF, using migrated configuration and override files	Setup the configuration file Create security definitions Build the executables (run-time files)
Step M4: Actions you can perform after configuring the new release of z/OSMF	a. Prepare for fallback b. Save copies of the prior releases' file systems
Step M5: Activate z/OSMF V2.1 by starting the z/OSMF server	START IZUANG1 START IZUSVR1
Step M6: Actions you perform after activating z/OSMF V2.1	Notify users of the correct URL to use for z/OSMF V2.1

Step M1: Actions you can perform before installing z/OSMF V2.1

- **If you are migrating from z/OSMF V1.13 AND If your current (old) system is currently running z/OSMF V1.13 in Repository Authorization Mode,**
  - You can optionally convert your existing security setup to SAF Authorization Mode before moving to z/OSMF V2.1.
    - Doing so will require you to repeat the steps of the z/OSMF configuration process, supplying your current configuration file as input.
    - The z/OSMF configuration process generates new REXX execs, which your security administrator can use to set up security for z/OSMF and authorize additional users to the product.
    - If more than the default set of user authorizations is required, your security administrator is responsible for converting your existing z/OSMF user authorizations to SAF profiles and groups, for use under SAF authorization mode.
  - If your current (old) system is currently running z/OSMF V1.12, you must convert to SAF Authorization Mode when configuring z/OSMF V2.1 on your system.

Step M2a: Actions you perform before configuring z/OSMF V2.1

- **To continue to use ZOSMFAD as a z/OSMF Administrator user ID**
  - In previous releases of z/OSMF, the configuration process created a special user ID known as the z/OSMF administrator user ID.
    - By default, the user ID was ZOSMFAD.
    - You used this user ID for running configuration scripts and performing administration tasks, such as adding users and working with z/OSMF log files.
  - In z/OSMF V2.1, the configuration process no longer creates, or requires the use of, the administrator user ID.
    - Though z/OSMF retains the concept of an administrator role, you can use *any* existing user ID for this purpose, as long as you define the user ID to the z/OSMF administrator security group (IZUADMIN) and ensure it has the proper authority.
  - If you want to continue using the ZOSMFAD user ID to run the z/OSMF V2.1 configuration scripts, then you must ensure that it has "superuser" authority.
    - See slide 18 for a a superuser authority requirements

Step M2b: Actions you perform before configuring z/OSMF V2.1 …

- **To Authorize the z/OSMF server to create PassTickets**
  - For the **Capacity Provisioning** plug-in, determine whether your installation is using PassTickets to authenticate requests against the CIM server on a remote system.
    - If so, you defined the profile IRRPTAUTH.CFZAPPL.* in the PTKTDATA class.
    - To authorize the z/OSMF server to create PassTickets, grant the z/OSMF started task user ID at least UPDATE access authority to this resource.
    - For example: PERMIT IRRPTAUTH.CFZAPPL.* CLASS(PTKTDATA) ID(IZUSVR) ACCESS(UPDATE) where IZUSVR is the z/OSMF started task user ID.
  - For the **Resource Monitoring** plug-in, determine whether your installation is using PassTickets to authenticate requests against the RMF Distributed Data Server (DDS) on a remote system.
    - If so, you defined the profile IRRPTAUTH.GPMSERVE.* in the PTKTDATA class.
    - To enable PassTicket creation for the z/OSMF server, give the z/OSMF started task user ID at least UPDATE access authority.
    - For example: PERMIT IRRPTAUTH.GPMSERVE.* CLASS(PTKTDATA) ID(IZUSVR) ACCESS(UPDATE) where *IZUSVR* is the z/OSMF started task user ID.

Step M2c: Actions you perform before configuring z/OSMF V2.1 …

- **Setting up the z/OSMF Started Procedures**
  - Ensure that the z/OSMF catalogued procedures reside in the SMP/E defined PROCLIB, as follows:
    - **ServerPac and CustomPac users:**
      - Ensure that SYS1.IBM.PROCLIB (or whatever you renamed it to) resides in the JES PROCLIB concatenation.
      - Or, copy its contents to a data set in the JES PROCLIB concatenation.
    - **CBPDO users:**
      - Ensure that SYS1.PROCLIB (or whatever you renamed it to) resides in the JES PROCLIB concatenation (and is catalogued).
      - Or, copy its contents to a data set in the JES PROCLIB concatenation.
    - Note that these steps are the same as you would do for any SMP/E installed cataloged procedure that is provided with z/OS.
  - Define the started procedures to RACF
    - When you create the new z/OSMF configuration (Step M3), the generated REXX EXEC **izuconfig1.cfg.rexx** contains RACF commands for defining the z/OSMF started procedures to the STARTED class.

Step M2d: Actions you perform before configuring z/OSMF V2.1 …

- **Migrating your configuration file and override file**
  - The **izumigrate.sh** script
    - Migrates your configuration file, and, if specified, your override file from a previous release of z/OSMF to the latest format
    - Retains your current settings when possible.
    - (For any properties that are no longer valid) Omits the properties when creating the updated files.
  - If you choose to migrate an existing override file, understand that:
    - The script processes only the properties that are specified in the override file.
      - It does not add any new properties to the updated override file.
  - The script records the results of the migrate operation in the migration report file.
    - You can review this file to see what settings were changed during the migrate operation, and what new properties are available.

Step M2d: Running the izumigrate.sh script

- **Run the script from**
  - A z/OS V2.1 system that has z/OSMF V2.1 SMP/E installed
  - A user ID with superuser authority
  - In either an OMVS or telnet/rlogin session.
    - You cannot run it from ISHELL
- You can migrate the configuration file and override file together in one invocation of the script. Or, if you prefer, you can migrate these files individually through separate invocations of the script.
- **Syntax**
  - **izumigrate.sh** -file *izuconfig1.cfg* -overridefile *izudflt.ovr*

    Where:
    - *izuconfig1.cfg* identifies the configuration file from a previous release of z/OSMF.
      - This file is expected to reside in the z/OSMF configuration directory <*IZU_CONFIG_DIR*>.
    - *izudflt.ovr* identifies an override file from a previous release of z/OS

Step M2d: izumigrate.sh Output

- As the script runs, it writes log information to the z/OSMF log file directory, which is identified by the IZU_LOGFILE_DIR environment setting for the UNIX shell.
  - By default, this directory is /var/zosmf/configuration/logs/.
- On completion of the izumigrate.sh script, it:
  - Migrates your configuration file and/or override file to the correct format for the new release of z/OSMF.
  - Creates backups of your existing configuration file and/or override file
  - Creates a report file named **izumigration.report**.
    - The report file records the actions that were taken to migrate your configuration and override files—the settings that have been modified, removed, or added between releases.
    - The report file is divided into two sections, one for the configuration file and one for the override file, if applicable.

Step M3: Configure z/OSMF V2.1, using migrated configuration and override files

- **You must follow all of the phases of the configuration process to set up and verify the z/OSMF V2.1 on your system**
  1. **Stage 1 – Configuration**
     - **a. Interactive mode (with an override file)**
       - **izusetup.sh -file *etc/zosmf/izuconfig1*.cfg -config -overridefile /etc/zosmf/izudflt.ovr**
     - **b. Fastpath mode**
     - **c. Interactive mode (without an override file)**
  2. **Stage 2 - Security setup**
     - **Invoke Security REXX EXEC**
       - ***/etc/zosmf*izuconfig1.cfg.rexx**
       - ***/etc/zomf*izuconfig1.cfg.**<z/OSMF Installer USERID>**.rexx**
     - **Verify the RACF Security Setup**
       - **izusetup.sh -file *etc/zosmf/izuconfig1*.cfg –verify racf**
  3. **Stage 3 – Build the executables – deploy the z/OSMF apps**
     - **Complete the setup (deploy, configure, and verify z/OSMF)**
       - **izusetup.sh -file *etc/zosmf/izuconfig1*.cfg -finish**

Step M4a: Prepare to revert back to a prior release

- **Before attempting a fallback, observe the following considerations:**
  - Each new release of z/OSMF adds functions and enhancements that might not be available on an older release, or might not operate in the expected manner.
    - You should not exploit new functions or enhancements on the new release until you are sure that you will NOT fallback to the prior release
  - The configuration process is unique in each release of the product. It is not possible to run the latest configuration scripts on a downlevel release of z/OSMF.
    - Therefore, ensure that you keep copies of the older release's configuration file, and if used, its override file
      - These should have be created by the izumigrate.sh script

Step M4b: Prepare to revert back to a prior release …

- **Reverting to an older release of z/OSMF can be made easier through preparation.**
  - Ensure that you create backup copies of the older release file systems before migrating to the new release. Specifically you must save copies of the following file systems:
    - **z/OSMF data file system**.
      - This is the directory mount point that was specified on the IZU_DATA_DIR variable during the configuration process.
    - **z/OSMF product file system**.
      - Usually this file system is mounted at /usr/lpp/zosmf/V1Rnn.
    - **IBM WebSphere Application Server OEM Edition for z/OS configuration file system**.
      - Usually, this file system is mounted at /zWebSphereOEM/V7R0/config1, but your installation might have specified another location for it.
      - Check the WebSphere response file for variable zConfigHfsName.
    - **IBM WebSphere Application Server OEM Edition for z/OS product file system**.
      - Usually, this file system is mounted at /usr/lpp/zWebSphereOEM/V7R0, but your installation might have specified another location for it.
      - Check the WebSphere response file for variable zSmpePath.

Step M5: Activate the z/OSMF server

- **To start the z/OSMF server manually, you can enter the MVS START command from the operator console.**
  - The START command specifies the member name to start and, optionally, the job name to use, for example:
    - **START IZUANG1**, JOBNAME=*jobname*
    - **START IZUSVR1**, JOBNAME=*jobname*
  - Start the tasks in the following sequence: IZUANG1 followed by IZUSVR1.
    - Otherwise, z/OSMF users might encounter authorization errors later when logging in to the z/OSMF Welcome page.
  - On server start-up, a number of messages are written to the z/OSMF log file, as follows.

    CWWKB0056I INITIALIZATION COMPLETE FOR ANGEL

    BPXM023I (IZUSVR) IZUG400I: The z/OSMF Web application services are initialized.

    +CWWKF0011I: The server zosmfServer is ready to run a smarter planet.
  - Consider having the server start automatically at system IPL time by:
    - Adding the commands to a COMMNDxx PARMLIB member, and
    - Updating BPXPRMxx to mount (or automount) the z/OSMF file systems

Step M6: Actions you perform after activating z/OSMF V2.1

- **Notify users of the correct URL to use for z/OSMF V2.1**
  - When you migrate to z/OSMF V2.1, if you changed port numbers then, the URL used to access the product has changed.
  - Be sure to provide users with the new URL to use for accessing z/OSMF through a web browser.
  - Users can add the URL to the browser bookmarks list.
  - To find the URL for z/OSMF on your system, see message IZUG349I, which was logged when you ran the izusetup.sh script with option -finish during the configuration process.
    - This log file is in the format: <*IZU_LOGFILE_DIR*>/izusetup_finish.*mm.dd.yy.hh.mm.ss.tt*.log where <*IZU_LOGFILE_DIR*> is the log file directory for your installation.
    - By default, this directory is /var/zosmf/configuration/logs/.
  - The URL for the z/OSMF Welcome page has the following format:

    https://hostname:port/zosmf/ or https://hostname/zosmf/ if the default ports are used.

Next Steps: Clean-up actions to perform when satisfied with the new release

- C1 - Cleanup old SAF profile prefix definitions
- C2 - Cleanup old port definitions
- C3 - Cleanup ZOSMFAD owned objects and authorizations from previous releases
- C4 - Cleanup WebSphere constructs from previous releases
- C5 - Cleanup APF Authorization for SYS1.MIGLIB
- C6: Cleanup SURROGAT Class profiles

Step C1: Cleanup old SAF profile prefix definitions

- **If your installation decided to change its SAF definitions from the configuration variable IZU_WAS_PROFILE_PREFIX, default of BBNBASE, then when you are certain that you will not need to fallback to your current (old) release you can remove those profiles**
  - To identify all of the affected profiles in a RACF database, you can use this RACF command: SEARCH ALL CLASS(ZMFAPLA) FILTER(BBNBASE.**)

Step C2: Cleanup old port definitions

- **With the removal of IBM WebSphere Application Server OEM Edition for z/OS in z/OSMF V2.1, you no longer need to reserve the 15 ports used by WAS OEM**
- **When you are certain that you will not need to fallback to your current (old) release you can remove those port definitions.**
  - Note if you are still using the following ports, do NOT delete them
    - 32207 for non-encrypted traffic
    - 32208 for SSL encrypted traffic

Step C3: Cleanup ZOSMFAD owned objects and authorizations from previous releases

- **If you are no longer using ZOSMFAD as a z/OSMF administrator user ID, when you are certain that you will not need to fallback to your current (old) release you can remove it and its associated authorizations.**
  - For a RACF installation, your security administrator can use a utility to identify the user ID objects and authorizations in the RACF database, including the following examples:
    - z/OSMF administrator user ID. By default, this is ZOSMFAD.
    - Directories and files that were created for the ZOSMFAD user ID, such as /home/zosmfad
    - Administrator user ID authorizations to z/OSMF resources, as follows:
      - WebSphere Application Server administrators group (WSCFG1)
      - CIM server administrators group (CFZADMGP)
      - Capacity Provisioning Query Group (CPOQUERY)
      - Capacity Provisioning Control Group (CPOCTRL)
      - Workload Management group (WLMGRP)

Step C4: Cleanup WebSphere constructs from previous releases

- In previous releases of z/OSMF, your installation configured an instance of IBM WebSphere Application Server OEM Edition for z/OS for each instance of z/OSMF.
- This process produced a number of WebSphere constructs on your system, such as configuration files and log files, and the WebSphere servant region user ID.
- In z/OSMF V2.1, these constructs are no longer needed; when you are certain that you will not need to fallback to your current (old) release you can remove them.
- To find the residual constructs, check the directories and files under mount point /zWebSphereOEM/V7R0/config1.
- Also, check for the WebSphere servant region user ID and any associated security authorizations in your security product.
  - In previous releases, this user ID was defined on variable IZU_SERVANT_USERID in your configuration file or override file. By default, the user ID is WSSRU1.

Step C5: Cleanup APF Authorization for SYS1.MIGLIB

- **Beginning in z/OSMF V2.1, the Incident Log task no longer requires that your SYS1.MIGLIB data set be APF-authorized**.
- If no other programs or functions on your system require SYS1.MIGLIB to be APF-authorized, you can remove this authorization when you are certain that you will not need to fallback to your current (old) release
  - Otherwise, leave this authorization in place.
- APF authorizations are defined in the PROGxx member of SYS1.PARMLIB, if your site follows IBM recommendations.
- If you added SYS1.MIGLIB to the APF list for z/OSMF or the Incident Log task, it is recommended that you remove the explicit authorization.
- To do so, locate the appropriate PROGxx member and edit it to remove the APF ADD statement associated with SYS1.MIGLIB.
- For more information about the PROGxx parmlib member, see *z/OS MVS Initialization and Tuning Reference*.

Step C6: Cleanup SURROGAT Class profiles

- When your installation configured z/OSMF V1R12, the z/OSMF configuration process included RACF commands for creating the SURROGAT class profile BBO.SYNC.<*user ID*> for the administration user ID and for any other user IDs you might have authorized.
- When you are certain that you will not need to fallback to your current (old) release you can remove these profiles

Next Steps Exploitation

User authorizations for the Capacity Provisioning task

- Prior to APAR PM74502, the z/OSMF configuration process supported using a generic security profile for the Capacity Provisioning task:
  - <*SAF-prefix*>.ZOSMF.CAPACITY_PROVISIONING.**
- With the installation of the APAR PM74502 or z/OSMF V2.1 z/OSMF now supports specific profiles:
  - <*SAF-prefix*>.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.VIEW
  - <*SAF-prefix*>.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT.**
- If you created the generic profile for the Capacity Provisioning task in a previous release of z/OSMF, when you are certain that you will not need to fallback to your current (old) release you can remove the generic profile

Next Steps Exploitation …

User authorizations for the Workload Management task

- In z/OSMF V1.12 only one authorization level was supported for Workload Management
- When migrating from z/OSMF V1.12 to z/OSMF V2.1, a mapping of authorization levels occurs.
- The default authorization for the Workload Management task in V1R12 is to allow access for the z/OSMF administrator group only.
- In z/OSMF V2.1,
  - the z/OSMF administrator group has access to **all** of the functions in the Workload Management task, and
  - the z/OSMF User group has **View** access only
- After a conversion from z/OSMF V1.12 to z/OSMF V2.1, z/OSMF Administrators have **all** access, and z/OSMF Users have **View** access.
- If this is unacceptable, you can create custom authorizations for z/OSMF users to the appropriate Workload Management SAF profiles.

Agenda

- Overview of z/OS Management Facility V2.1
- Ordering and Installing z/OS Management Facility V2.1
  - Via ServerPac or SMP/E
- New user setup and configure z/OSMF “base”
  - Using z/OSMF scripts
  - Using ServerPac jobs
- Existing user migrating to z/OSMF V2.1
- **Adding additional “plug-ins”**
  - **Configuring the z/OS requisites**
  - Configuring z/OSMF to include the “plug-ins”
- Authorizing users to z/OSMF

Adding z/OSMF Plug-ins

- Your decision on which plug-ins to configure will depend on your installation's desire to use the function, and your readiness to perform the various z/OS system requisite customization associated with each plug-in.
- When planning for z/OSMF, review the system pre-requisites for each plug-in
- To add a plug-in, you will repeat most of the steps you follow to create the initial configuration.
- After a plug-in is configured, you can remove it from z/OSMF only by repeating the configuration process and not selecting the plug-in.

Configure z/OS Prerequisites for z/OSMF Plug-ins

- **Based on your selection of plug-ins, you must complete the associated system prerequisites, as appropriate. The requirements for each plug-in follow.**
  - System prerequisites for the Capacity Provisioning task
  - System prerequisites for the Configuration Assistant task
  - System prerequisites for the Incident Log task
  - System prerequisites for the ISPF task
  - System prerequisites for the Resource Monitoring task
  - System prerequisites for the Software Management task
  - System prerequisites for the Workload Management task

System Prerequisites for Capacity Provisioning

- If you plan to use the Capacity Provisioning task, ensure that the capacity provisioning manager (CPM) is running on the system on which z/OSMF is installed.
  - Ensure that you have an IBM 31-bit SDK for z/OS Java Technology Edition V6 or higher
- **Optional:** Determine whether access to a remote Common Information Model (CIM) server is required. If it is, you will need to do the following:
  - Ensure that users of the Capacity Provisioning task are defined to the Provisioning Manager query security group (by default, the CPOQUERY group).
    - On a system with RACF, you can query the users in a group through the RACF command LISTGRP. For example: LISTGRP CPOQUERY.
  - Ensure that PassTickets are enabled for every user who might require access to the remote CIM server
  - Verify that users are defined in the security management product for your installation
  - Verify that the z/OSMF started task user ID is authorized to generate PassTickets.

  These security definitions are NOT defined as part of the –add process

System Prerequisites for Configuration Assistant

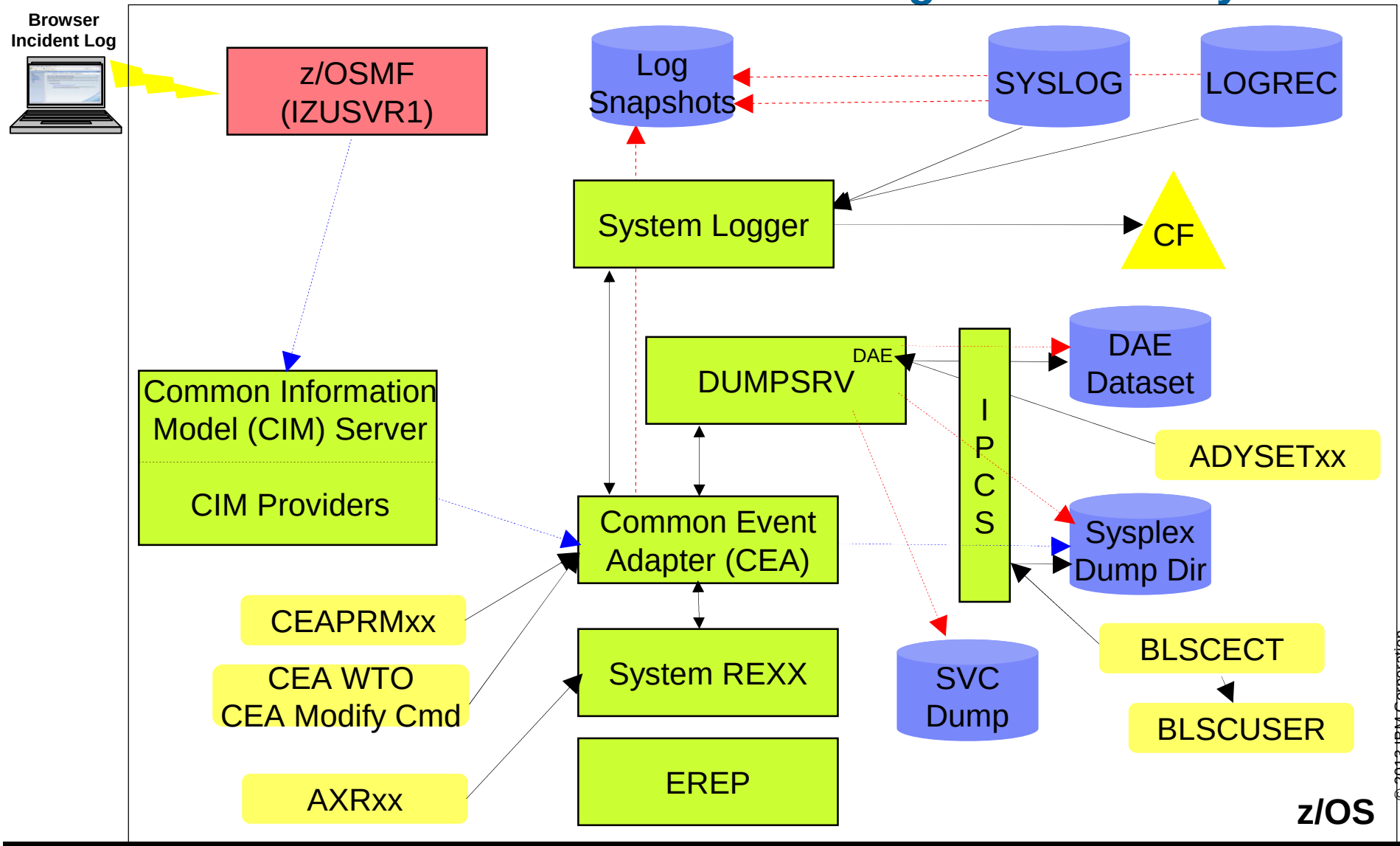
- No system customization is required to enable the Configuration Assistant task.
- **Optional:** If your installation uses the Windows desktop version of Configuration Assistant for z/OS Communications Server, and you want to continue using your existing data in z/OSMF, you can use the following procedure to transfer your backing store files into the z/OSMF environment.
  1. Determine the location of your existing backing store files. The files might reside on your Windows local drive, a LAN drive, or already on z/OS. Use the **File > Properties** menu option from the Windows client to view the file location.
  2. If the backing store files reside on your Windows local drive or LAN drive, copy the files to the z/OS system on which z/OSMF is running. A backing store file is binary and can be placed in a data set or in the z/OS UNIX file system.
  3. From the Configuration Assistant task in z/OSMF, use the **Actions > Tools > Transfer Backing Store file to z/OSMF** option to perform the transfer.
  4. Enter the name and path of your existing backing store files on z/OS. This required value can be a data set or a z/OS UNIX file.
  5. Click **Transfer** to copy the backing store files into z/OSMF.

Note: The Windows version of the Configuration Assistant for z/OS Communications Server is not available to be used with z/OS V2.1

Configure z/OS for Full Incident Log Functionality

- z/OSMF's Incident Log exploits existing best practices for data management for problem determination.
  1. Ensure that the Common Information Model (CIM) server is configured on your system, including security authorizations and file system customization.
  2. Optional: Use of System Logger for SYSLOG (OPERLOG) and LOGREC
  3. Enable error and message log snapshots on the host system, or optionally on a sysplex-wide basis.
  4. Automatic Dump Data Set Allocation
  5. Dump analysis and elimination (DAE) is active and its symptom data set is available
  6. Sysplex Dump Directory (required)
  7. Ensure that the common event adapter (CEA) component is configured on your system, including security authorizations.
  8. Ensure that System REXX (SYSREXX) is set up and active on your system.
  9. If your installation has chosen to rename a dump data set, ensure that the data set name in the sysplex dump directory is correct.
- Note: For more information on these topics see *z/OS MVS Diagnosis Tools and Service Aids* (GA22-7589)

z/OS Infrastructure for Full Incident Log Functionality



Configure z/OS for Full Incident Log Functionality ...

- **(1) CIM server setup**
  - Incident Log task requires that the Common Information Model (CIM) server be setup and running
  - CIM includes jobs to help you perform these tasks (CFZSEC and CFZRCUST). See the chapter on CIM server quick setup and verification in *z/OS Common Information Model User's Guide*, SC33-7998.
  - When configuring Incident Log plug-in or the Workload Management plug-in, the z/OSMF administrator user must have the proper level of access to the CIM server resources
  - Ensure that the CIM server is active on the system before continuing to the –finish step of configuring z/OSMF.
    - You can verify that the CIM server is started by entering a command like the following: D A,CFZCIM

Configure z/OS for Full Incident Log Functionality …

- **(2) Use of System Logger for SYSLOG (OPERLOG) and LOGREC**
  - OPERLOG and LOGREC are important z/OS diagnostic logs that provide a recording of system activity.
  - The OPERLOG and LOGREC log streams capture message and error log information from all systems in the sysplex, and writes that information to log streams managed by the system logger component of z/OS.
  - The log streams should be written to coupling facility structures (in non-monoplex environments) and are ultimately backed up to system managed storage (SMS)-DASD data sets.
  - The OPERLOG and LOGREC log streams have been the strategic method for capturing sysplex-scope log data for many years.
  - In the z/OSMF's Incident Log, the log streams are used to automate the gathering of diagnostic data (log snapshots) associated with an SVC dump.
  - Sample jobs are documented in the z/OSMF Configuration Guide.
  - Additional information documented in the August 2009 Hot Topics Newsletter

Notes:

1. Recommended for multi-system Parallel Sysplex environments
2. As of V1.12, SYSLOG and LOGREC datasets can be used instead to capture snapshots on DASD shared between the systems.

Configure z/OS for Full Incident Log Functionality …

- **(4) Automatic Dump Data Set Allocation**
  - SVC dump processing supports automatic allocation of dump data sets at the time the system writes the dump to DASD. Automatically allocated dumps will be written using the system-determined block size. The dump data sets can be allocated as SMS-managed or non-SMS-managed, depending on the VOLSER or SMS classes defined on the DUMPDS ADD command. When the system captures a dump, it allocates a data set of the correct size from the resources you specify.
    - Using Extended Format Sequential data sets, the maximum size of the dump can exceed the size allowed for non-SMS managed data sets.
    - If automatic allocation fails, pre-allocated dump data sets are used. If no pre-allocated SYS1.DUMPnn data sets are available, message IEA793A is issued, and the dump remains in virtual storage. SVC Dump periodically retries both automatic allocation and writing to a pre-allocated dump dataset until successful or until the captured dump is deleted either by operator intervention or by the expiration of the CHNGDUMP MSGTIME parameter governing message IEA793A.
      - If you set the MSGTIME value to 0, the system will not issue the message, and it deletes the captured dump immediately.
  - If you rename the dump data set, or copy it to another data set, you must include a batch job to update the dump data set name in the sysplex dump directory.
    - Doing so will allow Incident prepare and send to locate the dump.
    - See the z/OSMF Configuration Guide for more info.
  - Instructions on setting up automatic dump data set allocation is documented in the z/OSMF Configuration Guide.

Configure z/OS for Full Incident Log Functionality …

- **(5) Dump analysis and elimination (DAE)**
  - –Dump analysis and elimination (DAE) allows an installation to suppress SVC dumps and SYSMDUMP ABEND dumps that are not needed because they duplicate previously written dumps. To identify the cause of previous and requested dumps, DAE uses symptom strings, which contain data that describes a problem. DAE stores these symptom strings in a DAE data set that you provide.
  - –You can use the DAE data set in a single-system environment, or the systems in a sysplex can share a single DAE data set.
    - IBM suggests that you provide a name other than SYS1.DAE for the DAE data set to be shared in the sysplex.
  - –z/OSMF uses a shared DAE data set to allow the user to enable future dumps that occur on any system in the sysplex to be captured (not suppressed)
  - –Instructions on setting up the a shared DAE environment is documented in the z/OSMF Configuration Guide.

Configure z/OS for Full Incident Log Functionality …

- **(6) Sysplex Dump Directory**
  - The sysplex dump directory describes the SVC dumps generated by a sysplex in a central, compact, and manageable place. If you have write access, you can add source descriptions for other unformatted dumps that IPCS can format and for trace data sets.
  - When setting up the sysplex dump directory, arrange for all systems in the sysplex to share it:
    - Use the default name of SYS1.DDIR for the sysplex dump directory or specify the same name for it in the SYSDDIR statement in the BLSCUSER PARMLIB member.
    - Place the data set for the sysplex dump directory on a DASD shared by all systems in the sysplex.
    - When a system that has access to a sysplex dump directory generates an SVC dump, the system automatically records the source description for it in the sysplex dump directory. IPCS adds the source description without initializing the dump, which takes time.
  - Authorized users can access the sysplex dump directory and edit it.
  - Do not access the sysplex dump directory via a ISPF IPCS session
    - Doing so will lockout DUMPSRV and CEA, resulting in dumps not being recorded in the directory, and not appearing in the Incident Log summary
  - z/OSMF Incident Log uses the sysplex dump directory to get the dump data set name and display Summary and Detail information of incidents
  - Instructions on setting up the sysplex dump directory is documented in the z/OSMF Configuration Guide.

Configure z/OS for Full Incident Log Functionality …

(7) Customizing CEA

- Common event adapter (CEA) is a component of the BCP that provides the ability to deliver z/OS events to C-language clients, such as the z/OS CIM server. A CEA address space is started automatically during initialization of every z/OS system.
- **CEA has two modes of operation:**
  - *Full function mode*. In this mode, both internal z/OS components and clients such as CIM providers can use CEA indication functions.
  - *Minimum mode*. In this mode, only internal z/OS components can use CEA indication functions.
- **Incident Log requires CEA in full function mode.**
- **To start CEA in full function mode, perform the following customization:**
  - Define user ID CEA to the security product
    - The CEA sample job CEASEC can be used as a model
  - Give user ID CEA read access to the profile protecting SYS1.PARMLIB:
  - The user ID CEA needs write and execute access to the z/OS UNIX directory, /SYSTEM/var
- **If CEA is running in minimum mode, you can change to full function mode by:**
  - Making the security definitions above,
  - Stopping CEA (P CEA), and restarting it (S CEA).
- **Other customization that you might have to perform for CEA is the following:**
  - If your system will run with multilevel security, allow CEA to perform multilevel security file accesses you'll need additional security definitions
  - If your MAXCAD setting in PARMLIB member IEASYS*xx* is inadequate to accommodate the data space created by CEA, raise the setting.

z/OS Functionality for Incident Log - Summary

z/OS Function	z/OSMF Incident Log capability if enabled	z/OSMF Incident Log capability if NOT enabled
Sysplex Dump Directory	z/OSMF can display summary and details of incidents	None – function required
OPERLOG and LOGREC use of System Logger	Log snapshots are gathered for the entire sysplex	Log snapshots gathered for the specific system
Shared dump analysis and elimination (DAE)	z/OSMF can make DAE let future dumps be captured on any system in the sysplex	z/OSMF can NOT make DAE let future dumps be captured on other systems in the sysplex
Automatic Dump Data Set Allocation	Dump included in diagnostic data gathered and sent	Dump NOT included in diagnostic data gathered and sent[1]
AMATERSE program is enabled	Dump included in diagnostic data gathered and sent	Can NOT prepare or send any diagnostic data
CIM, CEA, and SYSREXX enabled and active	z/OSMF can display incidents	None – function required
Problem Documentation Upload Utility	Supports parallel encrypted FTP to IBM[2]	Dump not encrypted nor broken into multiple data sets
Keep IBM default name in IEAVTSEL - Post Dump Exit	z/OSMF can display summary and details of incidents	None – function required

1 – Depending on how you archive and reuse your dumps, some capabilities may exist to send dumps as part of diagnostic data

2 – z/OS V1.12 requires the Problem Documentation Upload Utility to be downloaded and installed. In z/OS V1.13 and z/OSMF V2.1 the Problem Documentation Upload Utility is included

System Prerequisites for the ISPF Plug-in

- **Ensure that the TRUSTED attribute is assigned to the common event adapter (CEA) started task, if you have not done so already, to allow the CEA address space to access or create any resource it needs.**
- **To use the ISPF task, a user should be an existing TSO/E user with a valid, non-expired password.**
- **For each user of the ISPF task, you must ensure that the corresponding user ID:**
  - Is authorized to TSO/E and has a valid password
  - Is authorized to a valid logon procedure TSO/E account number
  - Is authorized to the JES spool. This authorization allows the user to use various functions in TSO/E, such as the SUBMIT, STATUS, TRANSMIT, and RECEIVE commands, and to access the SYSOUT data sets through the command TSO/E OUTPUT command.
  - Has an OMVS segment defined, which allows for access to z/OSMF
  - Has a home directory defined, which is required for z/OSMF.
- **By default, the ISPF task is setup to use the logon procedure IKJACCNT, which is supplied by IBM.**
  - A user can select to use a different logon procedure, as long as the user's logon procedure is properly configured for ISPF.
- **Some TSO/E users require the use of multiple ISPF sessions (this is different than having split screens, which is also allowed). If you plan to allow the use of multiple ISPF sessions, the user's logon procedure must be configured to allow profile sharing.**
  - This option avoids enqueue lock outs and loss of profile updates when the same profile data set is used for concurrent ISPF sessions.
  - With profile sharing enabled, the user's logon procedure is required to allocate ISPF profile data sets with the disposition SHARED, rather than NEW, OLD, or MOD, and the data sets must already exist. Or, these data sets must be temporary data sets.

System Prerequisites - Resource Monitoring Task

- **Enable the optional priced feature, Resource Measurement Facility (RMF), on one of the systems in your enterprise.**
- **For data collection and monitoring of your systems, ensure that the RMF distributed data server (DDS) is active on one of the systems in your sysplex.**
  - To monitor several sysplexes, ensure that a DDS is running on one system in each sysplex.
  - You can use the following command to check for the existence of any GPMSERVE address spaces in your sysplex:
    - ROUTE *ALL,D A,GPMSERVE
    - ROUTE *ALL,D A,GPM*
  - For information about setting up the DDS server, see *z/OS RMF User's Guide*.
- **Determine whether the RMF Distributed Data Server (DDS) on the target system is configured to require authentication.**
  - If so, you must ensure that the PassTicket is set up properly. Also, you must verify that users are defined in the security management product for your installation, and that the z/OSMF started task user ID is authorized to generate PassTickets.

System Prerequisites - Resource Monitoring Task …

1. Activate the security class PTKTDATA, if this action is not already done.
   - SETROPTS CLASSACT(PTKTDATA)
   - SETROPTS RACLIST(PTKTDATA) GENERIC(PTKTDATA)
2. Define the profile GPMSERVE for the DDS in the PTKTDATA class and associate a secret secured signon key with the profile. The key must be the same on both the system on which the PassTicket is to be generated (the z/OSMF system) and the system on which the PassTicket is to be verified (the DDS system).
   - RDEFINE PTKTDATA GPMSERVE SSIGNON([KEYENCRYPTED|KEYMASKED](*key*))
   - SETROPTS RACLIST(PTKTDATA) REFRESH
     - where *key* is a user-supplied 16-digit value used to generate the PassTicket. You can specify a value of your choice. Valid characters are 0 - 9 and A - F.
3. To enable PassTicket creation for users, define the profile IRRPTAUTH.GPMSERVE.* in the PTKTDATA class, and set the universal access authority to NONE. You can do enable PassTicket creation for either for all user IDs or for a specific user ID, as shown in the examples that follow.
   - Example (for all user IDs):
   - Example (for a specific user ID):
     - RDEFINE PTKTDATA IRRPTAUTH.GPMSERVE.* UACC(NONE)
     - RDEFINE PTKTDATA IRRPTAUTH.GPMSERVE.specific_dds_login_userid UACC(NONE)
4. Grant the z/OSMF product permission to generate PassTickets for GPMSERVE.
   - Example (for all user IDs):
     - PERMIT IRRPTAUTH.GPMSERVE.* CLASS(PTKTDATA) ID(*passticket_creator_userid*) ACCESS(UPDATE)
   - Example (for a specific user ID):
     - PERMIT IRRPTAUTH.GPMSERVE.specific_dds_login_userid CLASS(PTKTDATA) ID(*passticket_creator_userid*) ACCESS(UPDATE)
       - where *passticket_creator_userid* is the user ID of the z/OSMF started task user ID. By default, this is IZUSVR.
5. Activate the changes, for example: SETROPTS RACLIST(PTKTDATA) REFRESH

Note: If you use RMF XP, the RACF profile name for the RMF XP DDS is GPM4CIM. Use this profile name instead of GPMSERVE when you complete Steps 2 through 4 in the above procedure

System Prerequisites for the Software Management

- **No system customization is required to enable the Deployment task.**
- **Optional: If you want to manage the priority of work performed by the Deployment task, your installation can define a Workload Manager transaction class to manage the execution of long-running work. This step is recommended.**
  - Using the z/OSMF Workload Management task or the WLM ISPF Administration Application, add a classification rule for subsystem CB (Component Broker) to your WLM service definition.
    - Specify qualifier type transaction class (TC) and qualifier name IZUGWORK for the classification rule and assign a service class with a goal of either discretionary or low velocity.
    - The subject service class should not have multiple periods and should not have a response time goal.
  - Create a report class specific for the IZUGWORK transaction class, for example, RIZUGWRK, and assign it to the classification rule, so that you can obtain a separate report on the actual usage of the Deployment task long-running work.
  - If your installation is running a System z Application Assist Processor (zAAP), and if IFAHONORPRIORITY is set to YES in the IEAOPTxx member of PARMLIB, discretionary work is not permitted to use a general central processor (GCP).
    - If this processing style is desired, use a discretionary goal.
    - To allow the work to cross-over to a GCP if the zAAP capacity is exhausted, use a low velocity goal.

  For more information on WLM, see *z/OS MVS Planning Workload Management*

System Prerequisites for the Software Management …

- **The Software Management task:**
  - Allows all users of the task to access deployment objects. Optionally, your installation can further restrict these authorizations.
    - You can use your security product to control access to the task and to create more granular authorizations, such as restricting access to an object or an action.
    - Access to the Software Management task and its objects are controlled through the following default resource profiles, which are defined in the ZMFAPLA class:
- **<safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.****
    - o <safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.DATA.**
    - o <safPrefix>.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.PRODUCT_INFO_FILE.*
    - With the default access authorities, z/OSMF users and administrators are allowed to perform all actions for all software instances, deployments, categories, and global zones, and only z/OSMF administrators are allowed to retrieve information from product information files.
  - 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

System Prerequisites for the Workload Management Task

- The Workload Management task requires that the Common Information Model (CIM) server is configured on your system, including security authorizations and file system customization.
  - As previously described
- Ensure that module BLDUXTID in SYS1.MIGLIB is program controlled. For example, in a RACF system, you can use the following commands to ensure that a library is program controlled:
  - RDEFINE PROGRAM BLSUXTID
  - RALT PROGRAM BLSUXTID ADDMEM('SYS1.MIGLIB'/'******'/NOPADCHK) UACC(READ)
  - SETROPTS WHEN(PROGRAM) REFRESH

  Note: This step is performed in the CIM provided job CFZSEC. See the chapter on customizing the security for the CIM server in *z/OS Common Information Model User's Guide*.

System Prerequisites for the Workload Management Task …

- **Authorizing users to the MVSADMIN.WLM.POLICY profile**
  - Users of the Workload Management task require UPDATE access to resources that are protected by the profile MVSADMIN.WLM.POLICY in class FACILITY. If you run the CFZSEC job when setting up the Common Information Model (CIM) server for z/OSMF, all users who are authorized for the CIM server are automatically authorized for this profile. If this set of authorizations is acceptable in your environment, no further steps are needed.
    - If not all CIM server users should have access to the MVSADMIN.WLM.POLICY profile, however, you must perform additional steps to avoid creating unwanted authorizations.
- **MVSADMIN.WLM.POLICY profile**
  - The Workload Management task performs periodic queries of WLM on the z/OS host system. To perform the queries, the Workload Management task uses the z/OSMF started task user ID. Therefore, you must ensure that the z/OSMF started task user ID has READ access to the profile MVSADMIN.WLM.POLICY and authorization to the CIM server. To manually authorize the z/OSMF started task user ID for the MVSADMIN.WLM.POLICY profile and the CIM server, complete the following steps:
    1. Grant the z/OSMF started task user ID read access to the profile MVSADMIN.WLM.POLICY.
    2. Connect the z/OSMF started task user ID to the CIM user group. By default, the CIM user group is CFZUSRGP, as defined on variable IZU_CIM_USER_GROUP_NAME in your override file.
    3. Ensure that the user ID under which the CIM server is running has SURROGAT access for the z/OSMF started task user ID. If a generic BPX.SRV.** profile is already authorized in the SURROGAT class (for example, because you ran the CFZSEC job when setting up the CIM server), no additional action is required.
       - Otherwise, define a discrete profile for the z/OSMF started task user ID and authorize it. If necessary, refresh the SURROGAT class.

System Prerequisites for the Workload Management Task ...

- **Using authorization levels for the Workload Management task**
  - Using predefined authorization levels, your installation can authorize users to specific functions within the Workload Management task.
  - The Workload Management task supports the following authorization levels:
    - **View** - This authorization level allows the user to invoke the Workload Management task, and view service definitions, service policies, and WLM status.
    - **Install** - This authorization level allows the user to install service definitions and activate service policies. A user authorized for this level also must be authorized for the View level to invoke the Workload Management task.
    - **Modify** - This authorization level allows a user to modify service definitions and to import service definitions from host data sets or local workstation files into z/OSMF. A user authorized for this level also must be authorized for the View level to invoke the Workload Management task.
  - To install service definitions and activate service policies, the user must also be authorized for the Install level. By default, the z/OSMF administrators security group is authorized for the View, Install, and Modify functions, which is equivalent to a WLM policy administrator.
- **Using a browser with WLM service definitions**
  - Users who plan to use the Internet Explorer browser to work with WLM service definitions should ensure that the browser is enabled for automatic prompting for file downloads.
    - This setting prevents the file download blocker from being invoked when the user downloads service definitions to the workstation. Otherwise, if automatic prompting is disabled (the default setting), the download blocker prompts the user to accept these file downloads, causing the browser session to be reloaded and the active tabs to be closed. Users can avoid this disruption by enabling automatic prompting for file downloads.

Agenda

- Overview of z/OS Management Facility V2.1
- Ordering and Installing z/OS Management Facility V2.1
  - Via ServerPac or SMP/E
- New user setup and configure z/OSMF “base”
  - Using z/OSMF scripts
  - Using ServerPac jobs
- Existing user migrating to z/OSMF V2.1
- **Adding additional “plug-ins”**
  - Configuring the z/OS requisites
  - **Configuring z/OSMF to include the “plug-ins”**
- Authorizing users to z/OSMF

Adding z/OSMF Plug-ins - Prompts and Override File

- **Use the worksheets for each plug-in as a guide for planning your input to the izusetup.sh –config –add script.**
  - Each worksheet entry includes a description of the input variable, its default value (if any), and a space to record your own value in case you do not want to use the default
- **If you are using an override file**
  - If you used an override file when configuring z/OSMF,
    - You can specify the new plug-ins as properties in your existing override file.
      - You would mark the plug-ins to be added with the character A.
      - You would add any additional plug-in specific parameters whose default you want to change.
        - » Some variables are initially set to a value of “NO.DEFAULT.VALUE”. These variables must be updated in the override file before invoking the **izusetup.sh –add** script to perform the configuration.
    - Alternatively, you can use a new override file to indentify the plug-ins that you want to add and plug-in specific parameters that you want to change.
      - Please note that if you run this script operation more than once, only your most recent plug-in selections are included in your configuration. Any non-selected plug-ins are removed. Therefore,
        - » Specify the complete set of desired plug-ins each time you invoke -add
  - You can respond to the script prompts to change any of the values in the override file.
- If you choose **NOT** to use an override file you can respond to the script prompts to make your plug-in selections and change any of the default values.

Step A1: Configure Additional z/OSMF Plug-ins

- The **izusetup.sh –config –add** script uses the input you supply, based on your environment and the z/OSMF tasks that you plan to configure.
- **Regardless of which mode you use, the script does the following:**
  - Creates/replaces a configuration file as output.
  - As an aid to your security administrator, the script creates a set of REXX EXEC programs with sample RACF commands that your security administrator can review and run. The exec name is a concatenation of your configuration file name, the plug-ins you selected, and ".rexx".
    - If you use "izuconfig1.cfg" as your configuration file name, for example, and add two plug-ins, the exec is created as:
      - izuconfig1.cfg.add.<*plug-in-1*>.<*plug-in-2*>.rexx
- **Sample command:**
  - izusetup.sh -file /etc/zosmf/izuconfig1.cfg -config -overridefile /etc/zosmf/izudflt.ovr -add

Use the same configuration file name

Step A2: Run the Security Commands

- **This EXEC is run by your installation's security administrator.**
- **Prior to running the REXX EXEC review the RACF commands and comments making any necessary changes**
  - If you provided the proper User ID and Group names during the configuration process, you shouldn't have to edit those commands
  - If you need to make any changes, copy the REXX EXEC to another file and make changes to the copied file

The name of the file is based on what plug-ins are being added

Captures command output in a file

- **Sample invocation of REXX EXEC**
  - From the /etc/zosmf/ directory
    - ./izuconfig1.cfg.add.IL.CA.WLM.RMF.CP.WISPF.DM.rexx | tee /var/zosmf/configuration/logs/izuconfig1.cfg.add.plugins.output

Step A3: Verify the RACF Security Setup

- **This exec is run by your installation's security administrator.**
- The **izusetup.sh** script verifies the RACF security setup actions that were performed in the previous steps.
- If your installation uses a security management product other than RACF, do not perform this step. Instead, take the appropriate steps to verify your security setup.
- **Sample command**
  - izusetup.sh -file /etc/zosmf/izuconfig1.cfg -verify racf

Same configuration file as prior command

- On completion, the script creates a report file called **izuracfverify.report**, which by default is stored in the following location:
  - /var/zosmf/configuration/logs/izuracfverify.report

Step A4: Complete the Setup

- **The script is intended to be run by the z/OSMF Installer (Superuser)**
- As it runs, the script writes messages to the script log file.
- **Sample command:**
  - izusetup.sh -file /etc/zosmf/izuconfig1.cfg -finish -add

Same configuration file as prior command

Agenda

- **Overview of z/OS Management Facility V2.1**
- **Ordering and Installing z/OS Management Facility V2.1**
  - Via ServerPac or SMP/E
- **New user setup and configure z/OSMF "base"**
  - Using z/OSMF scripts
  - Using ServerPac jobs
- **Existing user migrating to z/OSMF V2.1**
- **Adding additional "plug-ins"**
  - Configuring the z/OS requisites
  - Configuring z/OSMF to include the "plug-ins"
- **Authorizing users to z/OSMF**

Authorizing existing z/OS users to z/OSMF

- To authorize existing z/OS user ID to the z/OS components required for z/OSMF operations you need to:
  1. Run the **izuauthuser.sh** script
  2. Have your security administrator run the generated ***izuconfig1.USERID*.rexx** REXX EXEC
     - If your installation uses a security management product other than RACF, you can run this script, but you security administrator must create equivalent commands for your security product.

Running the izuauthuser script

- The **izuauthuser.sh script** creates a REXX EXEC (*izuconfig1*.*USERID*.rexx) with RACF commands for authorizing a user ID to one of the predefined z/OSMF roles.
  - During the z/OSMF configuration process, your security administrator created security groups for the roles. Each group is permitted to a default set of z/OSMF resources (tasks and links) appropriate for the role. By default:
    - **z/OSMF User** group is permitted to all z/OSMF application tasks and links (although some function is limited)
    - **z/OSMF Administrator** group is permitted to all z/OSMF tasks and links (full function), plus the ability to define/update z/OSMF links and settings
    - **z/OSMF Security Administrator** group is permitted to the Workflows task.
- If you add more plug-ins to your z/OSMF configuration later, you must re-run the izuauthuser.sh script and the generated REXX EXEC.
  - Note that doing so can result in an "overlap" of RACF commands, for the previous set of plug-ins and the newly added plug-ins. Your security administrator should handle these situations accordingly.

Running the izuauthuser script …

- This EXEC is run by your z/OSMF installer's ID.
- Script syntax
  - izuauthuser.sh -file izuconfig1.cfg -userid *userid* -role *role*

  Where:
  - izuconfig1.cfg is the configuration file that you created previously in.
  - *userid* is the existing user ID for which the RACF commands are to be created.
  - *role* is the z/OSMF role to which the user is to be assigned. The possible values for *role* are, as follows:
    - user Authorizes the user ID to the role z/OSMF user
    - admin Authorizes the user ID to the role z/OSMF administrator
    - security_admin Authorizes the user ID to the role z/OS Security Administrator.
- Sample Command
  - In the following example, the izuauthuser.sh script is used to authorize the user ID GDAYNES to the role z/OSMF administrator:
    - izuauthuser.sh -file izuconfig1.cfg -userid gdaynes -role *admin*

Running the *izuconfig1.USERID*.rexx REXX EXEC

- This EXEC is run by your installation's security administrator.
- This exec contains sample RACF commands for authorizing a user ID to the z/OS components used in z/OSMF operations.
- Prior to running the REXX EXEC review the RACF commands and comments making any necessary changes
  - If you need to make any changes, copy the REXX EXEC to another file and make changes to the copied file
- Sample invocation of REXX EXEC
  - From the /etc/zosmf/ directory
    - ./izuconfig1.cfg.USERID.rexx | tee /var/zosmf/configuration/logs/izuconfig1.cfg.USERID.rexx.output

    Where
    - USERID is the existing z/OS user id that you want to authorize to z/OSMF

Summary (1 of 2)

- **Overview of z/OS Management Facility V2.1**
- **Ordering and Installing z/OS Management Facility V2.1**
  - Via ServerPac or SMP/E
- **New user setup and configure z/OSMF "base"**
  - Using z/OSMF scripts
  - Using ServerPac jobs
- **Existing user migrating to z/OSMF V2.1**
- **Adding additional "plug-ins"**
  - Configuring the z/OS requisites
  - Configuring z/OSMF to include the "plug-ins"
- **Authorizing users to z/OSMF**

Session zSO53: Using z/OSMF Hands on Lab
z/OSMF Software Management Lab
Thurs 10:45 D. Manuel I

Summary (2 of 2)

- The recommended sequence for configuring z/OSMF has changed.
  - The new recommended approach for a new or first time installation is now a two-phase sequence:
    1. Create a base configuration (that is, with no optional plug-ins selected)
    2. Add plug-ins, users, and host system customizations later, when you choose to do so.
- The z/OSMF Configuration Guide has been restructured to reflect this change.

Backup

Additional Information

- **z/OS Management Facility website**
  - http://ibm.com/systems/z/os/zos/zosmf/
- **IBM z/OS Management Facility education modules in IBM Education Assistant**
  - http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r0/index.jsp
    - **Scroll down to z/OS Management Facility**
- **IBM z/OS Management Facility Configuration Guide (SA38-0657)**
- **Program Directory for z/OS Management Facility (GI11-9847)**
- **z/OS Management Facility V2.1 Resource Requirements**
  - http://www-.ibm.com/support/techdocs/atsmastr.nsf/Web/WhitePapers

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

IBM*	RACF*	ServerPac*	WebSphere*
IBM (logo)	Resource Measurement Facility	System z*	z/OS*
MVS	RMF	UNIX*	

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Firefox is a trademark of Mozilla Foundation

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license there from.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Internet Explorer is a trademark of Microsoft Corp

InfiniBand is a trademark and service mark of the InfiniBand Trade Association.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

See url http://www.ibm.com/legal/copytrade.shtml for a list of IBM trademarks.

z/OSMF Default Directory Names and Descriptions …

Directory	Permission bits	Description
/usr/lpp/zosmf/V2R1	**755**	**Default read-only mount point for product file system**
/etc/zosmf	**755**	**Default location of the read-write mount point used for the z/OSMF configuration file, override file, and security REXX EXECs.**
/var/zosmf/configuration/logs/	**755**	**Location of the configuration log files**
/var/zosmf/data	**755**	**Default location of the read-write mount point used for the persistence data file system**
/var/zosmf/data/logs/	**755**	**Location of the run-time log files**
/tmp/	**755**	**Location of the temporary directory to be used for sending z/OS UNIX file attachments through FTP when using Incident Log. The size will depend on what files are to be sent as attachments.**

Setting the z/OSMF environment variables for your shell session

To modify the environment variables for your shell session, follow these steps:

1. Copy the IBM-supplied environment variables file to a read/write directory.
   - Copy the file to a location that will be accessible from your shell session, such as the z/OSMF configuration directory /etc/zosmf.
2. Modify the existing export commands with new values, as needed.

```
# Default value for the configuration directory
export IZU_CONFIG_DIR=/etc/zosmf
#
# Default value for the logfile directory
export IZU_LOGFILE_DIR=/var/zosmf/configuration/logs
#
# Default value for the product binaries
export IZU_CODE_ROOT=/usr/lpp/zosmf/V2R1
#
# Setup PATH so the zOSMF binaries are accessible.
export PATH=.:/usr/lpp/zosmf/V2R1/bin:$PATH
#
# For problems with out of memory starting jvms
export _BPX_SHAREAS=NO
#
# Default value for the Java product directory
export JAVA_HOME=/usr/lpp/java/J7.0_64
#
# Default value for the CIM WBEM root directory
export PEGASUS_HOME=/usr/lpp/wbem
```

3. Make your changes effective.
   - Before running the z/OSMF shell scripts, export the variable IZU_ENV_FILE, setting it to the location of this file, or add it to the .profile for the user ID that you use to run the scripts. The following export command example assumes that you have placed the environment variables file in the configuration directory and named it izu_env.sh:
     - export IZU_ENV_FILE=/etc/zosmf/izu_env.sh

Verifying your workstation with the environment checker

- z/OSMF includes an environment checker tool to help you verify these settings.
- The environment checker tool inspects your web browser and workstation operating system for compliance with z/OSMF requirements and recommended settings.
- Before running the tool **c**heck to ensure that your workstation is set up correctly for z/OSMF and ensure that your browser is enabled for JavaScript.
- To run the tool, do the following:
  1. Open a web browser to the environment checker tool:
     - **https://hostname:port/zosmf/IzuUICommon/environment.jsp**

     where:
     - ***hostname*** is the hostname or IP address of the system on which z/OSMF is installed
     - ***port*** is the secure application port (not needed if the default secure port is used).
     - To find the hostname and port, see the link for z/OSMF in message IZUG349I. This message was written to the log file that was created when you ran the izusetup.sh script with the -finish option.
  2. Follow the instructions for your browser in the online help for the tool.
  3. Understand the results of the environment checker
     - For the steps to resolve a problem, see the appropriate entry in the tool's online help.
     - After updating a setting, use the browser reload button to run the environment checker again.
     - Repeat this process until you have resolved all of the errors and warnings.

IBM z/OS Management Facility - Environment Checker

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

Environment Option	Settings as of 2013-08-02T14:55:28.373Z	Requirements
JavaScript	JavaScript enabled	Enable JavaScript
Cookies	Cookies enabled	At a minimum, enable cookies for the z/OSMF server site
Pop-up Windows	Pop-up windows enabled	At a minimum, allow pop-up windows from the z/OSMF server site
Frames	Frames enabled	Enable frames
Screen Resolution	1440 by 810	Minimum screen resolution of 1024 by 768
Browser Content Dimensions	1425 by 659	Minimum browser content dimensions of 800 by 600
Browser Name and Version Browser User-Agent value	Firefox 17.0 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:17.0) Gecko/20100101 Firefox/17.0	Supported browsers by operating system:
Operating System	Microsoft Windows 7	Microsoft Windows XP Professional (32-bit) and Microsoft Windows 7 Professional (32-bit and 64-bit)
Add-ons	No problem add-ons detected	The Firebug add-on can affect browser performance.
Plug-ins	Shockwave Flash Adobe Acrobat Adobe Acrobat Adobe Acrobat IBM Developer Kit for Windows,Java,1.6.0 iTunes Application Detector Silverlight Plug-In ActiveTouch General Plugin Container IBM 821 Conference Plugin NVIDIA 3D VISION NVIDIA 3D Vision IE Tab Plug-in IBM GLOBAL PRINT DocuCom PDF Plus DocuCom PDF Plus NPCIG.dll Microsoft® Windows Media Player Firefox Plugin Microsoft Office 2003 IBM BluePages Add to NAB 1.1	Some plug-ins can affect browser performance.
z/OSMF Login ID	guest	An unauthenticated user will be "guest"
z/OSMF Version	Version Number: 2 Release Number: 1 Build Number: pm89803	z/OSMF version

Browser	Microsoft Windows XP Professional (32-bit)	Microsoft Windows 7 Professional (32-bit)	Microsoft Windows 7 Professional (64-bit)
Firefox ESR 17.0.x	Yes	Yes	Yes
Internet Explorer 8 (32-bit)	Yes	Yes	Yes
Internet Explorer 8 (64-bit)[1]	No	No	Yes
Internet Explorer 9 (32-bit)	No	Yes	Yes
Internet Explorer 9 (64-bit)[1]	No	No	Yes

[1]Requires Microsoft Windows 7 Professional (64-bit).

Configuring for High Availability in a Sysplex

- If you plan to use z/OSMF in a multi-system environment within a sysplex, the decisions you make during the first-time configuration can help to simplify the management of z/OSMF in a multi-system environment later.
- To do so, you must deploy z/OSMF in such a way that the product can be started from any system in the sysplex.
- By default, the configuration process creates the product directories as system-specific, based on the non-sharable mount points /etc and /var.
- For a multi-system environment, you can specify an alternative mount point for these directories, such as /sharedapps.
  - Doing so will help to simplify management in a multi-system environment later, for such operations as switchover and cloning.

Directory	Variable name	Setting for a single-system environment (default)	Suggested setting for a multi-system environment
z/OSMF data file system	IZU_DATA_DIR	/var/zosmf/data	/sharedapps/zosmf/data
z/OSMF configuration directory	IZU_CONFIG_DIR	/etc/zosmf	/sharedapps/zosmf/config
z/OSMF log directory	IZU_LOGFILE_DIR	/var/zosmf/configuration/logs	/sharedapps/zosmf/configuration/logs
Home directory for the z/OSMF started task	IZU_STARTED_TASK_USERID_HOME	/var/zosmf/data/home/izusvr	/sharedapps/zosmf/data/home/izusvr

Configuring for High Availability in a Sysplex ...

- If your initial instance of z/OSMF uses a **shared** data file system (that is, with a shared mount point and volume) and is read/write accessible from other systems in the sysplex, you can simply restart the z/OSMF server on another system.
  - If your initial instance of z/OSMF uses a non-shared data file system (one that is only read/write accessible from only the host z/OS system), switchover from the primary instance of z/OSMF to the backup will require that you unmount the data file system on the primary host z/OS system and mount it on the backup system.
- If you use a **shared** security database, this procedure is further simplified because the backup instance can use the same user IDs and groups as your primary instance.
- When using z/OSMF in a multi-system environment, each instance of z/OSMF must have a unique host name.
  - As part of the z/OSMF configuration process, you define a host name for your configuration.
    - You can specify an installation-specific value, or accept the default, @HOSTNAME, which instructs z/OSMF to do a host name lookup on the system.
  - You can either modify update the bootstrap.template file to substitute one or more system symbols in the host name value or you can use the z/OS Communications Server dynamic VIPA (DVIPA) function to create a DVIPA address for your sysplex, and use the DVIPA address as the z/OSMF host name.
    - Using the DVIPA approach allows users to connect to z/OSMF using the same IP address, regardless of which system is running z/OSMF.
      - In a multiple sysplex environment, you might still use symbols, perhaps to represent a different DVIPA address for each sysplex

Configuring for High Availability in a Sysplex …

- **To use system symbols to use the same z/OSMF configuration with a different hostnames (either for high availability or for cloning) you:**
  - Create/update an IEASYMxx PARMLIB member defining one or more symbols that make up that part of the hostname that you want to change
    - For example, to change a hostname from **ALPS4142**.POK.IBM.COM to **ALPS4249**.POK.IBM.COM
      - Define a symbol, **ALPSHOST,** for the first node of the hostname

```
   SYS1.PARMLIB(IEASYMMF) - 01.00
 ===> _____________________________
******************************** Top o
SYSDEF SYMDEF(&ALPSHOST='ALPS4249')
***************************** Bottom
```

      - Update LOADxx to use the system symbol during IPLs
        - » Note that the SETLOAD xx,IEASYM command can be used on z/OS V2.1 to dynamically activate the new/updated symbol definition

          e.g., SETLOAD 00,IEASYM (if IEASYMMF was defined in LOAD00)

Configuring for High Availability in a Sysplex ...

- Update the etc/zosmf/servers/zosmfServer/bootstrap.template to use the symbol definition(s)

```
******************************* Top of Data ***********************
# Licensed Materials - Property of IBM
#
# "Restricted Materials of IBM"
#
# Copyright IBM Corp. 2013 All Rights Reserved.
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with
# IBM Corp.
#
# ------------------------------------------------------------
#

izu.hostname=&ALPSHOST..POK.IBM.COM
izu.https.port=443
izu.http.port=80
```

- Stop and start the z/OSMF server (IZUSVR1) to use the updated definition and symbols