#SHAREorg

SHARE
Technology · Connections · Results

z/OSMF V1.13 Implementation and Configuration

Greg Daynes
IBM Corporation

August 9, 2012
Session Number 11723

SHARE in Anaheim 2012

Agenda

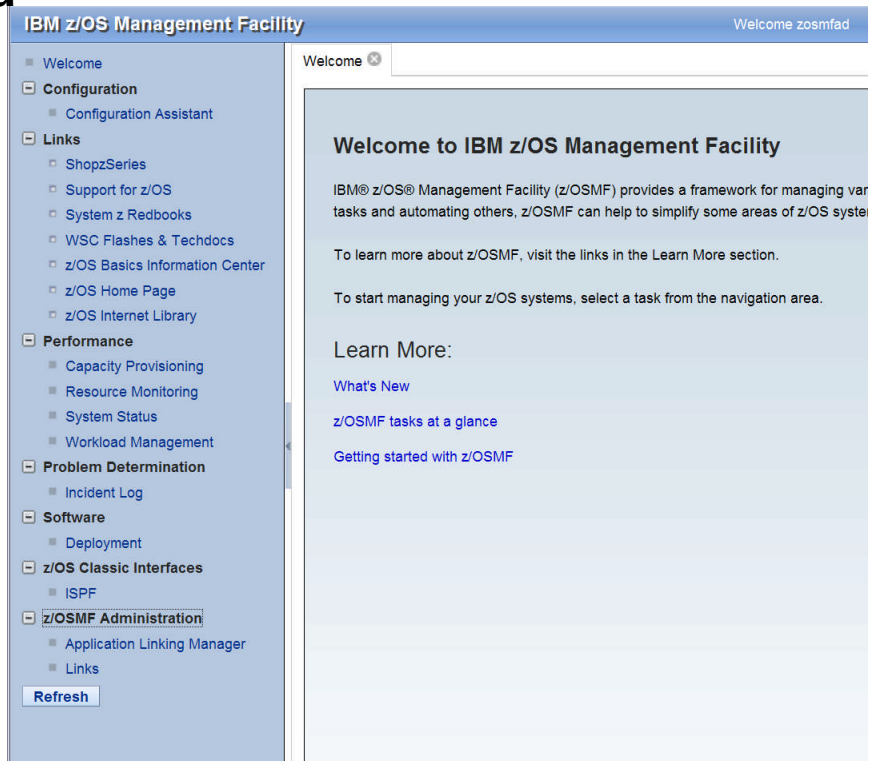
- **Overview of z/OS Management Facility V1.13**
- **Ordering and Installing z/OS Management Facility V1.13**
  - –Via ServerPac or SMP/E
- **Setup and configuration overall process**
  - –Configure z/OS prerequisites for WebSphere Application Server OEM Edition
  - –Configure WebSphere Application Server OEM Edition
  - –Configure z/OS prerequisites for z/OSMF Plug-ins
  - –Configure z/OSMF

Disclaimers

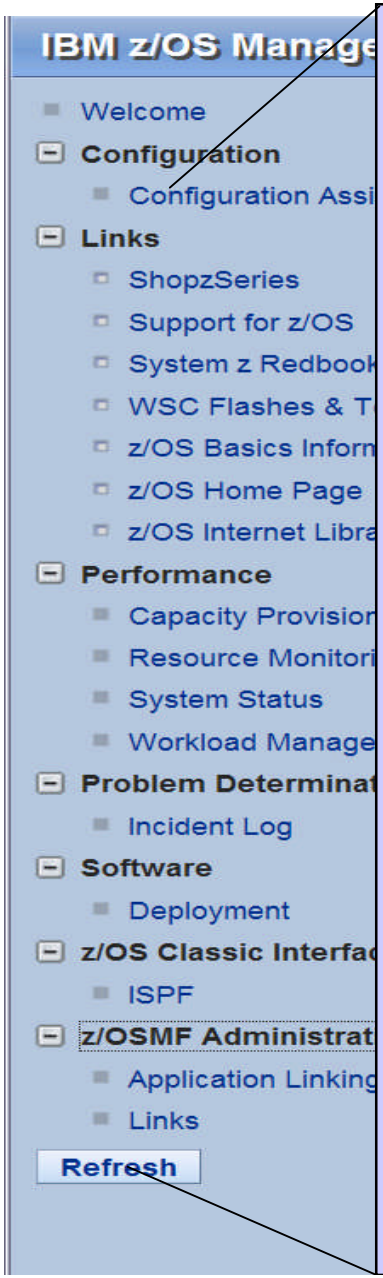
- **z/OSMF enables the user to tailor many different configuration settings. Not all of those options will be covered in this presentation.**
- **Most customer configurations are different. Some settings may need to be different in your environment. For example:**
  - If you use existing User IDs or Security Groups
  - If you use AUTOMOUNT
  - If you make changes to support shared OMVS sysplex environment

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.



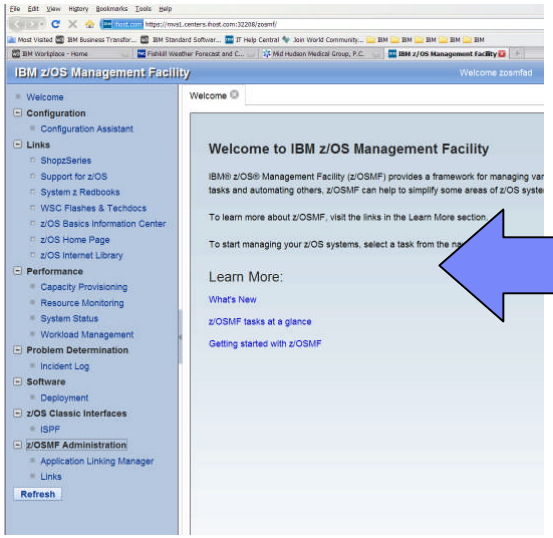
IBM z/OS Management Facility

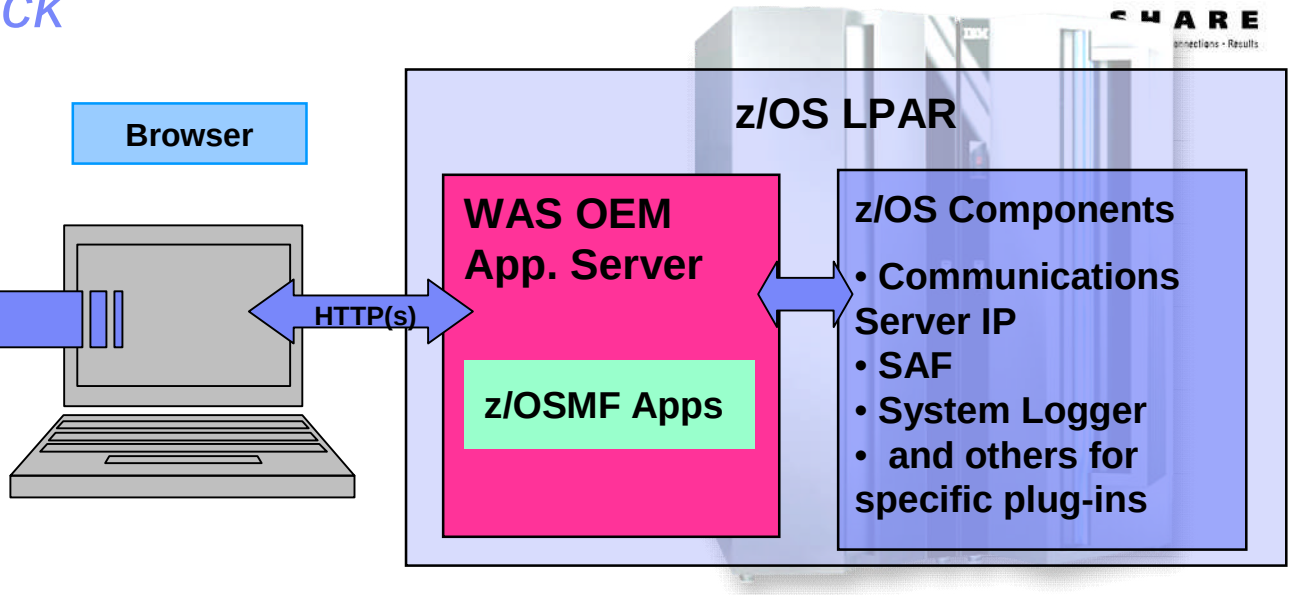


- **Configuration** category
  - **Configuration Assistant for z/OS Communication Server** application
  - Simplified configuration and setup of TCP/IP policy-based networking functions
- **Links** category
  - Links to resources - provides common launch point for accessing resources beyond z/OSMF
- **Performance** category
  - **Capacity Provisioning (R13)** manage connections to CPMs, view reports for domain status, active configuration and active policy.
  - **Resource Monitoring, System Status** (changed name in R13) - provides integrated performance monitoring of customer's enterprise
  - **Workload Manager Policy Editor** application
  - 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** provides a consolidated list of SVC Dump related problems, along with details and diagnostic data captured with each incident; facilitates sending the data for further diagnostics.
- **Software** category **(R13)**
  - **Deployment** make deployment of installed software simpler and safer.
- **z/OS classic Interface** category **(R13)**
  - **ISPF Task** integrates existing ISPF into z/OSMF to enable tasks from one interface and ability to launch to ISPF functions directly
- **z/OSMF Administration** category
  - z/OSMF authorization services for administrator: add users, define roles, dynamically add links to non-z/OSMF resources; application linking manager(R13)

IBM z/OS Management Facility

The Application Stack





- The z/OS Management Facility applications run on the z/OS system and are presented on a PC using a browser
- The z/OS Management Facility requires:
  - **z/OS Communications Server**
  - **Security definitions (SAF)**
  - **System Logger**
  - **Other components are required for specific z/OSMF plug-ins**
- z/OSMF uses industry standards, such as Java, Dojo, and CIM.
  - **z/OSMF is a set of WebSphere applications and uses a large amount of JAVA**
  - **Java and z/OS CIM Server workloads can run on available specialty engines.**

IBM z/OS Management Facility

- The IBM z/OS Management F[illegible] a separate licensed program product
  - z/OS Management [illegible]1.13 (5655-S28)
    - Same prog[illegible]er as z/OS Management Facility V1.11 and V1.12
  - z/OS Man[illegible]ent Facility V1.1 Subscription and Support (5655-S29)
- The IBM z/OS Management Facility product consists of :
  - WebSphere Application Server OEM Edition
  - z/OSMF core infrastructure
  - z/OSMF plug-ins
- z/OS Management Facility V1.11 runs on z/OS V1.10 through z/OS V1.13
  - The Configuration Assistant for z/OS Communications Server requires z/OS V1.11 or higher
- z/OSMF V1.12 requires z/OS V1.12 or higher
- z/OSMF V1.13 requires z/OS 1.13

No Additional Charge = Free

IBM z/OS Management Facility

- **z/OSMF V1.13 consists of ten (10) FMIDs:**
  - HSMA130 - z/OS Management Facility core
  - HSMA131 - z/OSMF ISPF
  - HSMA132 - z/OSMF RMF
  - HSMA133 - z/OSMF WLM
  - HSMA134 – z/OSMF Software Deployment
  - HSMA135 - z/OSMF Incident Log
  - HSMA136 - z/OSMF Capacity Provisioning
  - HSMA13A - z/OSMF Configuration Assistant
  - HSMA13F - z/OSMF DASD Management
  - HBBN700 - IBM WebSphere Application Server OEM Edition for z/OS

Ordering - S

Catalog view (Pro

Country/Region

Package type

Group

Language

MVS: z/OS Operat

	Product				
◆	[5694-A01]				
◆	[5694-A01]				
◆	[5655-S28]				
◆	[5655-S28]	z/OS Management Facility	[FMIDs]	1.13.00	English (US)

IBM

FMIDs

FMIDs for z/OS Management Facility

FMID	Description
HBBN700	IBM WebSphere Application Server OEM Edition for z/OS
HSMA13A	IBM z/OS Management Facility - Config Assist
HSMA13F	IBM z/OS Management Facility - Storage Manager (DFSMF GUI)
HSMA130	IBM z/OS Management Facility
HSMA131	IBM z/OS Management Facility - ISPF (WebISPF GUI)
HSMA132	IBM z/OS Management Facility - RM
HSMA133	IBM z/OS Management Facility - WLM
HSMA134	IBM z/OS Management Facility - Software Deployment (SMP/e GUI)
HSMA135	IBM z/OS Management Facility - Incident Log
HSMA136	IBM z/OS Management Facility - Capacity Provisioning

Prerequisites

- Client machine (no client machine install requirements)
  - Microsoft Windows Vista, Windows 7 (32 and 64 bit), and Windows XP
    - Mozilla Firefox 3.5
    - Mozilla Firefox 3.6
    - Internet Explorer 7
    - Internet Explorer 8
  - For a complete list of supported browsers see:
    - http://www-03.ibm.com/systems/z/os/zos/zosmf/browser_notes.html
- Host system
  - WebSphere Application Server OEM Edition running z/OSMF minimally needs to run on a 120 MIPS server
    - Note execution of the Java and CIM code can exploit specialty engines

Overall z/OSMF Installation and Configuration Process

- **Install the software (code)**
  - Via ServerPac or SMP/E
- **Configure WebSphere Application Server OEM Edition**
- **Configure z/OS prerequisites (if necessary)**
- **Configure z/OSMF**
- **Start WebSphere Application Server OEM Edition**
  - And Login to z/OSMF

Planning

- **There are two manuals that you will use to configure z/OSMF**
  - WebSphere Application Server OEM Edition Configuration Guide
  - z/OSMF Configuration Guide
- **Each manual has a planning chapter and planning worksheets**
  - You should read both planning chapters before you begin
  - You should complete the planning worksheets before you attempt to configure either WebSphere Application Server OEM Edition or z/OSMF
- **In general, you should:**
  1. Configure the prerequisites for WebSphere Application Server OEM Edition
  2. Configure and verify WebSphere Application Server OEM Edition
  3. Configure the prerequisites for the z/OSMF plug-ins you plan on using
     - This really can be done any time before you perform step 4
  4. Configure and verify z/OSMF

Note: Each step can involve creating or updating security definitions

Software Installation

- z/OSMF V1.13 ordered in a z/OS ServerPac
  - –Provides default customization via ServerPac provided customization job
    - Provided for Full System Replace installation path
    - Software Upgrade jobs and documentation provided but may need changes based on your existing environment
  - –Can also use the WebSphere Application Server OEM Edition Configuration Guide and z/OSMF Configuration Guide
    - Product configuration scripts to setup, if defaults are not viable
- z/OSMF V1.13 ordered in a CBPDO
  - –Use Program Directory to get started
  - –Use the WebSphere Application Server OEM Edition Configuration Guide and z/OSMF Configuration Guide
    - Product configuration scripts to setup

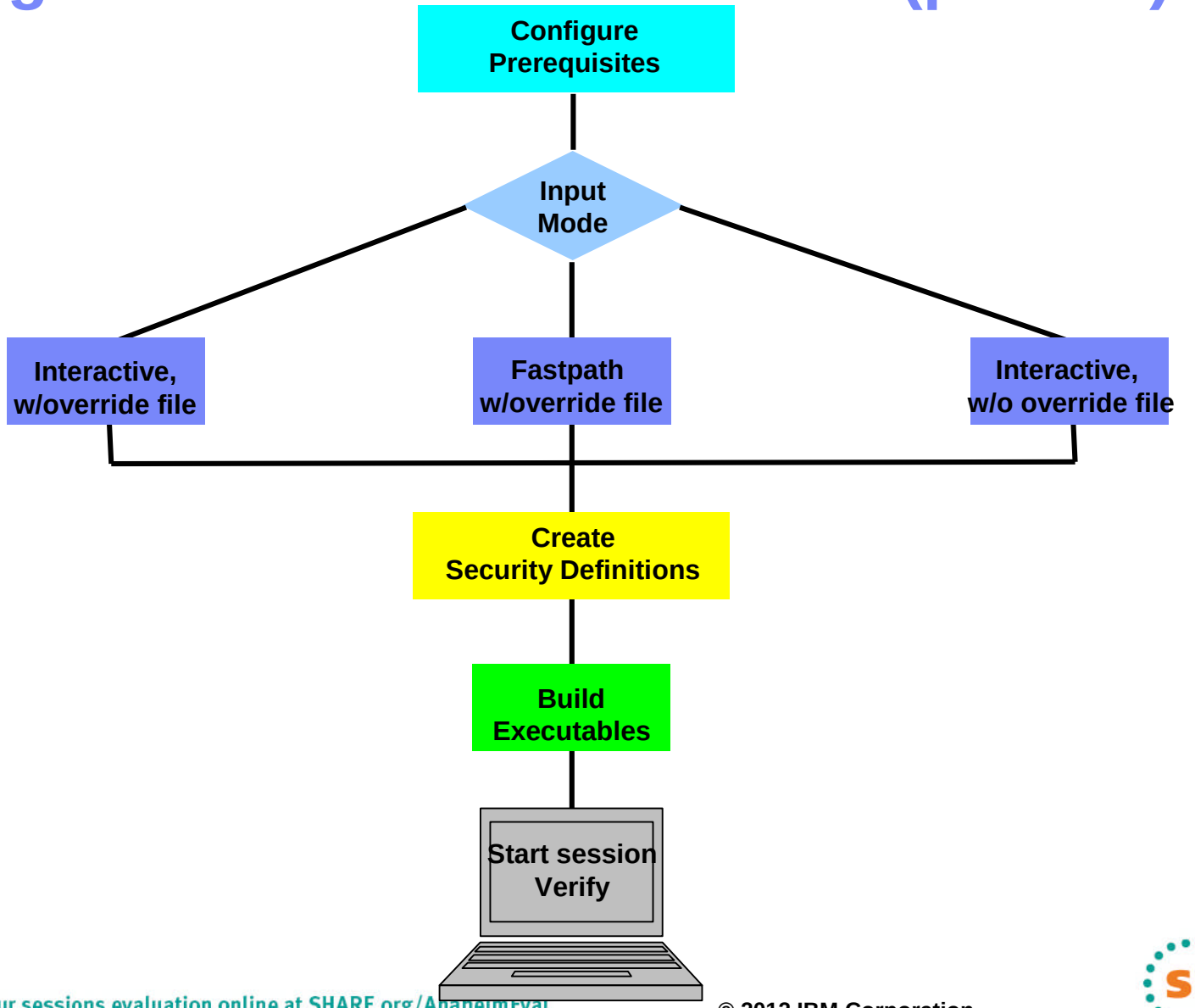
File Systems

- WebSphere OEM Edition
  - Product file system
    - Described by Program Directory
    - Allocated via sample job CYL(2400 50)
    - Can be HFS or zFS
    - Recommend zFS and use of AGGRGROW
  - Configuration file system
    - Described in IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide
    - Can be preallocated or allocated by scripts
    - Default is a ZFS, CYL(420,100)
    - Recommend CYL(620,100) and use of AGGRGROW
- z/OSMF Plug-ins
  - Product file system
    - Described by Program Directory
    - Allocated via sample job CYL(150 15)
      - 50% bigger than the z/OSMF V1.12 default size
    - Can be HFS or zFS
  - Persistent data file system
    - Described in z/OSMF Configuration Guide
    - Can be preallocated or allocated by scripts
    - Default is a ZFS, CYL(180,20)
      - Twice the z/OSMF V1.12 default size
    - Recommend use of AGGRGROW

Configuration Process Overview

- Both WebSphere Application Server OEM Edition and z/OSMF have four basic phases for configuration
  1. **Configure prerequisites**
  2. **Setup configuration files**
  3. **Create security definitions**
  4. **Build executables (run-time files)**
- **Most phases are driven through the use of z/OS UNIX configuration scripts**
  - The scripts to setup the configuration files can be run:
    - Interactively with an override or response file
      - Think of it as a PARMLIB member with only the values that you want to change
      - Customized values will be used in prompts, which can still be overridden
    - FASTPATH mode (minimal prompts)
      - Requires an override file (or a configured configuration file)
    - Interactively without an override file
      - Default values will be used in prompts, which can be overridden

Configuration Process Overview (picture)



Setup Configuration File Script Modes (1 of 3)

- Interactive mode (with an override file)
  - –Script prompts you for all 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.
  - –Use this mode if you want the configuration session to be preset with your installation-specific values.
  - –This method saves you from having to enter your customized values interactively in response to script prompts.
    - Instead, you need only review each value displayed by the script and press Enter to accept it.

Setup Configuration File Script Modes (2 of 3)

- Fastpath mode
  - The script runs to completion without any interactive prompting.
    - WebSphere Application Server OEM Edition has minimal 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.

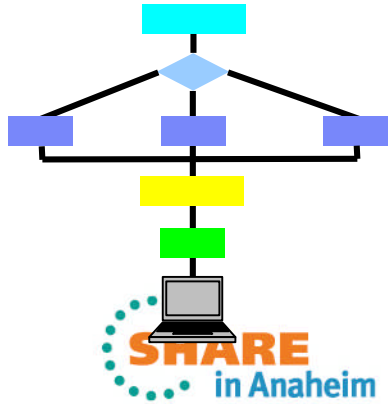
  - Use this mode if:
    - You prefer to supply your data in a standalone file, and have no need to review the values interactively.
    - You have verified that all of your configuration data is supplied through the configuration file, or the optional override file, or a combination of both files.
    - 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.

Setup Configuration File Script Modes (3 of 3)

- Interactive mode (without an override file)
  - The script prompts you for all 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.
  - Use this mode if 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.
    - Note that some values have no IBM defaults; these always require your input.

WebSphere Application Server OEM Edition Configuration Process

- **The configuration process occurs in three stages, and in the following order:**
  1. **Configure WebSphere Application Server OEM Edition prerequisites**
  2. **Configuration**
     a. **Interactive mode (with an response/override file)**
        - **Called "Advanced"**
     b. **Fastpath mode**
     c. **Interactive mode (with a default response/override file)**
        - **Called "Typical"**
  3. **Security setup**
     - **Submit Security Customization Jobs**
       - BBOSBRAK, BBOSBRAM, and BBOCBRAK
  4. **Server instance creation**
     - **Invoke WASOEM.sh in create mode**



Configure WebSphere Application Server OEM Edition Prerequisites

- **Verify that in your BPXPRMxx member:**
  - The MAXFILEPROC parameter is set to a value that is greater than, or equal to 2000.
  - The MAXTHREADS parameter is set to a value that is greater than, or equal to 10000.
  - The MAXTHREADTASKS parameter is set to a value that is greater than, or equal to 5000.
- **Verify that enough virtual memory is allocated to the address space for each server instance.**
  - The Java virtual machine for each server instance requires at least 250M of virtual memory.
    - Make sure that the address space for each server instance, as well as OMVS or batch job address spaces that run the Java virtual machines, have access to enough virtual memory below the 2-gigabyte bar.
  - The IBM Corporation recommends that you allocate at least 1024M of virtual memory to the address space for each server instance.
    - You can issue the following command to verify the current MEMLIMIT setting for your installation:
      - D SMF,O

Configure WebSphere Application Server OEM Edition Prerequisites

- **Verify that the following libraries are in the system link list and are APF authorized:**
  - Language Environment libraries, SCEERUN, and SCEERUN2
  - System SSL library, SIEALNKE
  - 64–bit support library, SCLBDLL2
- **Verify that TCPIP is configured and active**
- **Define a log stream for IBM WebSphere Application Server OEM Edition for z/OS to use**
  - System logger is required for RRS setup
- **Verify that Resource Recovery Services (RRS) is defined.**
  - See you z/OS documentation for more information about RRS.

WebSphere Application Server OEM Edition Configuration Hints and Tips

- z/OSMF V1.13 requires WAS OEM Server Fix Pack level 7.0.0.17 level
  - PTFs UK69589 UK69590 UK69591 UK69592 UK69593 UK69594 UK69598 UK69599 UK69600 UK69601 UK69602
    - Please refer to the HOLD information provided in PTF UK69589 for additional information in regards to servicing WebSphere Application Server OEM for z/OS V7.0.
  - Use the appropriate edition of the IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide (GA32-0631-05)
    - **The current level is GA32-0631-07, the current WAS OEM Server Fix Pack level is 7.0.0.21 (APAR PM59254, PTF UK76762)**
      - See APAR PM67692 before installing PTF UK76762
- Use the configuration worksheet as a guide determining the appropriate value that should be specified for your 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 WASOEM script.
- Use an override file if the default values don't suffice for the system onto which IBM WebSphere Application Server OEM Edition for z/OS is being configured.

WebSphere Application Server OEM Edition Configuration Hints and Tips

SHRLIBRGNSIZE

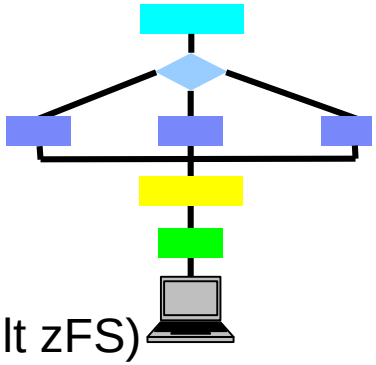
- **If you receive an error message that indicates that the SHRLIBRGNSIZE setting is too small, you need to increase this setting to a more appropriate value. However, when adjusting this setting, you must be careful not to make the setting so large for that it impacts other processes running**
  - IBM WebSphere Application Server OEM Edition for z/OS requires a minimum of 1 GB of real storage.
  - Refer to the topic “Using the shared library extended attribute” for guidelines on how to determine an appropriate setting for the SHRLIBRGNSIZE parameter.

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 IBM WebSphere Application Server OEM Edition for z/OS user IDs and groups.
    - Therefore 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.
    - Refer 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.

WebSphere Application Server OEM Edition Prompts and Response File

- **The following prompts are the ones that are most likely to require changes:**
  - GID and UID defaults (I use AUTOUID/AUTOGID to not require overrides)
  - 17 Port defaults (15 ports at 7.0.0.21)
  - Target Data sets High-level qualifier (HLQ)
  - Target Data sets High-level qualifier (HLQ) VOLSER
  - PROCLIB data set name
  - Configuration File System - Mount point (I take the default)
  - Configuration File System - Data set name
  - Job card information
  - Configuration File System - File system type (we take the default zFS)
  - Configuration File System – VOLSER
  - WebSphere Application Server Product File System - Product file system directory (we take the default)
  - System name, sysplex name and host name – these values are dynamically determined for the system by the script, but can be overridden



- **However, you should review ALL of the other prompts to determine if any additional configuration variables need to be updated.**
  - If so you can either in respond to the prompts, or update the response file with the changed values
    - We updated the wasOEMOverride.responseFile file

Sample WebSphere Application Server OEM Edition Response File

```
hostName=@HOSTNAME
zAdminConsolePort=30005
zAdminConsoleSecurePort=30006
zAdminLocalPort=30009
zConfigHfsName=ZOSBUILD.HBBN700.CONFIG1.ZFS
zConfigHfsVolume=ZCSDW
zDaemonHomePath=generated
zDaemonIPName=generated
zDaemonPort=30000
zDaemonSslPort=30001
zHighAvailManagerPort=30010
zHttpTransportPort=30007
zHttpTransportSslPort=30008
zJobStatement1=(ACCTNO,ROOM),'HELEN',CLASS=A,REGION=0M,
zJobStatement2=//         MSGCLASS=H,NOTIFY=&SYSUID,MSGLEVEL=(1,1)
zJobStatement3=//*
zJobStatement4=//*
zOrbListenerPort=30003
zOrbListenerSslPort=30004
zProclibName=ZOSBUILD.ZOSMF.PROCLIB
zServiceIntegrationMqPort=30013
zServiceIntegrationPort=30011
zServiceIntegrationSecureMqPort=30014
zServiceIntegrationSecurePort=30012
zSessionInitiationPort=30015
zSessionInitiationSecurePort=30016
zSoapPort=30002
zSysplexName=@PLEXNAME
zSystemName=@SYSNAME
zTargetHLQ=ZOSBUILD.HBBN700.CONFIG1.ZPMTJOBS
# end of file marker - do not remove
```

Complete response file used

Configuration - Required Authority

- **You can run the WASOEM.sh script from an OMVS or telnet/rlogin session.**
  - –You **cannot** run this script from under ISHELL.
- **The user ID you use to run the WASOEM.sh script must:**
  - –Be authorized to create and modify directories, data sets, and file systems in the locations specified by the variables in the configuration file.
  - –Have at least 2 GB of memory allocated for its use.
    - WASOEM.sh requires this amount of memory to properly complete the configuration, and instance creation processes.

Configuration – First Time

- **If this is the first time the product is being configured since it was installed, issue the following command:**
  - WASOEM.sh
- **This command copies the two required configuration files from the product installation location to a predetermined location in the file system.**
  - Default is /etc/zWebSphereOEM/V7R0
  - This action is required once per product installation
- **If you issue this command, and the files have already been copied to the predetermined location in the file system, the help message for the WASOEM.sh command displays.**

Configuration – With Prompting

1. **Edit and update the override response file (if required).**
2. **Allocate the configuration file system (if required).**
3. **Issue one of the following commands to configure an IBM WebSphere Application Server OEM Edition for z/OS server instance:**

– WASOEM.sh –config -mode advanced (My preference)
– WASOEM.sh –config –mode typical

Notes:

- When you issue the WASOEM.sh –config command, the WASOEM prompts will start.
- In response to these prompts, press enter to accept the default values, or specify your new values.
- During WASOEM.sh -config processing, a final response file is created which is used to invoke WebSphere Application Server for z/OS configuration technology in the form of the zpmt.sh install tool.
  - This script accepts the responseFile after it has been tailored and produces three (3) security jobs which are submitted in the next stage.

Configuration Modes

- **The configuration stage can be run in either the typical or advanced mode:**
  - The **typical** mode only prompts you for very system specific configuration details and utilizes many of the best practices defaults values that are used for a basic WebSphere Application Server for z/OS configuration.
    - Use this mode if you desire a basic functional configuration with minimal prompt interaction.
  - The **advanced** mode includes additional prompt that enable you to specify most configuration settings for your installation, and should only be used if the IBM WebSphere Application Server OEM Edition for z/OS server instance that you are creating requires a fine level of configuration specification.
    - During processing in the advanced mode, you can still select any of the default values that meet the needs of your installation.
    - However, the additional prompts that display give you the opportunity to override any of these default values that are not appropriate for your environment.
- **If you do not include the -mode parameter when you issue the WASOEM.sh –config command, the typical mode processing occurs because typical is the default value for the -mode parameter.**

Security - Required Authority

- You must run these customization jobs in the indicated order, using a user ID that has RACF special authority to run these jobs, and file system update authority, which is required by the BBOSBRAM job.
  - Whenever file system update authority is indicated for one of these jobs, the user ID that you use to run that job must have either UID = 0, or the following UNIXPRIV class profile privileges:
    - 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
- For more information about the UNIXPRIV class, see the z/OS Unix System Services Planning publication.
  - This publication is included in the z/OS Internet Library at:
    - http://www.ibm.com/systems/z/os/zos/bkserv/

Security Jobs

The security jobs must be run in the following order:

1. **The BBOSBRAK security job**
   - Running this job creates common IBM WebSphere Application Server OEM Edition for z/OS groups, and user IDs.
   - **Note:** This job creates the administrator ID (zAdminUserid) without a password, or password phrase. You must assign this user ID a password, or password phrase that complies with your standards.
   - If you are using a different security system, make sure that the administrator ID has a password or password phrase.
2. **The BBOSBRAM security job**
   - Running this job creates home directories for IBM WebSphere Application Server OEM Edition for z/OS. All of these home directories are subdirectories of /var/zWebSphereOEM/home, which has permission bits 755.
   - Run this job on each z/OS system that will host IBM WebSphere Application Server Edition for z/OS nodes using the IBM WebSphere Application Server OEM Edition z/OS common groups and owner user ID.
   - After this job finishes, verify that the directories exist on each system and ha correct permissions.
3. **The BBOCBRAK security job**
   - Running this job creates RACF users and profiles that are required h BM WebSphere Application Server OEM Edition for z/OS node.
   - When this job completes, all user IDs should be defined in the R atabase on each target system for the cell.

For other security products use these jobs as a model

Running the Security Jobs

- **The newly created customization jobs are located in the $zTargetHLQ.CNTL library.**
  - For example, if the default.Responsefile contained a setting of:
    - `$zTargetHLQ=BBN.V7R0.CONFIG1.ZPMTJOBS`
  - Then the security customization jobs would be found in the library
    - `BBN.V7R0.CONFIG1.ZPMTJOBS.CNTL`
  - And the REXX EXEC used to invoke the RACF commands would be found in the library
    - `BBN.V7R0.CONFIG1.ZPMTJOBS.DATA`

Note: The generated security definitions may need to change to fit your installation's policies

Invoke WASOEM.sh in Create Mode

Create an IBM WebSphere Application Server OEM Edition for z/OS server instance

- **Issue command to create a IBM WebSphere Application Server OEM Edition for z/OS server instance.**
  - This example uses the default configuration name, CONFIG1.
    - **WASOEM.sh -create CONFIG1**
- **The configuration data set specified in the configuration step is allocated and mounted during this step.**
- **When this step completes a series of messages**
  - Next chart

Sample Messages

```
BBN0016I:Success: Update of configuration completed.
The following ports have been set, ensure that they are added to the reserved port list:
zDaemonPort 30000
zDaemonSslPort 30001
zSoapPort 30002
zOrbListenerPort 30003
zOrbListenerSslPort 30004
zAdminConsolePort 30005
zAdminConsoleSecurePort 30006
zHttpTransportPort 30007
zHttpTransportSslPort 30008
zAdminLocalPort 30009
zHighAvailManagerPort 30010
zServiceIntegrationPort 30011
zServiceIntegrationSecurePort 30012
zServiceIntegrationMqPort 30013
zServiceIntegrationSecureMqPort 30014
zSessionInitiationPort 30015
zSessionInitiationSecurePort 30016
BBN0152I: To start the application server, issue the MVS command:
BBN0153I: START BBN7ACR,JOBNAME=BBNS001,ENV=BBNBASE.BBNNODE.BBNS001
BBN0154I: To stop the application server, enter the MVS command:
BBN0155I: STOP BBN7ACRS
BBN0231I: The administrative console for your server can be accessed at
        http://ALPS4142.POK.IBM.COM:30005/ibm/console using user ID WOEMADM
BBN0231I: A password needs to be assigned to WOEMADM before it can be used.
BBN0148I: WASOEM.sh has completed
Check log file /var/zWebSphereOEM/V7R0/logs/WASOEM_020810_180059.log for more
        information
```

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 and System Status task
  - System prerequisites for the Software Deployment 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.
- **Optional:** Determine whether access to a remote Common Information Model (CIM) server is required. This work can be done after you have configured z/OSMF.

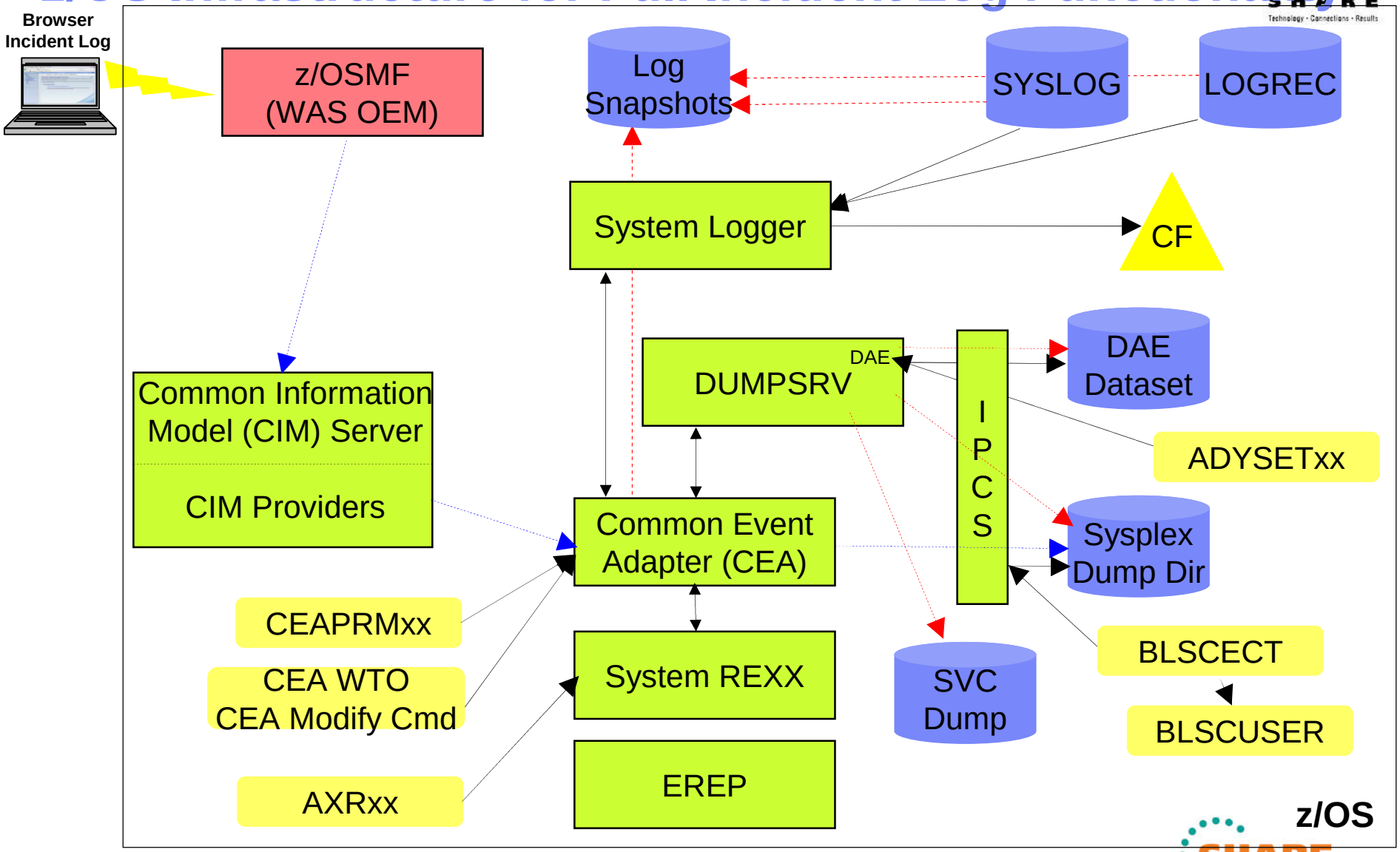
System Prerequisites for Configuration Assistant

- 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 transfer your backing store files to the z/OSMF environment. This setup can be done after configuring z/OSMF

Configure z/OS for Full Incident Log Functionality

- **z/OSMF's Incident Log exploits existing best practices for data management for problem determination.**
  1. **Sysplex Dump Directory (required)**
  2. **Use of System Logger for SYSLOG (OPERLOG) and LOGREC**
     - As of z/OSMF V1.12 Incident Log supports the creation of diagnostic log snapshots based on the SYSLOG and LOGREC data sets, as well as the OPERLOG and LOGREC sysplex log streams.
  3. **Dump analysis and elimination (DAE) is active and its symptom data set is available**
  4. **Automatic Dump Data Set Allocation**
  5. **AMATERSE program is enabled to run**
  6. **CEA, the CIM server, and System REXX components are available**
  7. **Parallel encrypted File Transfer Protocol FTP to IBM**
     - In z/OSMF V1.12 Incident log leverages the Problem Documentation Upload Utility, which offers encryption and parallel FTP of diagnostic data to IBM. Information can be found at
       - http://www14.software.ibm.com/webapp/set2/sas/f/zaids/pduf.html
     - In z/OS V1.13 the Problem Documentation Upload Utility is included
- **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) 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

- **(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

- **(3) 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

- **(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) AMATERSE program is enabled to run**
  - –AMATERSE is a service aid program that you use to pack a data set before transmitting a copy to another site, typically employing FTP as the transmission mechanism.
  - –A complementary unpack service is provided to create a similar data set at the receiving site.
  - –z/OSMF uses AMATERSE to prepare the diagnostic data to be sent (e.g., to IBM)
    - For z/OSMF to use AMATERSE, it must be explicitly APF authorized
      - o Ensure that SYS1.MIGLIB is APF-authorized

Configure z/OS for Full Incident Log Functionality

- **(6a) 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 –prime step.
    - 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

(6b) 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 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
  - 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 and System Status Tasks

- **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*, SC33-7990.
- **Determine whether the RMF Distributed Data Server (DDS) is configured to require authentication.**
  - You can use the following command to display the active DDS options: MODIFY GPMSERVE,OPTIONS. In the command output, the HTTP_NOAUTH statement indicates the scope of authentication for the DDS.
  - If your installation requires the authentication feature of the DDS: Ensure that the PassTicket is set up properly, and that the WebSphere Application Server servant user ID is authorized to generate PassTickets. This setup can be done after configuring z/OSMF.
  - If your installation does not require the authentication feature of the DDS: It is recommended that you disable DDS authentication. Doing so allows the Resource Monitoring and System Status tasks to access the DDS on behalf of z/OSMF users without encountering authentication errors.

System Prerequisites for the Software Deployment

- **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*, SA22-7602

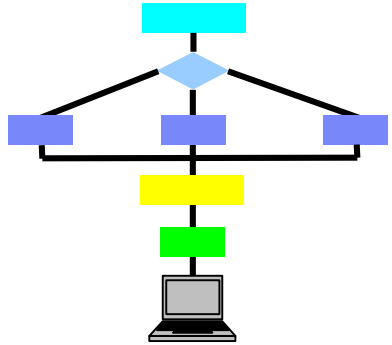
System Prerequisites for the Workload Management Task

- 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 on slide 43
- 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*, SC33-7998.

z/OSMF Configuration Process

- **The configuration process occurs in three stages, and in the following order:**

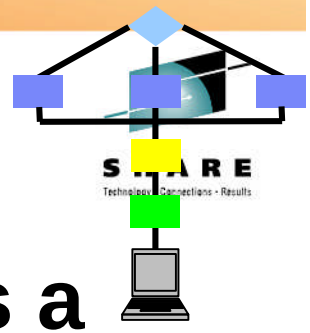


1. **Stage 1 – Configuration**
   a. **Interactive mode (with an override file)**
   b. **Fastpath mode**
   c. **Interactive mode (without an override file)**
2. **Stage 2 - Security setup**
   - **Invoke Security REXX EXEC**
     - ***/etc/zosmf*/izuconfig1.cfg.rexx**
   - **Verify the RACF Security Setup**
     - **izusetup.sh -file */etc/zosmf/izuconfig1*.cfg –verify racf**
3. **Stage 3 – Build the executables – deploy the z/OSMF apps**
   - **Prime the z/OSMF data file system**
     - **izusetup.sh -file */etc/zosmf/izuconfig1*.cfg -prime**
   - **Complete the setup (deploy, 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 1: Create the initial configuration	izusetup.sh -file <*pathname/filename*>.cfg -config *[...other options...]*	Superuser
Step 2: Run the security commands	<*IZU_CONFIG_DIR*>/izuconfig1.cfg.rexx	Security Administrator
Step 3: Verify the RACF security setup	izusetup.sh -file <*pathname/filename*>.cfg -verify racf	Security Administrator
Step 4: Prime the z/OSMF data file system	izusetup.sh -file <*pathname/filename*>.cfg -prime	Superuser
Step 5: Complete the setup	izusetup.sh -file <*pathname/filename*>.cfg -finish	z/OSMF Administrator
Step 6: Access the z/OSMF Welcome task	At the end of the z/OSMF configuration process, 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 Configuration Hints and Tips



- **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.**

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 but still need overrides)
  - WebSphere Application Server OEM Edition configuration file location
  - z/OSMF data filesystem data set name
  - Volume serial numbers for data sets
  - z/OSMF Administrator's TSO security segment settings
  - PARMLIB data set names
  - PARMLIB suffixes
  - Whether to configure CEA (Whether to configure the Incident Log Task)
    - CEA default parameters
  - Configure z/OSMF plug-ins (Y/N)
- **However, you should review ALL of the other prompts to determine if any additional configuration variables need to be updated.**
  - If so you can either in respond to the prompts, or update the override file with the changed values
    - **We used an *letc/zosmf/izuhlt.ovr* override file.**

Sample z/OSMF V1.13 Override File

```
# Licensed Materials - Property of IBM
# 5655-S28
# Copyright IBM Corp. 2009, 2010
# Status = HSMA130
# Information: SID=1.1.1.33  Delta Date=3/8/11 Delta Time=10:23:38
# Do not update or remove variable IZU_OVERRIDE_FILE_VERSION.
IZU_OVERRIDE_FILE_VERSION=1.13.0
IZU_DATA_DIR=/var/zosmf/data
IZU_DATA_FS_NAME=MVSBUILD.IZU.SIZUDATA
IZU_DATA_FS_TYPE=ZFS
IZU_DATA_FS_VOLUME=ZCSDW
IZU_DATA_FS_SIZE=500
IZU_AUTOUID_OVERRIDE=Y
IZU_AUTOGID_OVERRIDE=Y
IZU_ADMIN_PROC=ISPFPROC
IZU_ADMIN_ACCOUNT=FRED
IZU_WAS_CONFIG_FILE_KNOWN=Y
IZU_WAS_CONFIG_FILE_LOCATION=/etc/zWebSphereOEM/V7R0/conf/CONFIG1/CONFIG1.responseFile
IZU_IL_CEA_CONFIGURE=Y
IZU_CEA_PARM_NAME=MF
IZU_IEA_PARM_NAME=MF
IZU_INCIDENT_LOG=Y
IZU_CIM_SETUP=N
IZU_COUNTRY_CODE=000
IZU_BRANCH_CODE=035
IZU_STORAGE_VALUE="VOLSER(ZCSDW,ZCSDWX,ZCSDWY)"
IZU_CEAPRM_SOURCE_PARMLIB=SYS1.IBM.PARMLIB
IZU_CEAPRM_TARGET_PARMLIB=MVSBUILD.ZOSMF.PARMLIB
IZU_IEADMC_SOURCE_PARMLIB=SYS1.SAMPLIB
IZU_IEADMC_TARGET_PARMLIB=MVSBUILD.ZOSMF.PARMLIB
IZU_IL_CONFIGURE=Y
IZU_CA_CONFIGURE=Y
IZU_WLM_CONFIGURE=Y
IZU_RMF_CONFIGURE=Y
IZU_CIM_CONFIGURE=Y
IZU_CP_CONFIGURE=Y
IZU_DM_CONFIGURE=Y
IZU_WISPF_CONFIGURE=Y
```

Complete override file used

The default override file has additional entries

Migrating to a New z/OSMF Release

- Migrating to a new release of z/OSMF from an older release is a two-step process.
  1. Start by migrating your existing configuration file and override file to the latest format.
  2. Then, configure the product as you would normally, supplying the updated configuration and override files as input to the z/OSMF configuration process.
- Depending on your current release of z/OSMF, you might also need to perform additional migration actions.
- If you have a z/OSMF V1.11 or z/OSMF V1.12 system configured and want to migrate your configuration file or override file to z/OSMF V1.13 format, there is script support for doing that.
  - Use **izumigrate.sh**, to migrate the z/OSMF V1.11 configuration file to the z/OSMF V1.13 format, see the z/OSMF Configuration Guide
    - A report is produced that describes what was done during the execution of the migration script

Migrating to a New z/OSMF Release - izumigrate.sh

- **This script migrates your configuration file, and, if specified, your override file from a previous release of z/OSMF to the latest format.**
- **In updating the configuration file and override file, the script retains your current settings when possible.**
- **For any properties that are no longer valid for z/OSMF, the script omits the properties when creating the updated files.**
- **If your existing configuration file contains commented sections (it should not), the script removes this information from the updated configuration file.**
- **If you choose to migrate an existing override file, understand that:**
  - The script processes only the properties that are specified in the override file. The script does not add any new properties to the updated override file.
  - The script determines the version of the override file by examining the override file property IZU_OVERRIDE_FILE_VERSION.
    - This property, which was introduced in z/OSMF V1R12, should not be modified.
    - If this property is missing from the override file, the script processes the override file as though it had originated from a z/OSMF V1R11 configuration.
    - If this property is set incorrectly in the override file, the script fails with an error message.
  - If your existing override file contains user comments, these commented sections are retained in the updated override file, though the placement of these sections might change as a result of the migration processing, which removes properties that no longer apply.
- **You can migrate the configuration file and override file together in one invocation of this script. Or, if you prefer, you can migrate these files individually by running separate invocations of the script.**

Step 1: Create the initial configuration

- **The** izusetup.sh -config **script uses the input you supply, based on your environment and the z/OSMF tasks that you plan to configure. The script saves your input in the configuration file, which is used as input to subsequent script invocations.**
- **You can run the** izusetup.sh **script either interactively (like an "interview") or "quietly" (the fastpath option). When used in interactive mode, the izusetup.sh script provides a prompt environment to modify the configuration settings needed to create a working instance of z/OSMF.**
- **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 RACF commands in a REXX program, which your security administrator can verify and run. If your installation uses another security management product, you can create a REXX program with equivalent SAF commands. The REXX exec is tailored based on the plug-ins that you choose to configure for z/OSMF.
  - If during this step, your installation is changing the authorization mode for z/OSMF, this process produces a second security commands REXX exec. This exec contains only the delta of security commands that are required for setting up security under the new authorization mode
- **Sample command:**
  - izusetup.sh -file /etc/zosmf/izuconfig1.cfg -config -overridefile /etc/zosmf/izuhlt.ovr

Remember the name of the configuration file

Step 2: Run the Security Commands

- **Prior to running the REXX EXEC your security administrator must define security for z/OS components (CEA, CIM, and CP) by running the appropriate (customized) sample jobs**
  - CEASEC, CFZSEC, and CPOSEC1
- **This exec is run by your installation's security administrator.**
- **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.**

Scenario	Action to take
New installation of z/OSMF	**Run izuconfig1.cfg.rexx**
Migrating from an earlier release of z/OSMF to a new z/OSMF configuration	**Run izuconfig1.cfg.rexx (will need to edit the exec if existing security data base is used).**
New z/OSMF configuration is already created; just changing the authorization mode from Repository to SAF.	**Run izuconfig1.cfg.convertFromREPtoSAF.rexx**
New z/OSMF configuration is already created; just changing the authorization mode from SAF to Repository.	**Run izuconfig1.cfg.convertFromSAFtoREP.rexx (the exec might consist of commented sections only).**

Step 2: Run the Security Commands

- **Prior to running the REXX EXEC review the RACF commands and comments making any necessary changes**
  - For example,
    - Uncomment commands if running in an MLS environment
    - Uncomment commands for CEA.* data set protection
    - Update any commands to conform to installation security policies

Recommend making changes to a copy of the file

Note: If you provided the proper User ID and Group names during the configuration process, you shouldn't have to edit those commands

- **Sample invocation of REXX EXEC**
  - From the /etc/zosmf/ directory
    - ./izuconfig1.cfg.rexx | tee izuconfig1_cfg_rexx.log

Captures command output in a file

Step 3: 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 4: Prime the z/OSMF Data File System

- **The** izusetup.sh -prime **script performs the following:**
  - Initializes or "primes" the z/OSMF data file system. This work includes:
    - Allocating the z/OSMF data file system and mounting it, by default, at /var/zosmf/data.
    - The script mounts 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 AGGRGROW to allow the filesystem to grow dynamically, as needed.
    - The script also sets the permissions and ownership of the directories and files in the z/OSMF data file system.
  - Creates the home directory for the z/OSMF administrator, if one does not already exist. By default, this directory is /u/zosmfad
  - Changes ownership and permissions for the other directories that z/OSMF uses.
  - Creates and updates PARMLIB members as needed for the plug-ins to be configured. For example, if you configured the Incident Log plug-in, this script creates members in the target PARMLIB data set. By default, this is SYS1.PARMLIB.
  - Performs other data set allocations, as needed for z/OSMF processing.
- **Sample command:**
  - izusetup.sh -file /etc/zosmf/izuconfig1.cfg -prime

Same configuration file as prior command

Step 5: Complete the Setup

- **The izusetup.sh -finish script deploys z/OSMF, using the values you supplied earlier. Specifically, the script**:
  - Registers z/OSMF with IBM WebSphere Application Server OEM Edition for z/OS.
  - Updates the WebSphere Application Server configuration, based on settings from the izuadmin.env file.
  - Prepares your z/OS system for running the tasks associated with the plug-ins that you selected to configure earlier.
  - Verifies the setup for the z/OSMF functions and tasks. If you configured the Incident Log task, the script runs an installation verification program (IVP) that verifies the setup of the following z/OS system components:
    - Sysplex dump directory
    - System logger
    - Common event adapter (CEA)
    - System REXX.
  - The script creates a report indicating any areas that might require further actionon your part.
  - Lastly, the script issues message IZUG349I, which provides the link (a URL) for accessing z/OSMF after the application server is started on your system
- **The script is intended to be run by the z/OSMF Administrator**
  - By default no password or passphrase is assigned to this ID
  - Prior to running the script you will need to define a password for the User ID
    - Ex: ALU ZOSMFAD PASSWORD(password) NOEXPIRED
- **Also ensure that IBM WebSphere Application Server OEM Edition for z/OS is NOT running.**
- **Sample command:**
  - izusetup.sh -file /etc/zosmf/izuconfig1.cfg -finish

Same configuration file as prior command

Step 5: Results - izuincidentlogverify.report

The script checks that all necessary steps were carried out, and creates a report indicating any areas that might require further action on your part. If you selected to configure the Incident Log task, the script ran an installation verification program (IVP) to verify the setup of z/OS system components. To see the results of the IVP, check the report file named **/etc/zosmfizuincidentlogverify.report**.

```
--------------------------------
Incident Log Verification Report
--------------------------------
Sysplex Dump Directory : SUCCESS
CEA                    : SUCCESS
System REXX            : SUCCESS
System Logger Active   : SUCCESS
----------------------
Diagnostic Data Results
----------------------
SVCDump          : SUCCESS
Operations Log   : SUCCESS
Error Log        : SUCCESS
Error Log Summary : SUCCESS
--------------------------------
Incident Log Operations Results
--------------------------------
Prepare Dump Request                : SUCCESS
Prepare Operations Log Request      : SUCCESS
Prepare Error Log Request           :SUCCESS.
Prepare Error Log Summary Request   : SUCCESS
Prepare View Operations Log Request : SUCCESS
Prepare View Error Log Request      : SUCCESS
Prepare View Error Log Summary Request : SUCCESS
Set PMR Request                     : SUCCESS
Set Tracking Request                : SUCCESS
Set User Comment Field Request      : SUCCESS
------------------
CEA Parmlib Member
------------------
SnapShot      : Y
Branch        : 221
Country       : 897
Storage Value : AUXPK1
HLQ           : CEA
```

```
SLIP  OperLog       time : 1800
SLIP  LOGREC        time : 3600
SLIP  LOGRECSUMMARY time : 14400
DUMP  OperLog       time : 1800
DUMP  LOGREC        time : 3600
DUMP  LOGRECSUMMARY time : 14400
ABEND OperLog       time : 1800
ABEND LOGREC        time : 3600
ABEND LOGRECSUMMARY time : 14400
---------------------------------
Incident Log Logstreams Properties
---------------------------------
Operations Log              :  OPERLOG
Logrec                      :  LOGSTREAM
LOGR Subsystem Active       :  TRUE
Primary Logger CDS          :  "CIMPROV.LOGR001"
Alternate Logger CDS        :  "CIMPROV.LOGR002"
Number of LSR for Primary CDS :  60
CEA OperLog Logstream Model   :  "CEA.MODEL.OPERLOG"
CEA Logrec  Logstream Model   :  "CEA.MODEL.LOGREC"
---------------------------------
Sysplex Dump Directory Properties
---------------------------------
Name              :  "MVSSPT.SYSPLEX.DMPDIR"
Size              :  112 cylinders
On Shared Volume  :  TRUE
Free Space Available :  TRUE
IPCS Initialized  :  TRUE
```

z/OSMF V1.13 Configuration Enhancements (1 of 2)

- Support for new z/OSMF system management tasks
  - Capacity Provisioning, Software Deployment, and ISPF
- Command simplification
  - Can provide a single file to define global settings or environment variables and export the location of the file to your shell session.
  - -file and -override file parameters will pre-pend IZU_CONFIG_DIR if no path is specified.
  - Configuration and override files are kept in the configuration directory and managed by the scripts
  - Script log files and report files are written 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/.
  - Flexibility is enhanced through the addition of overrides which allow you set options globally for any UID or GID values that you choose not to specify individually.
  - z/OS configuration tasks moved to -prime step
    - Previously were in -config, -prime and –finish
    - -config is now just accumulation of configuration data

z/OSMF V1.13 Configuration Enhancements (2 of 2)

- Migration Improvements
  - Now supports both override and configuration files
    - From any prior supported release
    - Can do either, or both at the same time
  - Report file is generated
- Security Simplification
  - Group Management
    - Scripts only create groups owned by z/OSMF (Administrator, User, Storage Administrator).
    - Will prompt for and use other groups if known
  - Authorization Mode switch
    - Can specify either SAF or Repository and then switch later.
    - Will generate all necessary commands for this switch
    - Authorization of additional users is based on Mode
- RAS Items
  - Additional messages for better log file documentation and diagnosis
  - Temporary file handling is improved
  - Input validation improved

Summary (1 of 2)

- IBM z/OS Management Facility (z/OSMF) V1.13 is a new release of the separate product for z/OS V1.13 customers (Program Number 5655-S28) . It consists of ten (10) FMIDs:
  - HSMA130 - z/OS Management Facility core
  - HSMA131 - z/OSMF ISPF
  - HSMA132 - z/OSMF RMF
  - HSMA133 - z/OSMF WLM
  - HSMA134 – z/OSMF Software Deployment
  - HSMA135 - z/OSMF Incident Log
  - HSMA136 - z/OSMF Capacity Provisioning
  - HSMA13A - z/OSMF Configuration Assistant
  - HSMA13F - z/OSMF DASD Management
  - HBBN700 - IBM WebSphere Application Server OEM Edition for z/OS
- Configuration for WebSphere Application Server OEM Edition and z/OSMF has 3 basic phases:
  1. Setup configuration files
  2. Create Security Definitions
  3. Build executables (run-time files)
  - Note: Most phases are driven through the use of z/OS UNIX configuration scripts. Phase 1 can be run interactively (interview style) or silently (fastpath mode)
- z/OSMF Incident Log exploits existing best practices for data management for problem determination
  - Instructions on setting up the z/OS functional prerequisites is documented in the z/OSMF Configuration Guide.

Summary (2 of 2)

- Security, Security, Security
  - Security definitions required for:
    - z/OS infrastructure prerequisites
      - CIM sample job provided (CFZSEC)
      - Additional sample jobs provided in z/OS V1.13
    - WebSphere Application Server OEM Edition
      - Tailored sample RACF commands generated by script
        - » Defaults in Backup slides
    - z/OSMF setup
      - Tailored sample RACF commands generated by script
        - » Defaults in Backup slides
  - It is likely that the shipped default values need to be changed to conform to your site security policies or conventions.

BACKUP

System z Social Media

- **System z official Twitter handle:**
  - @ibm_system_z
- **Top Facebook pages related to System z:**
  - Systemz Mainframe
  - IBM System z on Campus
  - IBM Mainframe Professionals
  - Millennial Mainframer
- **Top LinkedIn Groups related to System z:**
  - Mainframe Experts Network
  - Mainframe
  - IBM Mainframe
  - System z Advocates
  - Cloud Mainframe Computing
- **YouTube**
  - IBM System z
- **Leac em z:**
  - Evangelizing Mainframe (Destination z blog)
  - Mainframe Performance Topics
  - Common Sense
  - Enterprise Class Innovation: System z perspectives
  - Mainframe
  - MainframeZone
  - Smarter Computing Blog
  - Millennial Mainframer

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**
- **z/OS Hot Topics, Issue 21 and 23:**
  - http://ibm.com/systems/z/os/zos/bkserv/hot_topics.html
- **IBM z/OS Management Facility Configuration Guide (SA38-0652)**
  - Renamed from IBM z/OS Management Facility User's Guide in z/OSMF V1.12
- **IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide, Version 7.0 (GA32-0631)**
- **Program Directory for z/OS Management Facility (GI11-2886)**
- **IBM z/OS Management Facility License Information (GC52-1263)**

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.

Coexistence Considerations

- Coexistence applies to lower-level systems which coexist (share resources) with latest z/OS systems.
  - If you require the capability to fall back from z/OS Management Facility V1.13 to a lower level system (z/OS Management Facility V1.11 or z/OSMF V1.12 system), you require:
    - z/OS Management Facility V1.11
      - o APAR PM09519
      - o APAR PM27448
      - o APAR PM43649
    - z/OS Management Facility V1.12
      - o APAR PM27450
      - o APAR PM32108
      - o APAR PM43649
  - For both of these z/OSMF releases the SMP/E Fix Category **IBM.Coexistence.z/OSMF.V1R13** can be used to identify z/OSMF coexistence service

WAS OEM Default Directory Names and Descriptions

Directory	Permission bits	Description
/usr/lpp/zWebSphereOEM/V7R0	**755**	**Default read-only mount point for product file system**
/usr/lpp/zWebSphereOEM/V7R0/bin	**755**	**Script files WASOEM.sh, createWASOEMHFS.sh, updateConfigWASOEM.py, zpmt.sh and the plexname module.**
/usr/lpp/zWebSphereOEM/V7R0/zOS-config/zpmt/samples	**755**	**Samples of the default response files wasOEMDefault.responseFile, and wasOEMOverride.responseFile, and the environment shell script wasOEM_env.sh,**
zWebSphereOEM/V7R0/config1	**775**	**Default read-write mount point for configuration file system**
/etc/zWebSphereOEM/V7R0/conf	**755**	**Location of the environment shell script along with custom response file entries**
/var/zWebSphereOEM/V7R0/logs	**755**	**Location of the log files**
/tmp/zWebSphereOEM/V7R0/zpmt/work	**755**	**Work area for zPMT**

WAS OEM Default Directory Names and Descriptions ...

- /usr/ **- requires READ and EXECUTE permissions for running scripts, and for the IBM WebSphere Application Server OEM Edition for z/OS server ID.**
- /etc/ **- requires READ, WRITE, and EXECUTE permissions. These permissions enable you to copy, or modify the configuration file and default environment files.**
  - Note: If you cannot use the /etc/ directory to store the configuration file and the default environment files, you can specify a different working directory for these files when you receive the script prompts. These prompts only appear the first time you issue the WASOEM.sh command.
- /tmp/ **- requires READ and WRITE permissions to create directories, and to read and write files.**
- /var/ **- requires READ, WRITE, and EXECUTE permissions. These permissions enable you to run scripts with log output.**

z/OSMF Default Directory Names and Descriptions …

Directory	Permission bits	Description
/usr/lpp/zosmf/V1R13	**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.**

Groups and User IDs (1 of 2)

Variable	Value	Component
zConfigurationGroup	WSCFG1	WASOEM
zConfigurationGroupGID	2500	WASOEM
zLocalUserGroup	WSCLGP	WASOEM
zLocalUserGroupGID	2502	WASOEM
zServantGroup	WSSR1	WASOEM
zServantGroupGID	2501	WASOEM
zAdminAsynchTaskUserid	WSADMSH	WASOEM
zAdminUnauthenticatedUserid	WSGUEST	WASOEM
zAdminUserid	WOEMADM	WASOEM
zControlUserid	WSCRU1	WASOEM
zServantUserid	WSSRU1	WASOEM
zAdminAsynchTaskUid	2504	WASOEM
zAdminUid	2403	WASOEM
zAdminUnauthenticatedUid	2402	WASOEM
zControlUid	2431	WASOEM
zServantUid	2432	WASOEM
zSAFProfilePrefix	BBNBASE	WASOEM
zDefaultSAFKeyringName	WASKeyring.BBNBASE	WASOEM
zClusterTransitionName	BBNC001	WASOEM
zCellShortName	BBNBASE	WASOEM
zAdminAsynchProcName	BBN7ADM	WASOEM
zDaemonProcName	BBN7DMNB	WASOEM
zControlProcName	BBN7ACR	WASOEM
zServerShortName	BBNS001	WASOEM

Groups and User IDs (2 of 2)

Variable	Value	Component
IZU_ADMIN_NAME	**ZOSMFAD**	**ZOSMF**
IZU_ADMIN_UID	**9001**	**ZOSMF**
IZU_ADMIN_GROUP_NAME	**IZUADMIN**	**ZOSMF**
IZU_ADMIN_GROUP_GID	**9003**	**ZOSMF**
IZU_USERS_GROUP_NAME	**IZUUSER**	**ZOSMF**
IZU_USERS_GROUP_GID	**9004**	**ZOSMF**
IZU_WAS_PROFILE_PREFIX	**BBNBASE**	**ZOSMF**
IZU_CELL_SHORT_NAME	**BBNBASE**	**ZOSMF**
IZU_CLUSTER_TRANSITION_NAME	**BBNC001**	**ZOSMF**
IZU_CONTROL_USERID	**WSCRU1**	**ZOSMF**
IZU_SERVANT_USERID	**WSSRU1**	**ZOSMF**
IZU_WLM_GROUP_NAME	**WLMGRP**	**ZOSMF-WLM**
IZU_CP_QUERY_GROUP_NAME	**CPOQUERY**	**ZOSMF-CP**
IZU_CP_CONTROL_GROUP_NAME	**CPOCTRL**	**ZOSMF-CP**
IZU_CIM_ADMIN_GROUP_NAME	**CFZADMGP**	**ZOSMF - CIM**
IZU_CEA_HLQ	**CEA**	**ZOSMF-IL**

Security Resources and Required Access (1 of 4)

Class	Profile	UID/ GID	Users/Groups Authorized	Access	Component	Defined By
Group	WSCFG1	2500	WSSRU1,ZOSMFAD		WASOEM	BBOSBRAK
Group	WSCLGP	2502			WASOEM	BBOSBRAK
Group	WSSR1	2501			WASOEM	BBOSBRAK
User	WSADMSH	2504	WSCFG1		WASOEM	BBOCBRAK
User	WSGUEST	2402	WSCLGP		WASOEM	BBOCBRAK
User	WOEMADM	2403	WSCFG1		WASOEM	BBOSBRAK
User	WSCRU1	2431	WSCFG1		WASOEM	BBOSBRAK
User	WSSRU1	2432	WSSR1		WASOEM	BBOSBRAK
APPL	BBNBASE		WSCFG1,WSGUEST	READ	WASOEM	BBOCBRAK
EJBROLE	BBNBASE.adminsecuritymanager		WOEMADM	READ	WASOEM	BBOCBRAK
EJBROLE	BBNBASE.auditor		WOEMADM	READ	WASOEM	BBOCBRAK
EJBROLE	BBNBASE.administrator		WSCFG1	READ	WASOEM	BBOCBRAK
EJBROLE	BBNBASE.CosNamingRead		WSGUEST	READ	WASOEM	BBOCBRAK
EJBROLE	BBNBASE.CosNamingWrite		WSCFG1	READ	WASOEM	BBOCBRAK
EJBROLE	BBNBASE.CosNamingCreate		WSCFG1	READ	WASOEM	BBOCBRAK
EJBROLE	BBNBASE.CosNamingDelete		WSCFG1	READ	WASOEM	BBOCBRAK
EJBROLE	BBNBASE. monitor			NONE	WASOEM	BBOCBRAK
EJBROLE	BBNBASE. configurator			NONE	WASOEM	BBOCBRAK
EJBROLE	BBNBASE. operator			NONE	WASOEM	BBOCBRAK
EJBROLE	BBNBASE. deployer			NONE	WASOEM	BBOCBRAK

Security Resources and Required Access (2 of 4)

Class	Profile	UID/ GID	Users/Groups Authorized	Access	Component	Defined By
FACILITY	BBO.SYNC.BBNBASE.BBNC001			NONE	WASOEM	BBOCBRAK
FACILITY	BPX.WLMSERVER		WSSR1	READ	WASOEM	BBOCBRAK
FACILITY	IRR.DIGTCERT.LIST		WSCFG1	READ	WASOEM	BBOCBRAK
FACILITY	IRR.DIGTCERT.LISTRING		WSCFG1	READ	WASOEM	BBOCBRAK
FACILITY	BBO.TRUSTEDAPPS.BBNBASE.BBNC001		WSCFG1	READ	WASOEM	BBOCBRAK
STARTED	BBN7ADM.*		WSADMSH		WASOEM	BBOCBRAK
STARTED	BBN7DMNB.*		WSCRU1		WASOEM	BBOCBRAK
STARTED	BBN7ACR.*		WSCRU1		WASOEM	BBOCBRAK
STARTED	BBNS001A.*		WSCRU1		WASOEM	BBOCBRAK
STARTED	BBNS001S.*		WSSRU1		WASOEM	BBOCBRAK
SERVER	CB.*			NONE	WASOEM	BBOCBRAK
SERVER	CB.*.BBNC001.*		WSCRU1, WSSR1	READ	WASOEM	BBOCBRAK
SERVER	CB.*BBNC001ADJUNCT.*		WSCRU1	READ	WASOEM	BBOCBRAK
CBIND	CB.BIND.BBNBASE.**		WSCFG1	CONTROL	WASOEM	BBOCBRAK
CBIND	CB.BBNBASE.**			READ	WASOEM	BBOCBRAK
CERTAUTH	WebsphereCA					
KEYRING	WASKeyring.BBNBASE		WSCRU1, WSSRU1, WOEMADM, WSADMSH		WASOEM	BBOCBRAK
KEYRING	WASKeyring.BBNBASE.Root		WSCRU1		WASOEM	BBOCBRAK
KEYRING	WASKeyring.BBNBASE.Signers		WSCRU1		WASOEM	BBOCBRAK
CERT	DefaultWASCert.BBNBASE		WSCRU1		WASOEM	BBOCBRAK
CERT	DefaultDaemonCert.BBNBASE		WSCRU1		WASOEM	BBOCBRAK

Security Resources and Required Access (3 of 4)

Class	Profile	UID/GID	Users/Groups Authorized	Access	Component	Defined By
Group	**IZUADMIN**	**9003**			**ZOSMF**	**izuconfig1.cfg.rexx**
Group	**IZUUSER**	**9004**			**ZOSMF**	**izuconfig1.cfg.rexx**
Group	**IZUSTGA**	**9005**			**ZOSMF**	**izuconfig1.cfg.rexx**
User	**ZOSMFAD**	**9001**	**IZUADMIN**		**ZOSMF**	**izuconfig1.cfg.rexx**
Group	**WLMGRP**	**xxxx**			**WLM**	**Documentation**
Group	**CPOQUERY**		**ZOSMFAD**		**CP**	**CPOSEC1**
Group	**CPOCTRL**		**ZOSMFAD**		**CP**	**CPOSEC1**
Group	**CFZADMGP**		**ZOSMFAD**		**CIM**	**CEASEC**
Group	**CFZUSRGP**				**CIM**	**CEASEC**
APPL	**BBNBASE**		**IZUADMIN, IZUUSER**	**READ**	**ZOSMF**	**izuconfig1.cfg.rexx**
EJBROLE	**BBNBASE.izuUsers**		**IZUADMIN, IZUUSER**	**READ**	**ZOSMF**	**izuconfig1.cfg.rexx**
FACILITY	**BBO.SYNC.BBNBASE.BBNC001**		**WSCRU1**	**CONTROL**	**ZOSMF**	**izuconfig1.cfg.rexx**
FACILITY	**MVSADMIN.WLM.POLICY**		**WLMGRP**	**UPDATE**	**ZOSMF-WLM**	**izuconfig1.cfg.rexx**
SERVAUTH	**CEA.CEATSO.***		**IZUADMIN, IZUUSER, WSSRU1**	**READ**	**ZOSMF-ISPF**	**izuconfig1.cfg.rexx**
SERVAUTH	**CEA.CEAGETPS**		**IZUADMIN, IZUUSER**	**UPDATE**	**ZOSMF-IL**	**izuconfig1.cfg.rexx**
SERVAUTH	**CEA.CEADOCMD**		**IZUADMIN, IZUUSER**	**UPDATE**	**ZOSMF-IL**	**izuconfig1.cfg.rexx**
SERVAUTH	**CEA.CEAPDWB***		**IZUADMIN, IZUUSER**	**UPDATE**	**ZOSMF-IL**	**izuconfig1.cfg.rexx**
SERVAUTH	**CEA.CEADOCONSOLECMD**		**IZUADMIN, IZUUSER**	**UPDATE**	**ZOSMF-IL**	**izuconfig1.cfg.rexx**
DATASET	**CEA.***		**IZUADMIN, IZUUSER**	**ALTER**	**ZOSMF-IL**	**izuconfig1.cfg.rexx**

Security Resources and Required Access (4 of 4)

Class	Profile	UID/ GID	Users/Groups Authorized	Access	Component	Defined By
ZMFAPLA	BBNBASE.ZOSMF.**		IZUADMIN, IZUUSER	READ	ZOSMF	izuconfig1.cfg.rexx
ZMFAPLA	BBNBASE.ZOSMF.ADMINTASKS.**		IZUADMIN, IZUUSER	READ	ZOSMF	izuconfig1.cfg.rexx
ZMFAPLA	BBNBASE.ZOSMF.LINK.**		IZUADMIN, IZUUSER	READ	ZOSMF	izuconfig1.cfg.rexx
ZMFAPLA	BBNBASE.ZOSMF.CONFIGURATION_ASSISTANT.**		IZUADMIN, IZUUSER	READ	ZOSMF-CA	izuconfig1.cfg.rexx
ZMFAPLA	BBNBASE.ZOSMF.INCIDENT_LOG.**		IZUADMIN, IZUUSER	READ	ZOSMF-IL	izuconfig1.cfg.rexx
ZMFAPLA	BBNBASE.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.VIEW		IZUADMIN, IZUUSER	READ	ZOSMF-WLM	izuconfig1.cfg.rexx
ZMFAPLA	BBNBASE.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.MODIFY		IZUADMIN	READ	ZOSMF-WLM	izuconfig1.cfg.rexx
ZMFAPLA	BBNBASE.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.INSTALL		IZUADMIN	READ	ZOSMF-WLM	izuconfig1.cfg.rexx
ZMFAPLA	BBNBASE.ZOSMF.RESOURCE_MONITORING.**		IZUADMIN, IZUUSER	READ	ZOSMF-RMF	izuconfig1.cfg.rexx
ZMFAPLA	BBNBASE.ZOSMF.CAPACITY_PROVISIONING.**		IZUADMIN, IZUUSER	READ	ZOSMF-CP	izuconfig1.cfg.rexx
ZMFAPLA	BBNBASE.ZOSMF.SOFTWARE_DEPLOYMENT.**		IZUADMIN, IZUUSER	READ	ZOSMF-SD	izuconfig1.cfg.rexx
ZMFAPLA	BBNBASE.ZOSMF.ISPF.**		IZUADMIN, IZUUSER	READ	ZOSMF-ISPF	izuconfig1.cfg.rexx

Security Resources and Required Access for CEA

Class	Profile	UID / GID	Users/Groups Authorized	Access	Component	Defined By
User	**CEA**	**9002**	**SYS1**		**CEA**	**CEASEC**
STARTED	**CEA.****		**SYS1**		**CEA**	**CEASEC**
DATASET	**CEA.***		**SYS1**		**CEA**	**Sec Admin**
SERVAUTH	**CEA.CEAGETPS**			**NONE**	**CEA**	**CEASEC**
SERVAUTH	**CEA.CEADOCMD**			**NONE**	**CEA**	**CEASEC**
SERVAUTH	**CEA.CEADOCONSOLECMD**			**NONE**	**CEA**	**CEASEC**
SERVAUTH	**CEA.CEAPDWB***			**NONE**	**CEA**	**CEASEC**
SERVAUTH	**CEA.CEATSO***			**NONE**	**CEA**	**CEASEC**
SERVAUTH	**CEA.CEAPDWB.CEACHECKSTATUS**			**NONE**	**CEA**	**CEASEC**
SERVAUTH	**CEA.CEAPDWB.CEADELETEINCIDENT**			**NONE**	**CEA**	**CEASEC**
SERVAUTH	**CEA.CEAPDWB.CEAGETINCIDENT**			**NONE**	**CEA**	**CEASEC**
SERVAUTH	**CEA.CEAPDWB.CEAGETINCIDENTCOLLECTION**			**NONE**	**CEA**	**CEASEC**
SERVAUTH	**CEA.CEWPDWB.CEAPREPAREINCIDENT**			**NONE**	**CEA**	**CEASEC**
SERVAUTH	**CEA.CEAPDWB.CEASETINCIDENTINFO**			**NONE**	**CEA**	**CEASEC**
SERVAUTH	**CEA.CEAPDWB.CEASETPROBLEMTRACKINGNUMBER**			**NONE**	**CEA**	**CEASEC**
SERVAUTH	**CEA.CEAPDWB.CEAUNSUPPRESSDUMP**			**NONE**	**CEA**	**CEASEC**
SERVAUTH	**CEA.CEATSO.CEATSOREQUEST**			**NONE**	**CEA**	**CEASEC**
SERVAUTH	**CEA.CONNECT**			**NONE**	**CEA**	**CEASEC**
SERVAUTH	**CEA.SUBSCRIBE.WTO_***			**NONE**	**CEA**	**CEASEC**
SERVAUTH	**CEA.SUBSCRIBE.ENF_***			**NONE**	**CEA**	**CEASEC**
SERVAUTH	**CEA.SUBSCRIBE.PGM_***			**NONE**	**CEA**	**CEASEC**
SERVAUTH	**CEA.SUBSCRIBE.ENF_0068***			**NONE**	**CEA**	**CEASEC**

Security Resources and Required Access for CP

Class	Profile	UID / GID	Users/Groups Authorized	Access	Component	Defined By
User	CPOSRV				CP	CPOSEC1
STARTED	CPOSERV.*				CP	CPOSEC1
FACILITY	IXCARM.SYSCPM.SYSCPO		CPOSRV	UPDATE	CP	CPOSEC1
Group	CPOQUERY	xxxx	CPOSRV	USE	CP	CPOSEC1
Group	CPOCTRL	xxxx	CPOSRV	USE	CP	CPOSEC1
Group	CFZUSRGP		CPOSRV	USE	CIM	CFZSEC
DATASET	CPO.DOMAIN1.*		CPOSRV	UPDATE	CP	CPOSEC1
DATASET	CPOSRV.**		CPOSRV	CONTROL	CP	CPOSEC1
FACILITY	BPX.CONSOLE		CPOSRV	READ	CP	CPOSEC1
PTKTDATA	CFZAPPL SSIGNON(KEYMASKED(.....)) APPLDATA('NO REPLAY PROTECTION')				CP	CPOSEC1
PTKTDATA	CFZAPPL		CPOSRV	READ	CP	CPOSEC1
PTKTDATA	IRRPTAUTH.CFZAPPL.CPOSRV		CPOSRV	UPDATE	CP	CPOSEC1
FACILITY	IRR.RTICKETSERV		CPOSRV	READ	CP	CPOSEC1
SERVAUTH	CEA.CONNECT		CPOSRV	READ	CP	CPOSEC1
SERVAUTH	CEA.SUBSCRIBE.ENF_0068*		CPOSRV	READ	CP	CPOSEC1
FACILITY	HWI.APPLNAME.HWISERV		CPOSRV	READ	CP	CPOSEC1
FACILITY	HWI.TARGET.netname.cpc1		CPOSRV	CONTROL	CP	CPOSEC1
FACILITY	HWI.CAPREC.netname.cpc1.*		CPOSRV	READ	CP	CPOSEC1

Security Resources and Required Access for CIM (1 of 3)

Class	Profile	UID / GID	Users/Groups Authorized	Access	Component	Defined By
GROUP	CFZSRVGP	9501			CIM, ZOSMF	CFZSEC
GROUP	CFZADMGP	9502			CIM, ZOSMF	CFZSEC
GROUP	CFZUSRGP	9503			CIM, ZOSMF	CFZSEC
USER	CFZSRV	0	CFZSRVGP		CIM, ZOSMF	CFZSEC
CDT	WBEM				CIM, ZOSMF	CFZSEC
WBEM	CIMSERV		CFZSRV	CONTROL	CIM, ZOSMF	CFZSEC
WBEM	CIMSERV		CFZADMGP	CONTROL	CIM, ZOSMF	CFZSEC
WBEM	CIMSERV		CFZUSRGP	UPDATE	CIM, ZOSMF	CFZSEC
SURROGAT	BPX.SRV.**		CFZSRV	READ	CIM, ZOSMF	CFZSEC
FACILITY	BPX.SERVER		CFZSRV	UPDATE	CIM, ZOSMF	CFZSEC
FACILITY	BPX.SMF		CFZSRV	READ	CIM	CFZSEC
FACILITY	BPX.CONSOLE		CFZSRV	READ	CIM	CFZSEC
FACILITY	IXCARM.DEFAULT.CFZ_SRV_*		CFZSRV	UPDATE	CIM	CFZSEC
FACILITY	MRCLASS.CLUSTER		CFZADMGP	UPDATE	CIM	CFZSEC
FACILITY	MRCLASS.CLUSTER		CFZUSRGP	UPDATE	CIM	CFZSEC
FACILITY	MVSADMIN.*		CFZADMGP	UPDATE	CIM, ZOSMF	CFZSEC
FACILITY	MVSADMIN.*		CFZUSRGP	UPDATE	CIM, ZOSMF	CFZSEC
FACILITY	MVSADMIN.XCF.*		CFZADMGP	UPDATE	CIM	CFZSEC
FACILITY	MVSADMIN.XCF.*		CFZUSRGP	UPDATE	CIM	CFZSEC
FACILITY	MVSADMIN.XCF.CFRM		CFZADMGP	UPDATE	CIM	CFZSEC
FACILITY	MVSADMIN.XCF.CFRM		CFZUSRGP	UPDATE	CIM	CFZSEC

Security Resources and Required Access for CIM (2 of 3)

Class	Profile	UID / GID	Users/Groups Authorized	Access	Component	Defined By
FACILITY	IOSCDR		CFZADMGP	UPDATE	CIM	CFZSEC
FACILITY	IOSCDR		CFZUSRGP	UPDATE	CIM	CFZSEC
FACILITY	MVSADMIN.WLM.*		CFZADMGP	UPDATE	CIM, ZOSMF	CFZSEC
FACILITY	MVSADMIN.WLM.*		CFZUSRGP	UPDATE	CIM, ZOSMF	CFZSEC
FACILITY	MVSADMIN.WLM.POLICY		CFZADMGP	UPDATE	CIM, ZOSMF	CFZSEC
FACILITY	MVSADMIN.WLM.POLICY		CFZUSRGP	UPDATE	CIM, ZOSMF	CFZSEC
APPL	CFZAPPL		CFZSRV	READ	CIM, ZOSMF	CFZSEC
APPL	CFZAPPL		CFZADMGP	READ	CIM, ZOSMF	CFZSEC
APPL	CFZAPPL		CFZUSRGP	READ	CIM, ZOSMF	CFZSEC
STARTED	CFZCIM.*				CIM, ZOSMF	CFZSEC
DATASET	CEA.*		CFZADMGP, CFZUSRGP	ALTER	CIM, ZOSMF	CFZSEC
SERVAUTH	CEA.*		CFZADMGP, CFZUSRGP	UPDATE	CIM, ZOSMF	CFZSEC
SERVAUTH	CEA.CONNECT		CFZADMGP	UPDATE	CIM	CFZSEC
SERVAUTH	CEA.SUBSCRIBE		CFZADMGP	UPDATE	CIM	CFZSEC
SERVAUTH	CEA.SUBSCRIBE.ENF_0068*		CFZADMGP	UPDATE	CIM	CFZSEC
SERVAUTH	CEA.CEAGETPS		CFZADMGP	UPDATE	CIM, ZOSMF	CFZSEC
SERVAUTH	CEA.CEADOCMD		CFZADMGP	UPDATE	CIM, ZOSMF	CFZSEC
SERVAUTH	CEA.CEAPDWB		CFZADMGP	UPDATE	CIM, ZOSMF	CFZSEC
SERVAUTH	CEA.CEADOCONSOLECMD		CFZADMGP	UPDATE	CIM, ZOSMF	CFZSEC
SERVAUTH	CEA.*		CFZADMGP, CFZUSRGP	UPDATE	CIM, ZOSMF	CFZSEC

Security Resources and Required Access for CIM (3 of 3)

Class	Profile	UID / GID	Users/Groups Authorized	Access	Component	Defined By
SERVAUTH	CEA.CONNECT		CFZUSRGP	UPDATE	CIM	CFZSEC
SERVAUTH	CEA.SUBSCRIBE		CFZUSRGP	UPDATE	CIM	CFZSEC
SERVAUTH	CEA.SUBSCRIBE.ENF_0068*		CFZUSRGP	UPDATE	CIM	CFZSEC
SERVAUTH	CEA.CEAGETPS		CFZUSRGP	UPDATE	CIM, ZOSMF	CFZSEC
SERVAUTH	CEA.CEADOCMD		CFZUSRGP	UPDATE	CIM, ZOSMF	CFZSEC
SERVAUTH	CEA.CEAPDWB		CFZUSRGP	UPDATE	CIM, ZOSMF	CFZSEC
SERVAUTH	CEA.CEADOCONSOLECMD		CFZUSRGP	UPDATE	CIM, ZOSMF	CFZSEC
SERVAUTH	EZB.CIMPROV.*		CFZADMGP	READ	CIM	CFZSEC
SERVAUTH	EZB.CIMPROV.*		CFZUSRGP	READ	CIM	CFZSEC
PTKTDATA	GPMSERVE				CIM, ZOSMF	CFZSEC
PTKTDATA	IRRPTAUTH.GPMSERVE.*		CFZSRV	UPDATE	CIM, ZOSMF	CFZSEC

Security Resources and Required Access other(1 of 1)

Class	Profile	UID / GID	Users/Groups Authorized	Access	Component	Defined By
JESSPOOL	**your_system_name'.+MASTER+.SYSLOG.*.***		**CEA**	**ALTER**	**ZOSMF-IL**	**izuconfig1.cfg.rexx**
DATASET	**YOUR_MASTER_CATALOG'**		**ZOSMFAD**	**UPDATE**	**ZOSMF-IL**	**izuconfig1.cfg.rexx**
OPERCMDS	**MVS.DISPLAY.****		**CFZSRV**	**READ**	**ZOSMF-IL**	**izuconfig1.cfg.rexx**
OPERCMDS	**MVS.DUMP**		**CFZSRV**	**CONTROL**	**ZOSMF-IL**	**izuconfig1.cfg.rexx**
OPERCMDS	**MVS.MODIFY.JOB.CEA**		**CFZSRV**	**UPDATE**	**ZOSMF-IL**	**izuconfig1.cfg.rexx**

Other Scripts and Options

- izuauthuser.sh
  - Your security administrator can use this script to create a REXX EXEC with RACF commands for authorizing users to z/OSMF.
    - The content of the exec is automatically tailored for the plug-ins you select when configuring z/OSMF.
  - This script replaces the scripts izuaddcoreuser.sh and izuaddloguser.sh from z/OSMF V1.11
  - Repository mode
  - SAF mode
    - Authorizing a user is a two step process
      1. Running this script and resultant REXX EXEC
      2. Using the z/OSMF UI
  - SAF mode
    - Running this script and resultant REXX EXEC
- izusetup.sh
  - An option, **-add**, is added to the izusetup.sh script to allow you to add plug-ins to an already configured instance of z/OSMF.
    - Specify the –add option with the existing options -config to limit the scope of the script operations to new plug-ins only.
      - izusetup.sh -file <pathname/filename.cfg> -config [-overridefile <overridefilename>] [-fastpath] –add
  - An option, **-addlink**, is added to the izusetup.sh script provides an alternative means of adding a link to the z/OSMF navigation area.
    - In most cases, however, it is recommended that you use the Links task to add a link.
  - An option, **-service**, is added to the izusetup.sh script to allow you to deploy service to your z/OSMF instance without re-configuration.

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/V1R13
##
Setup PATH so the zOSMF binaries are accessible.
export PATH=.:/usr/lpp/zosmf/V1R13/bin:$PATH
##
For problems with out of memory starting jvms
export _BPX_SHAREAS=NO
```

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