

z/OS Management Facility (z/OSMF) V1.12 Implementation and Configuration

Session: 8698



Greg Daynes

gdaynes@us.ibm.com

z/OS Installation and Deployment Architect

Permission is granted to SHARE Inc. to publish this presentation paper in the SHARE Inc. proceedings; IBM retains the right to distribute copies of this presentation to whomever it chooses

Agenda

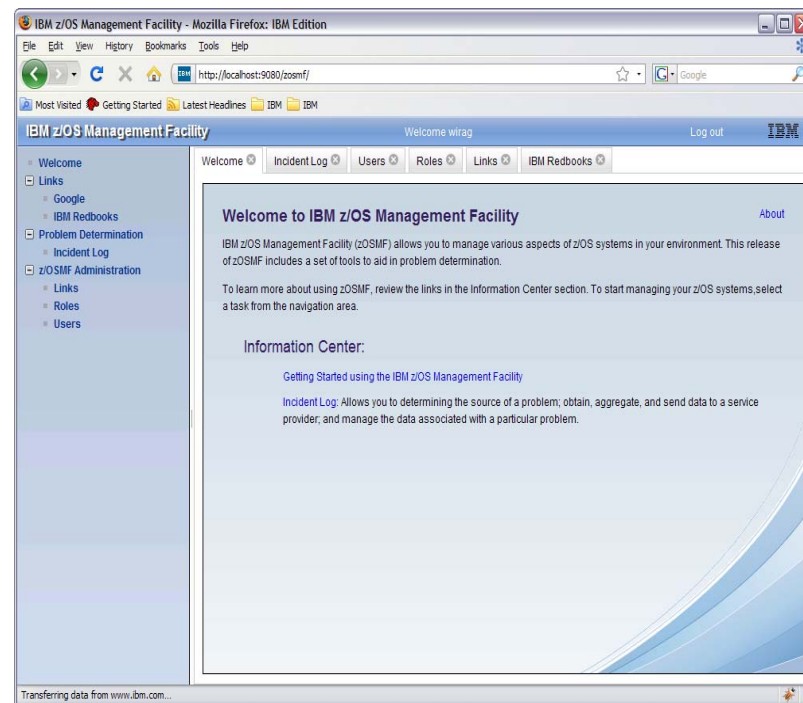
- Overview of z/OS Management Facility
- Ordering and Installing the software (code)
 - Via ServerPac or SMP/E
- Setup and configuration overall process
 - **Configure WebSphere Application Server OEM Edition**
 - **Configure z/OS prerequisites for Incident Log**
 - **Configure z/OSMF**

Greg's Disclaimers

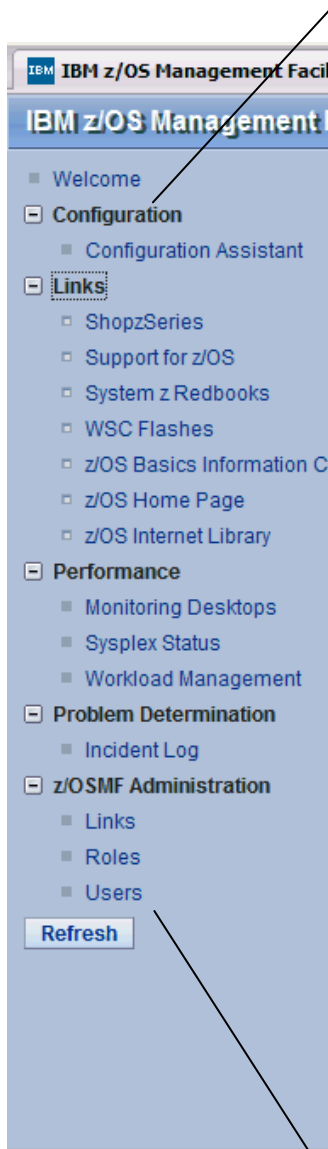
- z/OSMF enables the user to tailor many different configuration settings. Not all of those options will be covered in this presentation.
- Customers existing configurations are different. Some settings may need to be different in your environment. For example:
 - If you use existing User IDs or Security 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 new product for z/OS that provides support for a modern, Web-browser based management console for z/OS.
- **First release is z/OSMF V1.11, introduced with z/OS V1.11**
- **Helps system programmers to 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) guides you through tasks and helps provide simplified operations.



IBM z/OS Management Facility



- **Configuration** category

- **Configuration Assistant for z/OS Communication Server**

- 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 (R12)

- **Monitoring Desktops task**

- Allows you to monitor the performance of the z/OS sysplexes or Linux (System z or Intel) images in your environment. You can monitor most of the metrics supported by the Resource Measurement Facility (RMF) Monitor III, create and save custom views of the metrics, and display real-time data as bar charts

- **Sysplex Status task**

- Allows you to quickly assess the performance of the workloads running on the z/OS sysplexes in your environment. This task also provides a single location from which you can define the z/OS sysplexes to be monitored in the Monitoring Desktops task.

- **Workload Manager Policy Editor**

- Facilitate the creation and editing of WLM service definitions, installation

- **Problem Determination** category

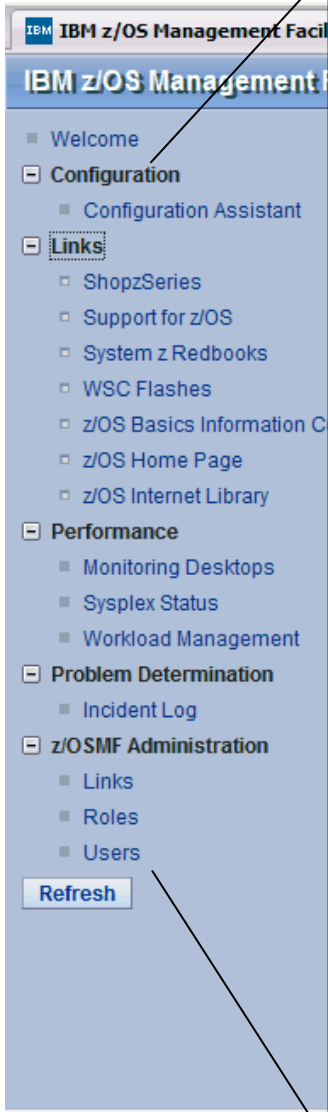
- **Incident Log**

- Provides a consolidated list of SVC Dump related problems, along with details and diagnostic data captured with each incident. It also facilitates sending the data for further diagnostics.

- **z/OSMF Administration** category

- z/OSMF authorization services for administrator: add users, define roles, dynamically add links to non-z/OSMF resources.

IBM z/OS Management Facility



- **Configuration** category
 - **Configuration Assistant for z/OS Communication Server**
 - Simplified configuration and setup of TCP/IP policy-based networking functions
- **Links** category
 - Links to resources - provide common launch point for accessing resources beyond z/OSMF
- **Performance** category (Performance)
 - **Monitoring Desktops**
 - Allows you to monitor z/OS or Linux (System z or Intel) images in your environment. You can view the Resource Measurement views of the metrics, and display real-time data.
 - **Sysplex Status**
 - Allow you to monitor the z/OS sysplexes in your environment. You can define the z/OS sysplexes.
 - **Facility Configuration**
 - Facilitate the configuration of z/OSMF.
- **Problem Determination** category
 - **Incident Log**
 - Provides console messages, along with details and diagnostic data captured with each message, for the data for further diagnostics.
- **z/OSMF Administration** category
 - z/OSMF authorization services for administrator: add users, define roles, dynamically add links to non-z/OSMF resources.

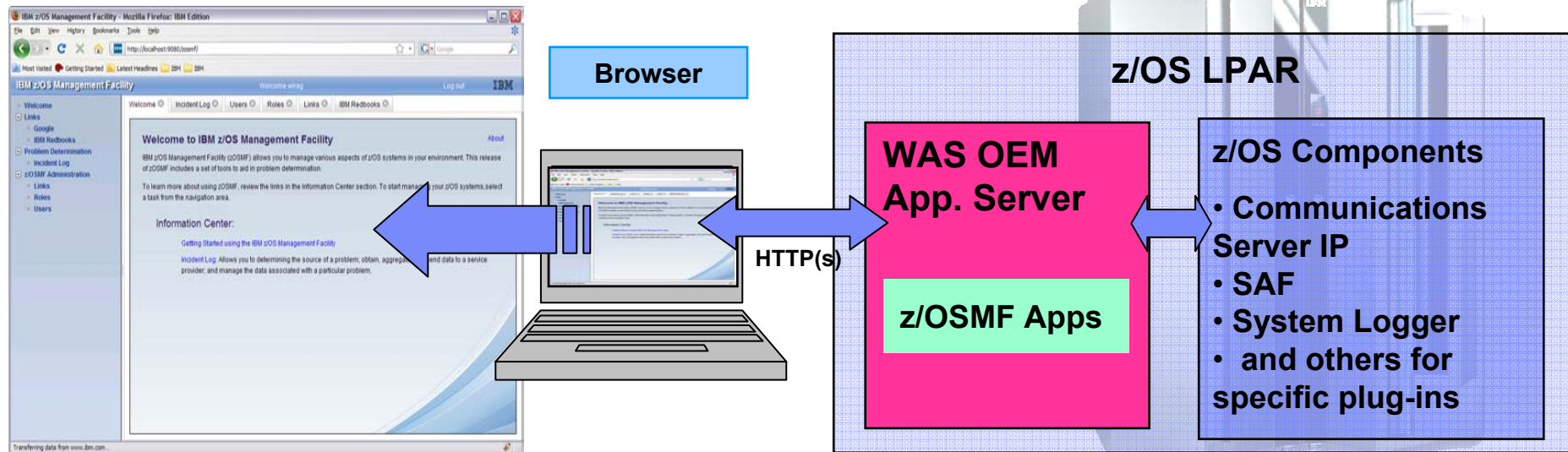
New in z/OSMF V1.13
a Software Deployment capability
Attend session 9039:
z/OS Software Deployment
Thursday 8AM Room 201B

IBM z/OS Management Facility V1.12

- IBM z/OS Management Facility (z/OSMF) V1.12 (5655-S28) provides new and enhanced applications for system programmers:
 - A new system management task, **Workload Management (policy editor)**, can simplify the creation, modification, and review of z/OS WLM service definitions, potentially reducing many hours of manual tasks down to minutes.
 - New system management tasks, **Sysplex Status and Monitoring Desktops**, can provide real-time status of resources of all your servers, sysplexes, as well as Linux images from one location, enabling you drill down in just second to see the detailed health of all monitored systems.
 - The **Configuration Assistant for the z/OS Communications Server** (available since z/OSMF V1.11) has been updated with added support for IP security IKEv2, new cryptographic and authentication algorithms, and enhancements to the support for Application Transparent Transport Layer Security.
 - The **Incident Log** capability (available since z/OSMF V1.11) adds support for encrypted parallel FTP dumps to be sent to IBM, and allows you to add custom information to individual incidents. These enhancements are intended to help you manage problem data more easily.

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

IBM z/OS Management Facility

- **The IBM z/OS Management Facility is a licensed program product**
 - z/OS Management Facility (5655-S28)
 - Same program number as z/OS Management Facility V1.11
 - z/OS Management 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 and z/OS V1.11**
 - The Configuration Assistant for z/OS Communications Server requires z/OS V1.11
- **z/OSMF V1.12 requires z/OS V1.12**

No Additional Charge = Free

IBM z/OS Management Facility

- z/OSMF V1.11 consists of two (2) FMIDs:
 - HBBN700 - IBM WebSphere Application Server OEM Edition for z/OS
 - HSMA110 - z/OS Management Facility (core and applications)

- z/OSMF V1.12 consists of six (6) FMIDs:
 - HBBN700 - IBM WebSphere Application Server OEM Edition for z/OS
 - HSMA120 - z/OS Management Facility core
 - HSMA122 - z/OSMF RMF
 - HSMA123 - z/OSMF WLM
 - HSMA125 - z/OSMF Incident Log
 - HSMA12A – z/OSMF Configuration Assistant

Ordering - ShopzSeries

- Shopz
- Product catalog
- Help
- News
- Feedback
- Customer service

Shopz >

Proc



ShopzSeries

FMIDs

Catalog

Country/

Package

Group

Language

MVS: z/OS

FMIDs for z/OS Management Facility	
FMID	Description
HBBN700	IBM WebSphere Application Server OEM Edition for z/OS
HSMA12A	IBM z/OS Management Facility - Config Assist Plug-in
HSMA120	IBM z/OS Management Facility
HSMA122	IBM z/OS Management Facility - RMF Plug-in
HSMA123	IBM z/OS Management Facility - WLM Plug-in
HSMA125	IBM z/OS Management Facility - Incident Log Plug-in

[Terms of use](#) [Privacy](#) [Close \[X\]](#)

[\[5655-P97\]](#) Encryption Facil Encrypt Ser [\[FMIDs\]](#) 1.02.00 English (US)

Prerequisites

■ Client machine (no client machine install requirements)

– z/OSMF V1.11

- Windows XP operating system
 - Mozilla Firefox 3.0.6
 - Mozilla Firefox 2
 - Internet Explorer 7
 - Internet Explorer 6

– z/OSMF V1.12

- Microsoft Windows Vista, 32 bit Windows 7, and Windows XP
 - Mozilla Firefox 3.0.15
 - Mozilla Firefox 3.5
 - Internet Explorer 7
 - Internet Explorer 8
- Note: In the future, IBM z/OS Management Facility browser and client machine platform support is planned to be expanded to include support for Microsoft Windows 7 Professional Edition 64 bit with the 32 bit version of Firefox 3.5 and Internet Explorer 8 Web browsers.

* Statements regarding IBM future direction and intent are subject to change or withdrawal, and represents goals and objectives only.

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

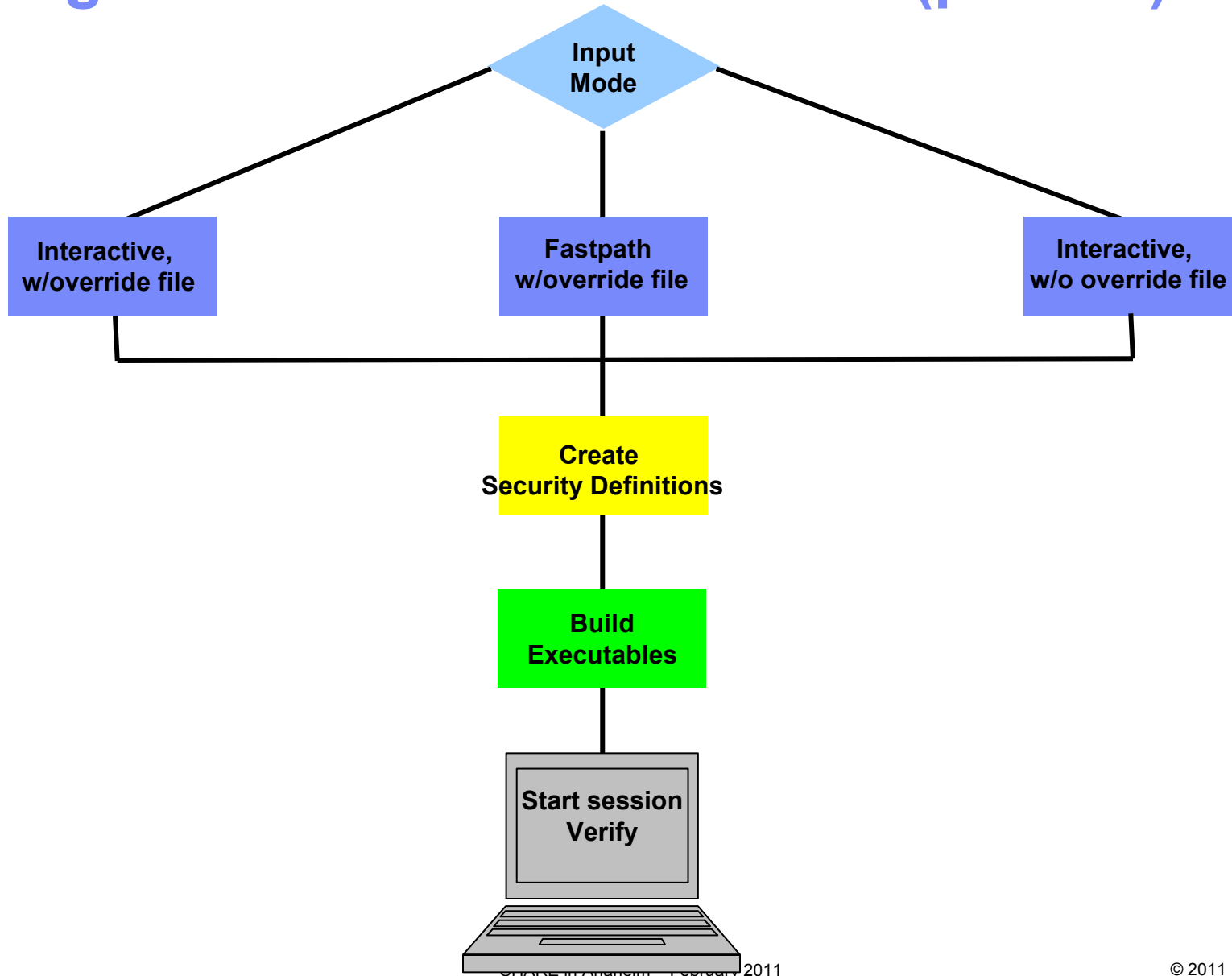
Software Installation

- z/OSMF V1.11 or z/OSMF V1.12 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 V1.11 or z/OSMF V1.12 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
- **Setting additional instances (test, service, backup)**
 - Follow the Configuration guide for instructions

Configuration Process Overview

- Both WebSphere Application Server OEM Edition and z/OSMF have three basic phases for configuration
 1. Setup configuration files
 2. Create Security Definitions
 3. Build executables (run-time files)
- Most phases are driven through the use of z/OS UNIX configuration scripts
 - Phase 1 scripts can be run:
 - Interactively with an override 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.

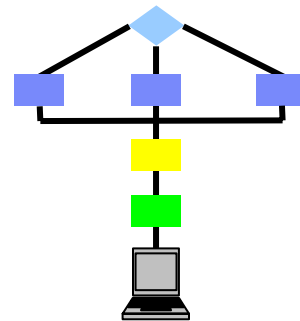
- In response to each prompt, you must either press Enter to use the configuration file value, or type your installation specific value.

–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.

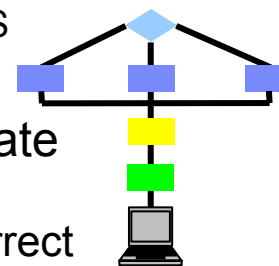
WebSphere Application Server OEM Edition Configuration Process

- The configuration process occurs in three stages, and in the following order:
 1. **Stage 1 – Configuration**
 - a. **Interactive mode (with an response/override file)**
 - Called “Advanced”
 - b. **Fastpath mode**
 - c. **Interactive mode (without an response/override file)**
 - Called “Typical”
 2. **Stage 2 - Security setup**
 - **Submit Security Customization Jobs**
 - **BBOSBRAK, BBOSBRAM, and BBOCBRAK**
 3. **Stage 3 - Server instance creation**
 - **Invoke WASOEM.sh in create mode**



WebSphere Application Server OEM Edition Configuration Hints and Tips

- For z/OSMF V1.11
 - **If you install WAS OEM Server Fix Pack level 7.0.0.7 level**
 - APARs PM02335, PM02337, PM02390-PM02426, PTFs UK52509-UK52546
 - Use the Second Edition of the IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide (GA32-0631-01)
 - **If you install WAS OEM Server Fix Pack level 7.0.0.9 level**
 - APARs PM13020- PM13058, PTFs UK56521-UK56529, UK56534, UK56536, UK56538, UK56540-UK56566
 - Use the Third Edition of the IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide (GA32-0631-02)
- z/OSMF V1.12 requires WAS OEM Server Fix Pack level 7.0.0.9 level
 - APARs PM13020- PM13058, PTFs UK56521-UK56529, UK56534, UK56536, UK56538, UK56540-UK56566
 - Use the Third Edition of the IBM WebSphere Application Server OEM Edition for z/OS Configuration Guide (GA32-0631-02)
- 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.

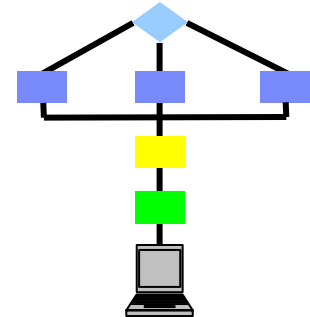
AUTOUID/AUTOGID

- 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/AUTOUID to not require overrides)
 - 17 Port defaults
 - 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

Stage 1: 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.

Stage 1: 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.
 - 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.

Stage 1: 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.

- o This script accepts the responseFile after it has been tailored and produces three (3) security jobs which are submitted in the next stage.

Stage 2: 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/>

Stage 2: Security Jobs

The security jobs must be run in the following order:

1. The BBOSBRAK security job

- Running this job creates the following 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. You must use the password or password phrase that you assign to this user ID when you logon to the IBM WebSphere Application Server OEM Edition for z/OS administrative console.
- 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 the following 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 OEM Edition for z/OS nodes using the IBM WebSphere Application Server OEM Edition for z/OS common groups and owner user ID.
- After this job finishes, verify that the directories exist on each system and have the correct permissions.

3. The BBOCBRAK security job

- Running this job creates the following RACF users and profiles that are required by the IBM WebSphere Application Server OEM Edition for z/OS.
- When this job completes, all user IDs listed in the previous section for job BBOCBRAK should be defined in the RACF database on each target system for the cell.

Stage 2: 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`

Stage 3: 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

Stage 3: 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.BBNODE.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 for Full Incident Log Functionality

- z/OSMF's Incident Log exploits existing best practices for data management for problem determination.
 - Sysplex Dump Directory (required)**
 - Use of System Logger for SYSLOG (OPERLOG) and LOGREC**
 - z/OSMF V1.12 Incident Log is planned to also support the creation of diagnostic log snapshots based on the SYSLOG and LOGREC data sets, as well as the OPERLOG and LOGREC sysplex log streams.
 - Dump analysis and elimination (DAE) is active and its symptom data set is available**
 - Automatic Dump Data Set Allocation**
 - AMATERSE program is enabled to run**
 - CEA and System REXX components are available**
 - CIM server setup can be configured along with z/OSMF
 - z/OSMF V1.12 the Incident Log supports parallel encrypted File Transfer Protocol FTP to IBM**
 - Incident log leverages the Problem Documentation Upload Utility, which offers encryption and parallel FTP of diagnostic data to IBM. Information can be found at
 - o <http://www14.software.ibm.com/webapp/set2/sas/f/zaid/pdof.html>
- Note: For more information on these topics see *z/OS V1R11.0 MVS Diagnosis Tools and Service Aids (GA22-7589)*

Configure z/OS for Full Incident Log Functionality

■ 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 uses the sysplex dump directory to 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

- **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

Note: Recommended for multi-system Parallel Sysplex environments

Configure z/OS for Full Incident Log Functionality

■ **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

■ 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

- **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
 - **Ensure that SYS1.MIGLIB is APF-authorized**

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 ¹	<ul style="list-style-type: none"> ▪ Log snapshots are NOT gathered¹ ▪ Planned for z/OSMF V1.12*
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 ²
AMATERSE program is enabled	Dump included in diagnostic data gathered and sent	Can NOT prepare or send any diagnostic data
Problem Documentation Upload Utility	Supports parallel encrypted FTP to IBM ³	Dump not encrypted nor broken into multiple data sets

1 – In z/OSMF V1.11, DASD-only logs can be used in monoplex environments, but not in basic sysplex environments. In z/OSMF V1.12, Incident Log is planned to also support the creation of diagnostic log snapshots based on the SYSLOG and LOGREC data sets, as well as the OPERLOG and LOGREC sysplex log streams.

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

3 – z/OSMF V1.12 function

System prerequisites for the Monitoring Desktops and Sysplex Status tasks (z/OSMF V1.12 only)

- 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 GPMSEIVE address spaces in your sysplex:
 - ROUTE *ALL,D A,GPMSEIVE
 - ROUTE *ALL,D A,GPM*
- For information about setting up the DDS server, see *z/OS RMF User's Guide*, SC33-7990.

z/OSMF Configuration Process

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

1. Stage 1 – Configuration

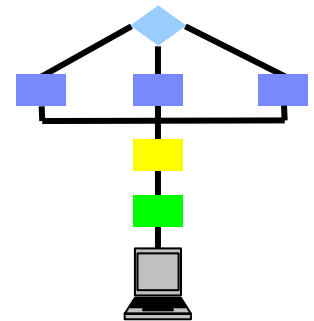
- a. Interactive mode (with an override file)
- b. Fastpath mode
- c. Interactive mode (without an override file)

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*



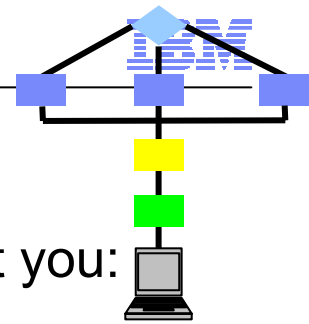
z/OSMF V1.12 Configuration Enhancements

- **The following enhancements were made in z/OSMF V1.12**
 - Configuration log file management
 - Fewer configuration log files in z/OSMF V1.12
 - z/OSMF V1.11 had multiple logfiles, each sub script generating it's own. This is now consolidated
 - The location of the configuration log file is now customizable
 - In z/OSMF V1.11 the log files were located in the configuration directory
 - Ability to run the –prime multiple times
 - CIM Server setup is now performed separately
 - New quick start procedure is added to the CIM User's Guide.
 - SAMPLIB jobs to setup the CIM server as started task also provided
 - Initial configuration can have 0-N plug-ins
 - Can optionally add plug-ins that weren't already configured
 - Improve and streamline the handling of configuration parameters
 - New parameters added (e.g., to configure z/OSMF plug-ins)
 - Some configuration parameters have changed from z/OSMF V1.11 to z/OSMF V1.12
 - A few parameters have been deprecated: some parameters have been removed or renamed.

z/OSMF Configuration Roles and Authorities

Action to perform	Script invocation	Performed by
Step 1: Create the initial configuration	<pre>izusetup.sh -file <pathname/filename>.cfg - config [...other options...]</pre>	Superuser
Step 2: Run the security commands	<code><IZU_CONFIG_DIR>/izuconfig1.cfg.rexx</code>	Security Administrator
Step 3: Verify the RACF security setup	<pre>izusetup.sh -file <pathname/filename>.cfg -verify racf</pre>	Security Administrator
Step 4: Prime the z/OSMF data file system	<pre>izusetup.sh -file <pathname/filename>.cfg - prime</pre>	Superuser
Step 5: Complete the setup	<pre>izusetup.sh -file <pathname/filename>.cfg -finish</pre>	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



- For z/OSMF V1.11, if you haven't started yet, make sure that you:
 - *Install z/OSMF APAR PK97274/PTF UK52956*
 - Use the Third Edition (-02 level), December 2009 of the IBM z/OS Management Facility User's Guide
- For z/OSMF V1.12, use the IBM z/OS Management Facility Configuration Guide *Version 1 Release 12*
- Using 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
 - PARMLIB data set names
 - PARMLIB suffixes
 - Whether to configure CIM
 - In z/OSMF V1.12 recommendation is to specify “N” and use the CIM sample jobs
 - Whether to configure CEA (Whether to configure the Incident Log Task)

- 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 */etc/zosmf/izuhlt.ovr* override file.**

Sample z/OSMF V1.12 Override File

```
# Licensed Materials - Property of IBM
# 5655-S28
# Copyright IBM Corp. 2009, 2010
#
# Status = HSMA120
IZU_OVERRIDE_FILE_VERSION=1.12.0
IZU_ADMIN_UID=AUTOUID
IZU_ADMIN_GROUP_GID=AUTOGID
IZU_WAS_CONFIG_FILE_KNOWN=Y
IZU_WAS_CONFIG_FILE_LOCATION=/etc/zWebSphereOEM/V7R0/conf/CONFIG1/CONFIG1.responseFile
IZU_DATA_FS_NAME=MVSBUILD.IZUDATA
IZU_DATA_FS_TYPE=ZFS
IZU_DATA_FS_SIZE=500
IZU_DATA_FS_VOLUME=ZCSDW
IZU_CIM_GROUP_ID=AUTOGID
IZU_CEA_UID=AUTOUID
IZU_CEA_GROUP_ID=AUTOGID
IZU_CEA_PARM_NAME=MF
IZU_IEA_PARM_NAME=MF
IZU_PARMLIB=MVSBUILD.ZOSMF.PROCLIB
IZU_PARMLIB_SOURCE=SYS1.PARMLIB.INSTALL
IZU_INCIDENT_LOG=Y
IZU_CIM_SETUP=N
IZU_ADMIN_PROC=ISPFPROC
IZU_ADMIN_ACCOUNT=FRED
IZU_COUNTRY_CODE=000
IZU_BRANCH_CODE=035
IZU_STORAGE_VALUE="VOLSER(ZCSDW,ZCSDWX,ZCSDWY)"
#IZU_STORAGE_VALUE="STORCLAS(STRCLS)"
#IZU_STORAGE_VALUE="VOLSER(VOL1,VOL2,VOL3,VOL4,VOL5,VOL6,VOL7)"
IZU_IL_CONFIGURE=Y
IZU_CA_CONFIGURE=Y
IZU_WLM_CONFIGURE=Y
IZU_RMF_CONFIGURE=Y
IZU_CIM_CONFIGURE=Y
```

Complete override file used

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 file for storing your configuration information (the configuration file). If you retained the configuration file from a previous configuration of z/OSMF, and you wish to re-use some or all of the values for this configuration, you can select that file to use when you invoke this script.
 - If the z/OSMF data file system is not already allocated and mounted, the script allocates the data file system and mounts it at the mount point you specify. The default mount point is `/var/zosmf/data`.
 - The script also creates a REXX exec with RACF commands for creating the necessary security definitions for your installation.
 - For z/OSMF V1.12 the REXX script will be tailored based on the set of plug-ins selected
 - If you specify that the script is to set up the Incident Log task, the generated REXX exec will include the RACF commands that your security administrator can use to create security definitions for the CIM server, CEA, and other system components, and the security definitions that allow the z/OSMF administrator to access and run the Incident Log task.
- 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

- 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.
- Prior to running the REXX EXEC review the RACF commands and comments making any necessary changes

Recommend making changes to a copy of the file

–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

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 > 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 called **izuracfverify.report**, which is stored by default in the following location:
 - `/etc/zosmf/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, which is mounted by default at `/var/zosmf/data`
 - Changes the permissions and ownership of the directories and files in `/var/zosmf/data`
 - 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.
- In z/OSMF V1.11 priming the data file system can be done only once.
- 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, which includes creating a symbolic link.
 - Updates the WebSphere Application Server configuration
- The script also prepares your z/OS system for running the Incident Log task, if you chose to configure this task earlier. Specifically, the script performs the following z/OS setup actions:
 1. Copies the IEADMCnn member to the installation PARMLIB you specified earlier.
 2. Copies the IBM-supplied CEAPRM00 member to the installation PARMLIB you specified earlier and modifies it.
 3. Activates the new CEAPRMnn member.
 4. The script verifies the setup for all 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 z/OS system components such as:
 - ▶ Sysplex dump directory, System logger, Common event adapter (CEA), and System REXX.
 5. Upon completion, the script issues an informational message (IZUG349I) that contains the URL that you use to log in to z/OSMF.
- 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`

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`.

<pre> ----- 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 : 999 Country : 000 Storage Value : STANDARD HLQ : CEA </pre>		<pre> SLIP OperLog time : 3540 SLIP LOGREC time : 3540 SLIP LOGRECSUMMARY time : 14400 DUMP OperLog time : 3540 DUMP LOGREC time : 3540 DUMP LOGRECSUMMARY time : 14400 ABEND OperLog time : 3540 ABEND LOGREC time : 3540 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 </pre>
<pre> ----- continue → </pre>		

Migration Considerations

- If you have a z/OSMF V1.11 on a z/OS V1.10 or z/OS V1.11 system and want to migrate your configuration file to z/OSMF V1.12 format, there is script support for doing that.
 - Requires that z/OSMF V1.11 be at the PTF UK52956/APAR PK97274 (or higher) prior to migration
 - Use **izumigrate.sh**, to migrate the z/OSMF V1.11 configuration file to the z/OSMF V1.12 format, see the z/OSMF Configuration Guide
 - Run the setup steps via **izusetup.sh** to enable the z/OSMF V1.12 level of plug-ins
 - In z/OSMF V1.12 all plug-ins are optional.
 - During the -config step, you can choose which plug-ins are configured
 - After that you can use the **–add** option to add the new plug-ins added in z/OSMF V1.12

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 V1.12 to a lower level system (z/OS Management Facility V1.11 on a z/OS 1.10 or z/OS V1.11 system), and retain the use of the data repository from z/OS Management Facility V1.12, you require
 - **APAR PM09519** z/OS Management Facility V1.11
 - o SMP/E Fix Category **IBM.Coexistence.z/OSMF.V1R12** can be used to identify z/OSMF coexistence service
 - z/OS BCP APAR **OA32285** on the lower level z/OS systems (z/OS V1.10 or V1.11)
 - o If this is **not** installed, under certain circumstances, some datasets will not be deleted when the rest of the incident is deleted.

New 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 the previous release
- Authorizing a user is a two step process
 1. Running this script
 2. Using the z/OSMF UI

■ **izusetup.sh**

- A new option, **-add**, is added to the izusetup.sh script.
 - This option allows you to add plug-ins to an already configured instance of z/OSMF.
 - o Specify the **-add** option with the existing options **-config**, **-prime**, and **-finish** to limit the scope of these script operations to new plug-ins only.
- A new option, **-addlink**, is added to the izusetup.sh script.
 - This option 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.
- A new option, **-service**, is added to the izusetup.sh script.
 - This option allows you to deploy service to your z/OSMF configuration.

Summary

- **IBM z/OS Management Facility (z/OSMF) V1.11 was a new product for z/OS customers (Program Number 5655-S28)**
 - The product consists of two (2) FMIDs:
 - HBBN700 - IBM WebSphere Application Server OEM Edition for z/OS
 - HSMA110 - z/OS Management Facility (core and plug-ins)
- **IBM z/OS Management Facility (z/OSMF) V1.12 is a new release of the separate product for z/OS V1.12 customers (Program Number 5655-S28)**
 - The product consists of two (6) FMIDs:
 - HBBN700 - IBM WebSphere Application Server OEM Edition for z/OS
 - HSMA120 - z/OS Management Facility core
 - HSMA122 - z/OSMF RMF
 - HSMA123 - z/OSMF WLM
 - HSMA125 - z/OSMF Incident Log
 - HSMA12A - z/OSMF Configuration Assistant
- **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.

BACKUP

Additional information

- z/OS Management Facility Web Page
 - <http://www.ibm.com/systems/z/os/zos/zosmf/>
- Program Directory for z/OS Management Facility GI11-2886-01
- IBM z/OS Management Facility (R11) User's Guide SA38-0652-02
- IBM z/OS Management Facility (R12) Configuration Guide SA38-0652-03
- IBM WebSphere® Application Server OEM Edition for z/OS Configuration Guide, Version 7.0, GA32-0631-02
- z/OS Hot Topic Newsletter (August 2009 – Issue 21) GA22-7501-17
- IBM z/OS Management Facility education modules in IBM Education Assistant
- z/OS Hot Topics, Issue 21:
 - ibm.com/systems/z/os/zos/bkserv/hot_topics.html
- z/OS Hot Topics, Issue 23:
 - ibm.com/systems/z/os/zos/bkserv/hot_topics.html

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.

New: Adding an plug-in to a z/OSMF configuration

- **z/OSMF 1.12 provides support to optionally add plug-ins later that may not be configured initially.**
 - `izusetup.sh -file <pathname/filename.cfg> [-overridefile <overridefilename>] [-fastpath] -add -config`
 - Indicate which plug-ins are to be added in your override file, which you specify on the `-overridefile` option.
 - In the override file, mark the plug-ins to be added with the character **A**.
 - Example: To add the Workload Management plug-in to a configured instance of z/OSMF. which has previously deployed the Incident Log plug-in and the Configuration Assistant plug-in, while omitting the Resource Monitoring plug-in.
 - » `IZU_IL_CONFIGURE=Y`
 - » `IZU_CA_CONFIGURE=Y`
 - » `IZU_WLM_CONFIGURE=A`
 - » `IZU_RMF_CONFIGURE=N`
 - If you omit the override file, the script prompts you for the plug-ins to be added.
 - Respond to the prompt with one or more of the following plug-in identifiers separated by comma:
- **On completion, the `izusetup.sh` script creates a REXX exec with RACF commands for creating the security definitions for your installation.**
 - The exec name is a concatenation of your configuration file name and **".rexx"**.
 - If you use `"izuconfig1.cfg"` as your configuration file name, for example, the exec is created as `"izuconfig1.cfg.WLM.rexx"`
- You need to complete all four steps, supplying the `-add` parameter, to complete the add operation