#SHAREorg

SHARE
Technology · Connections · Results

z/OSMF Configuration made easy!

Anuja Deedwaniya
IBM Corp.
anujad@us.ibm.com

August 2013
Session Number **14247**

SHARE in Boston

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.

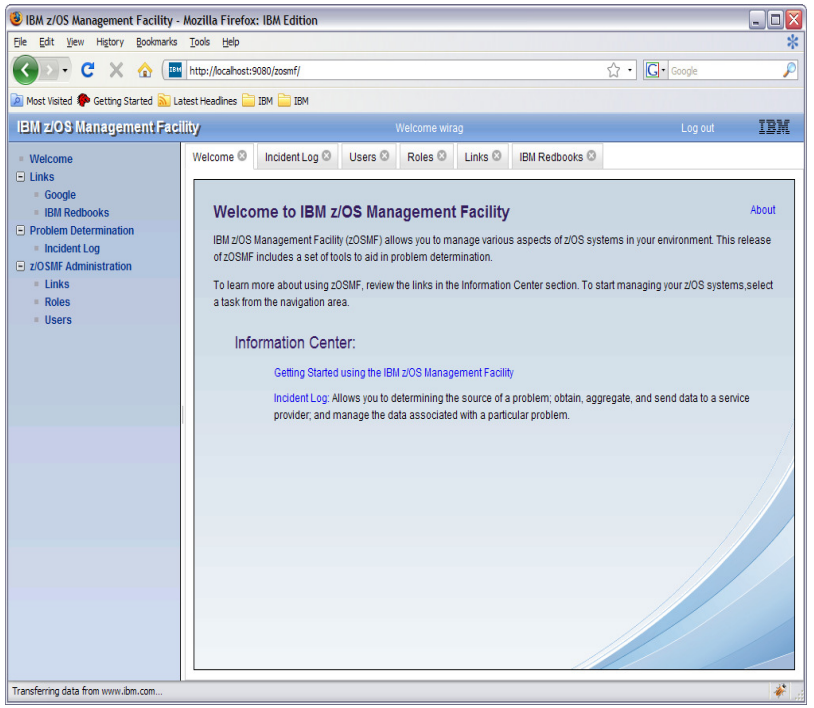
Agenda

- Overview of z/OS Management Facility V2.1
- Ordering and Installing z/OS Management Facility V2.1
  - Via ServerPac or SMP/E
- Setup and configuration overall process
  - z/OSMF requirements
  - Configure z/OSMF
    - Basic installation, no plug-ins
- Next steps
  - Add Plug-ins
    - Configure z/OS prerequisites for z/OSMF Plug-ins
    - Configure z/OSMF plug-ins
  - Authorizing additional userids
- Migration

Thanks to Frank Paxhia for his contribution to this presentation

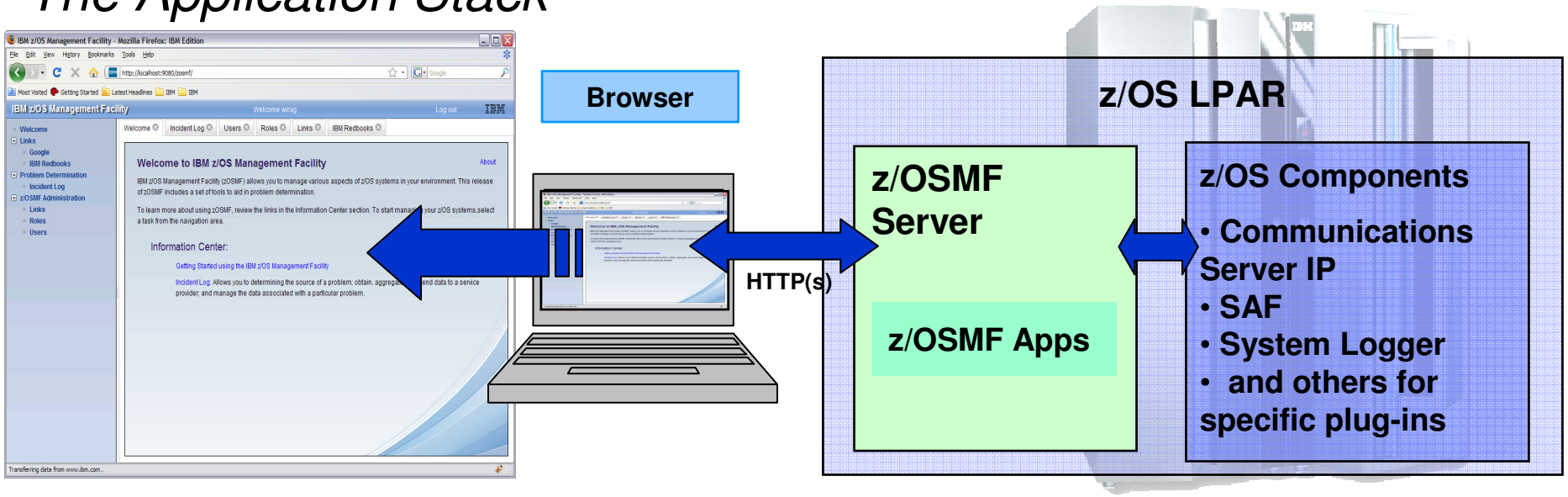
IBM z/OS Management Facility

- The IBM z/OS Management Facility is a zero priced 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.



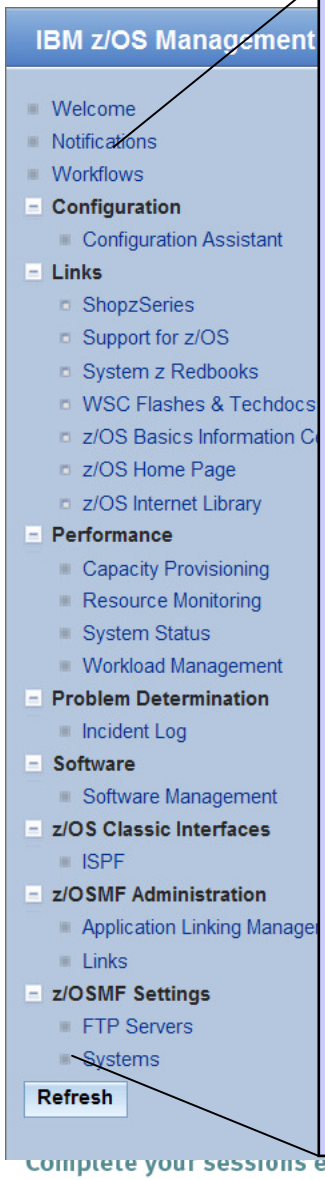
IBM z/OS Management Facility

The Application Stack



- The z/OS Management Facility application runs on the z/OS system and is presented on a PC using a browser via a secure HTTPs connection
- 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, JavaScript, Dojo, and CIM.
  - z/OSMF is a web 2.1 application and uses JAVA
  - Java and z/OS CIM Server workloads can run on available specialty engines.

IBM z/OS Management Facility



- **Notifications and Workflow *(R2.1)**
- **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** (updated)manage connections to CPMs, view reports for domain status, active configuration and active policy.
  - **Resource Monitoring, System Status** - provide integrated performance monitoring of customer's enterprise
  - **Workload Manager Policy Editor** application
  - 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 :** provide a consolidated list of SVC Dump related problems, along with details and diagnostic data captured with each incident; facilitate sending the data for further diagnostics.
- **Software** category (updated)
  - **Management:** deployment of installed software simpler and safer, manage service levels and product levels
- **z/OS classic Interface** category
  - **ISPF Task** integrate existing ISPF into z/OSMF to enable tasks from single interface and ability to launch to ISPF functions directly
- **z/OSMF Administration** category
  - z/OSMF authorization services for administrator:- dynamically add links to non-z/OSMF resources; application linking manager(R13)
- **z/OSMF Settings** category (New!)
  - Manage FTP destinations and systems

IBM z/OS Management Facility

- **The IBM z/OS Management Facility is a zero priced separately licensed product**
  - z/OS Management Facility V2.1 (5610-A01)
    - Different program number than z/OS Management Facility V1.11, 1.12 and V1.13 (5655-S28)
  - z/OS Management Facility V1.1 Subscription and Support (5655-S29)
- z/OSMF V2.1 consists of Nine (9) FMIDs:
  - HSMA210 - z/OS Management Facility core
  - HSMA211 - z/OSMF ISPF
  - HSMA212 - z/OSMF RMF
  - HSMA213 - z/OSMF WLM
  - HSMA214 – z/OSMF Software Deployment
  - HSMA215 - z/OSMF Incident Log
  - HSMA216 - z/OSMF Capacity Provisioning
  - HSMA217 – z/OSMF Workflow
  - HSMA21A - z/OSMF Configuration Assistant
- z/OSMF can be ordered via SHOPzSeries

z/OSMF Prerequisite

The IBM z/OS Management Facility product consists of :

- z/OSMF Server
- z/OSMF core infrastructure
- z/OSMF plug-ins

z/OSMF 2.1 Requires**:**

- z/OS V2.1
- **z/OSMF V2.1 requires JAVA 1.7 64 bit SR 3**
  - Java 1.7:
    - UK83228
    - UK83229
- Metal C
  - UA68210
  - UA65303
  - UA67499

z/OSMF configuration Evolution

- z/OSMF V1R11
  - z/OSMF includes WebSphere OEM and z/OSMF apps
  - Separate setup required for each, with similar steps
  - CIM server setup included, and non-optimal
  - Phase 1 fixpack included many changes – collapsed 11 distinct script invocations to 3 with the same script.
- z/OSMF V1R12
  - Separated CIM setup, only emitted CIM security setup if requested
    - Improved CIM setup instructions
  - Added new plug-ins, all plug-in setup now optional
  - Security setup enhanced, simplified
- z/OSMF V1R13
  - Added new plugins
  - Security updates – authorization modes, roles, groups
- z/OSMF V2R1* plans
  - Eliminate WebSphere OEM package and separate setup
  - Single stream configuration, 1 setup only
  - Improved performance, reduced resources

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

Planning

- There is one manual that you will use to configure z/OSMF
  - z/OSMF Configuration Guide
- The manual has a planning chapter and planning worksheets
  - You should read the planning chapter before you begin
  - You should complete the planning worksheets before you attempt to configure z/OSMF
  - Use an override file if the default value does not suffice for the system onto which z/OSMF is being configured.
- In general, you should:
  1. Configure and verify the base z/OSMF which doesn't include any plug-ins.
  2. Configure the prerequisites for the z/OSMF plug-ins you plan on using
  3. Configure and verify the z/OSMF optional plug-ins

  Note: Each step can involve creating or updating security definitions

z/OSMF Installation and Configuration Process

- Install the software (code)
  - Via ServerPac or SMP/E
- Configure z/OSMF
  - New instance or migration from prior release
- Start z/OSMF Server
  - And Login to z/OSMF
- Configure z/OS prerequisites (if necessary)
- Add optional plug-ins
- Authorize additional z/OSMF users

Software Installation

- **z/OSMF V2.1 ordered in a z/OS ServerPac**
  - Provides default customization via ServerPac provided customization jobs
    - Provided for Full System Replace installation path
    - Software Upgrade jobs and documentation provided but may need changes based on your existing environment
    - Only configures the minimal z/OSMF – no optional plug-ins
  - Can also use the z/OSMF Configuration Guide
    - Use product configuration scripts to setup, if defaults are not viable
- **z/OSMF V2.1 ordered in a CBPDO**
  - Use Program Directory to get started
  - Use the z/OSMF Configuration Guide
    - Product configuration scripts to setup

File Systems

- **z/OSMF**
  - Product file system
    - Described by Program Directory
    - Allocated via sample job CYL(150 15)
    - Can be HFS or zFS
    - Recommend use of AGGRGROW
  - Persistent data file system
    - Described in z/OSMF Configuration Guide
    - Can be pre-allocated or allocated by scripts
    - Default is a ZFS, CYL(180,20)
    - Recommend use of AGGRGROW

Configuration Process Overview

- z/OSMF has three basic phases for configuration
  1. Setup configuration files
     - Provide the input for the configuration
     - Define the configuration file
  2. Setup Security
     - Implement the security setup based on generated definitions
     - RACF definitions created
     - Security worksheets available for non RACF users
     - Verify security setup
  3. Build executables (run-time files)

- Most phases are driven through the use of z/OS UNIX configuration scripts

Configuration Process Overview

- Phase 1 scripts can be run:
  - Interactively with an override file
    - Customized values will be used in prompts, which can still be overridden
    - Recommended for first time configuration and when multiple changes required
  - FASTPATH mode (minimal prompts)
    - Requires an override file (or a configured configuration file)
    - Recommended when minimal changes needed
  - Interactively without an override file
    - Default values will be used in prompts, which can be overridden
    - Note: Potential for typographical errors if many changes required
- Note: Use an override file if the default value does not suffice for the system onto which z/OSMF is being configured.

z/OSMF Configuration Process

- **The configuration process occurs in three phases, and in the following order:**
  1. **Phase 1 – Define the Configuration**
     - izusetup.sh -file *izuconfig1*.cfg –config
  2. **Phase 2 – Setup Security**
     - **IF RACF user**
       - ***Invoke RACF REXX EXECs***
         - /etc/zosmf/*izuconfig1.cfg.rexx*
         - /etc/zosmf/*izuconfig1.cfg.<USERID>.rexx*
       - ***Verify the RACF Security Setup***
         - *izusetup.sh -file* izuconfig1*.cfg –verify racf*
     - **Non-RACF users use the exec and security worksheets to implement equivalent security setup**
  3. **Phase 3 – Build the executables – configure the z/OSMF apps**
     - *izusetup.sh -file* 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 2a: Verify the RACF security setup	izusetup.sh -file *<pathname/filename>*.cfg -verify racf	Security Administrator
Step 3: Complete the setup	izusetup.sh -file *<pathname/filename>*.cfg -finish	Superuser
Step 4: 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

Step 1: Create the initial configuration

- Use the *izusetup.sh -config* script to create the initial configuration file.
  - The script saves your input in the configuration file, which is used as input to subsequent script invocations.
    - The script can either create a new file for storing your configuration information or re-use the configuration file from a previous configuration of z/OSMF
  - 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.
    - The REXX exec will be tailored based on the set of plug-ins selected

- Sample command:
  - izusetup.sh -file izuconfig1.cfg -config -overridefile izudflt.ovr

Remember to save the name and location of config file for later use

z/OSMF Prompts and Override File

- Defaults may be taken for most input variables.
- 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)
  - z/OSMF data filesystem and data set name
  - Volume for data sets
- However, you should review ALL the prompts to determine if any additional configuration variables need to be updated.
  - If so you can either respond to the prompts, or update the override file with the changed values
- z/OSMF enables the user to tailor many different configuration settings. Not all of those options will be covered in this presentation.

Sample z/OSMF V2.1 Override File 1 of 2

```
# Licensed Materials - Property of IBM
# 5610-A01
# Copyright IBM Corp. 2013
#
# Status = HSMA210
#
# Information:
#
# SID=%I%
# Delta Date=%G%
# Delta Time=%U%
#
# The izudflt.ovr file does not contain every variable=value pair that is in the izudflt.cfg file.
# Those variables that are least likely to be modifed do not appear in this file.
# If your installation requires a change to a variable that isn't in this file, and you would prefer
# to configure it in your override file, simply add it with the modified value.
#
# Do not update or remove variable IZU_OVERRIDE_FILE_VERSION.  The information
# is required for the configuration processing.
IZU_OVERRIDE_FILE_VERSION=2.1.0
IZU_DATA_DIR=/var/zosmf/data
IZU_DATA_FS_NAME=IZU.SIZUDATA
IZU_DATA_FS_TYPE=ZFS
```

Sample z/OSMF V2.1 Override File 2 of 2

- IZU_DATA_FS_VOLUME='*'
- IZU_DATA_FS_SIZE=200
- IZU_AUTOUID_OVERRIDE=N
- IZU_AUTOGID_OVERRIDE=N
- IZU_ADMIN_GROUP_NAME=IZUADMIN
- IZU_ADMIN_GROUP_GID=9003
- IZU_USERS_GROUP_NAME=IZUUSER
- IZU_USERS_GROUP_GID=9004
- IZU_UNAUTHENTICATED_GROUP_NAME=IZUUNGRP
- IZU_UNAUTHENTICATED_GROUP_GID=9012
- IZU_HTTP_SSL_PORT=443
- IZU_APPSERVER_HOSTNAME=@HOSTNAME
- IZU_CIM_ADMIN_GROUP_NAME=CFZADMGP
- IZU_CIM_USER_GROUP_NAME=CFZUSRGP
- IZU_ZOS_SECURITY_ADMIN_GROUP_NAME=IZUSECAD
- IZU_ZOS_SECURITY_ADMIN_GROUP_GID=9006
- IZU_CA_CONFIGURE=N
- IZU_CP_CONFIGURE=N
- IZU_CP_QUERY_GROUP_NAME=CPOQUERY
- IZU_CP_CONTROL_GROUP_NAME=CPOCTRL
- IZU_DM_CONFIGURE=N
- IZU_IL_CONFIGURE=N
- IZU_IL_CEA_CONFIGURE=Y

- IZU_CEA_HLQ='CEA'
- IZU_COUNTRY_CODE=NO.DEFAULT.VALUE
- IZU_BRANCH_CODE=NO.DEFAULT.VALUE
- IZU_STORAGE_VALUE=NO.DEFAULT.VALUE
- IZU_CEAPRM_SOURCE_PARMLIB=SYS1.PARMLIB
- IZU_CEAPRM_TARGET_PARMLIB=SYS1.PARMLIB
- IZU_IEADMC_SOURCE_PARMLIB=SYS1.SAMPLIB
- IZU_IEADMC_TARGET_PARMLIB=SYS1.PARMLIB
- IZU_CEA_PARM_NAME=01
- IZU_IEA_PARM_NAME=ZM
- IZU_WISPF_CONFIGURE=N
- IZU_RMF_CONFIGURE=N
- IZU_WLM_CONFIGURE=N
- IZU_WLM_GROUP_NAME=WLMGRP
- IZU_STARTED_TASK_USERID_NAME=IZUSVR
- IZU_STARTED_TASK_USERID_UID=9010
- IZU_STARTED_TASK_HOME=/var/zosmf/data/home/izusvr
- IZU_STARTED_TASK_PROGRAM=/bin/sh
- IZU_SAF_PROFILE_PREFIX=IZUDFLT
- IZU_DEFAULT_CERTAUTH=Y
- IZU_UNAUTHENTICATED_NAME=IZUGUEST
- IZU_UNAUTHENTICATED_UID=9011

Step 2: Setup Security

- Prior to running the REXX EXEC your security administrator must define security for z/OS components (CEA, CIM, and CP) if needed for the plugins selected, 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, izuconfig1.cfg.<USERID>.cfg
Migrating from an earlier release of z/OSMF to a new z/OSMF 2.1 configuration – If already in SAF mode	Run izuconfig1.cfg.rexx (will need to edit the exec if existing security data base is used).
Just changing the authorization mode from Repository to SAF (i.e. prior to migrating to z/OSMF 2.1).	Run izuconfig1.cfg.convertFromREPtoSAF.rexx

Step 2: Run the Security Commands

- Review the RACF commands and comments prior to running the REXX EXEC, making any necessary changes as needed
  - **Recommend saving the original copy of the file first**
  - **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 | tee /var/zosmf/configuration/logs/izuconfig1_cfg_rexx.log

Captures command output in a file

Step 2a: 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 izuconfig1.cfg -verify racf
- On completion, the script creates a report called izuracfverify.report, which is stored by default in the following location:
  - /var/zosmf/configuration/logs/izuracfverify.report

Step 3: Complete the Setup

- **The izusetup.sh -finish script configures z/OSMF, using the values you supplied earlier.**
- **Specifically, the script:**
  - **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.**
  - **Configures the z/OSMF server to start the selected optional plug-ins if specified.**
- **The script also prepares your z/OS system for running the Incident Log task, if you chose to configure this task earlier.**
- **The script is intended to be run by a Superuser**

Note: you need to use the same configuration file from the initial step

- **Sample command:**
  - izusetup.sh -file izuconfig1.cfg -finish

Upon completion, the script issues an informational message (IZUG349I) that contains the URL that you use to log in to z/OSMF.

Start the z/OSMF server

- Two procedures are part of the z/OSMF package and are SMP/E installed into your SMP/E managed proclib
  - IZUANG1
  - IZUSVR1

- Starting z/OSMF:
  - S IZUANG1
  - S IZUSVR1

- Open a browser window and log into z/OSMF
  - **To find the URL to , see message IZUG349I**

IZUG349I The function ***function-name*** can be accessed at link ***link-name*** after the z/OSMF server is started on your system.

z/OSMF Next Steps

Adding z/OSMF Plug-ins

- Decide on which plug-ins (functionality) you would like to add
- Configure the respective z/OS pre-requisites
- Update the override file
  - Change the respective plug-in configuration variable to an "A"
    - Eg: IZU_CP_CONFIGURE=N to IZU_CP_CONFIGURE=A
- Invoke the setup script with the "-add" parameter
  - **izusetup.sh -file *izuconfig1*.cfg –config –add**
- Complete the security setup for this plug-in
  - ***/etc/zosmf*/izuconfig1.cfg.CP.rexx**
- Complete the z/OSMF setup
  - **izusetup.sh -file *izuconfig1*.cfg –finish –add**
- Restart the zosmf server:
  - P IZUSVR1
  - S IZUSVR1

Authorizing additional users to z/OSMF

- Use the supplied script to generate a RACF REXX exec
  - izuauthuser.sh –file izuconfig1.cfg –userid IBMUSER –role admin
    - This produces a file in the configuration directory:
      - *izuconfig1.cfg.IBMUSER.rexx*
- There are three supplied default roles
    - z/OSMF Administrator (admin)
    - z/OSMF User (user)
    - z/OS Security Admininstrator (security_admin)
- Additional roles may be created by defining groups and permitting different resource profiles.
- Either invoke the generated REXX exec or perform and equivalent security setup

z/OSMF Migration

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. There is script support for doing that.
  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.
- In z/OSMF 2.1 SAF mode authorization is required.
- If migrating from z/OSMF 1.13, you can convert to SAF mode prior to migrating or during the migration.
- If migrating from z/OSMF 1.12, the conversion to SAF mode is performed during the migration

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 properties that are no longer valid, 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:
  - 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, 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.
- Then you use the existing scripts to configure the new release of z/OSMF

z/OSMF Plug-ins
z/OS Pre-req setup

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 plug-in
  - System prerequisites for the Configuration Assistant plug-in
  - System prerequisites for the Incident Log plug-in
  - System prerequisites for the ISPF plug-in
  - System prerequisites for the Resource Monitoring and System Status plug-in
  - System prerequisites for the Software Deployment plug-in
  - System prerequisites for the Workload Management plug-in

System Prerequisites for Capacity Provisioning

- If you plan to use the Capacity Provisioning task, ensure that the capacity provisioning manager (CPM) is running and z/OSMF can connect to it.
- You need z/OSMF on one system where you administer your domain.
- CPM does not require z/OSMF on the same system.
- 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.

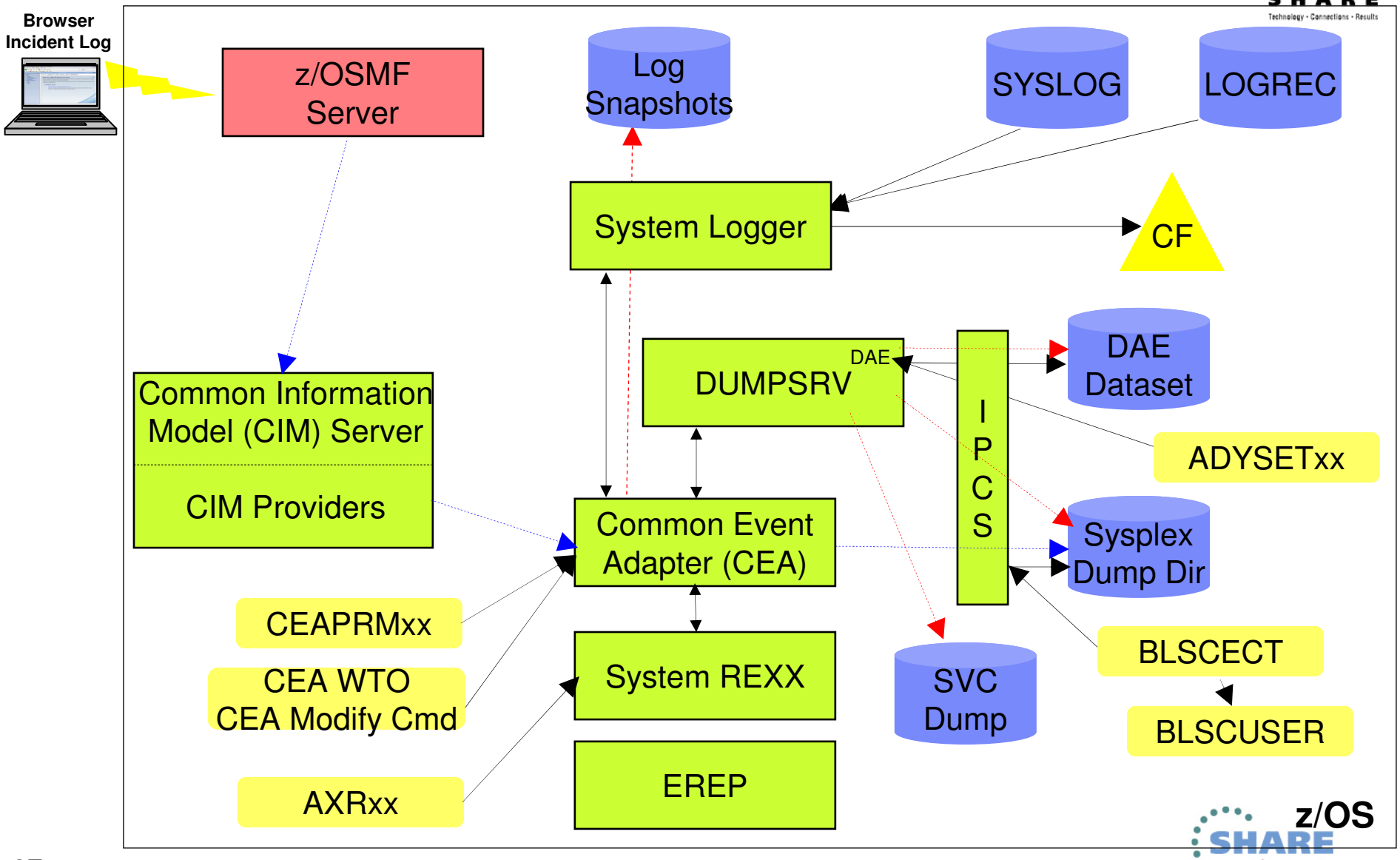
System Prerequisites for Configuration Assistant

- 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

System Prerequisites for Incident Log

- 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, the CIM server, and System REXX components are available**
  - **Incident log leverages the Problem Documentation Upload Utility, which offers encryption and parallel FTP of diagnostic data to IBM.**
  - **Note: For more information on these topics see *z/OS V1R11.0 MVS Diagnosis Tools and Service Aids* (GA22-7589)**

z/OS Infrastructure for Incident Log



System Prerequisites for the ISPF Plug-in

- **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 IBM supplied logon procedure IKJACCNT. A user can select to use a different logon procedure,
- If you plan to allow the use of multiple ISPF sessions from multiple browsers and TSO, 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.
- 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.

System Prerequisites for the 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.

- Ensure that library 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

  - 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.

The highlights….

z/OSMF V2R1 Package*

- New product package plan
  - Remove WASOEM (HBBN700)
  - Much smaller size
  - Only contain z/OSMF product file system
    - WAS Liberty Profile part of z/OSMF
- Setup and configuration overall process
  - JAVA 1.7 64 bit SR3 required (pre-req)
  - Configure z/OS prerequisites for z/OSMF Plug-ins
  - Configure z/OSMF
- Improved performance
  - Faster configuration since there is no deployment of apps nor data movement
  - Faster startup
  - Reduced memory requirement.

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

V2R1 Configuration changes*

- Simplified Configuration:
  - z/OSMF setup no longer requires two unique configurations (WebSphere OEM and z/OSMF applications)
  - z/OSMF setup collapsed, with fewer steps:
    - izusetup.sh –file izuconfig1.cfg –config
    - Security setup
    - izusetup.sh –file izuconfig1.cfg –finish
  - Support default TCPIP Port for HTTP communication
    - http port 80 and https port 443
    - Note: https port preserved on migration, http port default set to 80
- Security
  - Only support SAF authorization mode
  - Include setup of the necessary certificates and keyring for SSL
    - Create a CA by default, and server cert (self-signed)
      - Optionally can choose not to create a CA
        - Useful for multiple z/OSMFs in the enterprise
    - Support for hardware crypto built in
- Simplified service; follow the normal z/OS model;
  - Perform normal SMPE receive/apply and restart z/OSMF to pick up new service.
    - Separate step not required for activation (i.e. No izusetup.sh –file izuconfig1.cfg –service step)

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

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, 23, 25 and 27:
  - http://ibm.com/systems/z/os/zos/bkserv/hot_topics.html
- IBM z/OS Management Facility Configuration Guide (SA38-0652)
- Program Directory for z/OS Management Facility (GI11-2886)
- IBM z/OS Management Facility License Information (GC52-1263)

Summary

- IBM z/OS Management Facility (z/OSMF) V2.1 is a new release of the separate product for z/OS V2.1 customers (Program Number 5610-A01) .

- Configuration for 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)

- It is recommended that you configure the base z/OSMF application first
- Then add the different plugins as needed or when the z/OS pre-requisites for the plugins have been setup.

BACKUP

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 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

- **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*

Configure z/OS for Full Incident Log Functionality

- **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

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
  - 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[1]	•Log snapshots are NOT gathered[1] •Available with z/OSMF V1.12[3]
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 diagnc 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[3]	Dump not encrypte ken into multiple data set

IEAVTSEL – Post Dump Exit Name List Exit

1 – In z/OSMF V1.11, DASD-only logs can be used in monoplex environments, but no sysplex environments. In z/OSMF V1.12, Incident Log also support the creation of diagnostic log snapsh 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 t to send dumps as part of diagnostic data

3 – z/OSMF V1.12 function

Set up for Incident Log

- If you chose to configure the Incident Log task, the *–finish* step of the script also prepares your z/OS system for running that task.
- 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 z/OSMF core functions and 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.

Step 5: Results - izuincidentlogverify.report

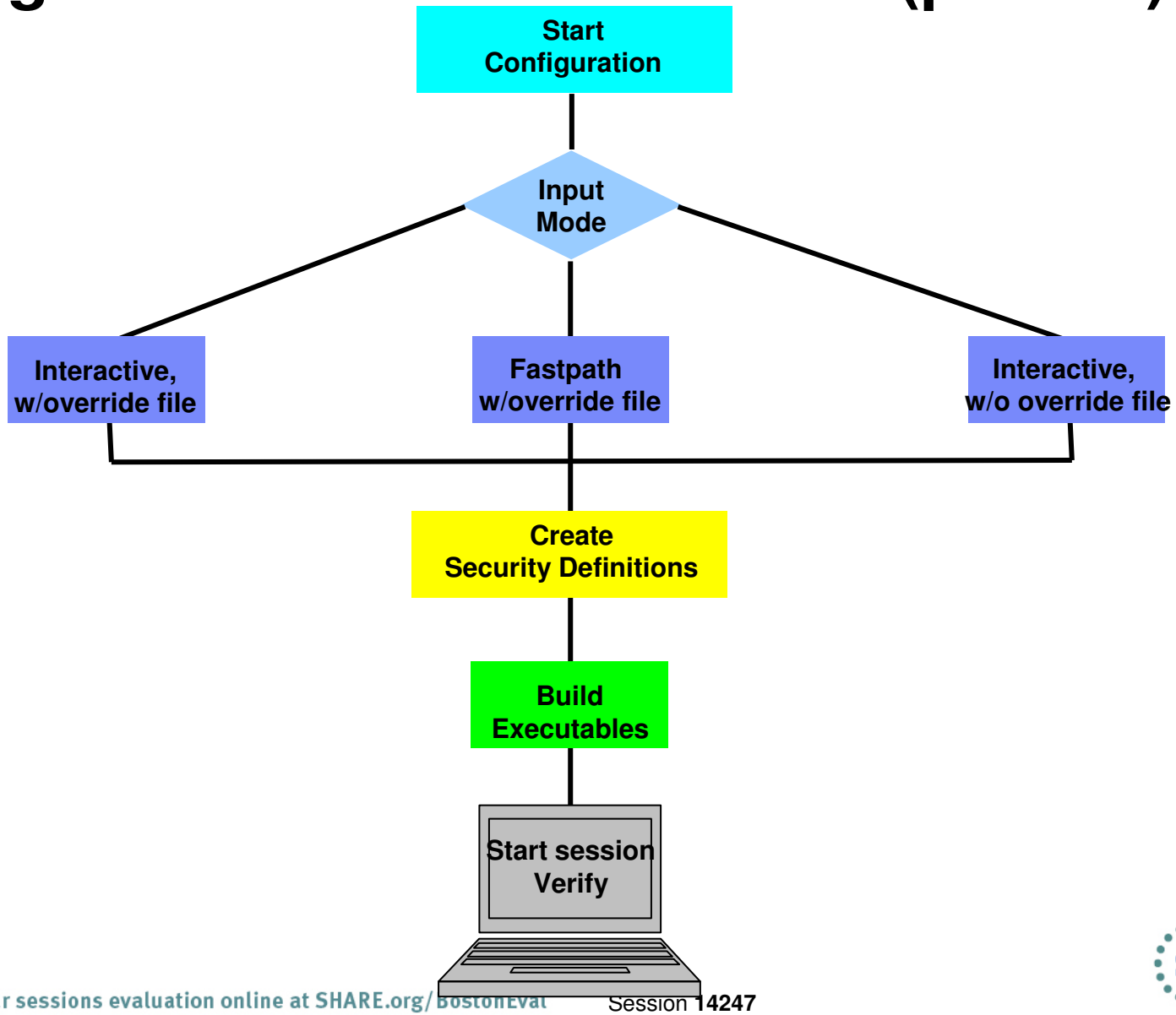
The script checks that all necessary steps were carried out, and creates a report indicating any areas that might require further action on your part. If you selected to configure the Incident Log task, the script ran an installation verification program (IVP) to verify the setup of z/OS system components. 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       : 999
Country      : 000
Storage Value : STANDARD
HLQ          : CEA                          continue →
```

```
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.MODE                G"
CEA Logrec  Logstream Model   : "CEA.MOD                 C"
                    ---------------------------------
                    Sysplex Dump Direct              ies
                    ---------------------------------
Name              : "MVSSPT.SYS                  DIR"
Size              : 112 cylinders
On Shared Volume  : TR
Free Space Available : 7
IPCS Initialized  : T
```

Need to replace with R13 version

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.
  - 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.

z/OSMF Default Directory Names and Descriptions …

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

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_STORAGE_GROUP_NAME	IZUSTGA	ZOSMF-DASD MGMT
IZU_STORAGE_GROUP_GID	9005	ZOSMF-DASD MGMT
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
ZMFAPLA	BBNBASE.ZOSMF.DASD_MANAGEMENT.**		IZUSTGA	READ	ZOSMF-DM	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