z/OS Containers Extensions
What Do I Need to Know from a Security Prespective

Session 26941

Julie Bergh
jbergh@rocketsoftware.com

Introduction

Abstract

- z/OS 2.4 announced z/OS Container Extensions (zCX). This session will talk briefly on what are the z/OS Container Extensions and how they are secured.

- Multiple sessions this week on more detailed aspects of z/OS Container Extensions.

zCX

- z/OS V2.4 introduces an exciting new capability, IBM z/OS Container Extensions, to enable the ability to run almost any Linux® on IBM Z Docker container in z/OS alongside existing z/OS applications and data without a separate provisioned Linux server. This extends the strategic software stack on z/OS as developers can build new, containerized apps, using Docker and Linux skills and patterns, and deploy them on z/OS, without requiring any z/OS skills

- zCX enables clients to deploy Linux on Z applications as Docker containers in a z/OS system to directly support workloads that have an affinity to z/OS. This is done without the need to provision a separate Linux server.

Terms

- Docker - Docker container image is a lightweight, standalone, executable package of software that includes everything needed to run an application: code, runtime, system tools, system libraries and settings.
- Container - A container is a standard unit of software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another.

- Not getting into the application and details that could use zCX

zCX

A zCX instance runs as a standard z/OS address space. Docker containers running inside a zCX instance have no way to access the memory or data contained in any other address space running in the z/OS LPAR.

zCX

- Now that you have decided to use zCX, it is time to prepare your system to support zCX and plan for your zCX instance. zCX requires IBM z14™ or later release servers with the Container Hosting Foundation (feature code 0104).

- zCX also requires z/OS V2R4 with the z/OS Management Facility (z/OSMF) configured and running on your system.

Let's Talk Security

For a zCX instance, you must consider the following issues:

- z/OSMF

- RACF user IDs and groups that you must administer and manage
- zFS data sets
- USS directories and files
- zFS files and VSAM linear data sets
- TCPIP

zCX - RACF

You provision a zCX instance in three main steps:

1. Use z/OSMF to run the zCX provisioning workflow.
2. Run the zCX instance as a started task on z/OS.
3. Access the zCX instance by using the admin user ID.

Before you start, you must plan what user IDs and groups to use for the different parts. You could use a single user ID for all steps of provisioning a zCX instance, but that is not recommended.

When you plan your RACF setup, it is always recommended that you define a user ID under which a started task runs on z/OS. That way, you can prevent this user ID from being used to log on to any z/OS application.

zCX - RACF

The suggested approach is as follows:

1. Define user IDs that can be used to execute the zCX workflows in z/OSMF.
2. Define user IDs that the zCX instance started tasks run under.
3. Define user IDs that are used to connect to admin user ID in the zCX instance.
4. Each of the preceding groups of user IDs would be in their own RACF groups.

What is z/OSMF

- IBM z/OS Management Facility (z/OSMF) provides system management functions in a task-oriented, web browser-based user interface with integrated user assistance, so that you can more easily manage the day-to-day operations and administration of your mainframe z/OS systems. By streamlining some traditional tasks and automating others, z/OSMF can help to simplify some areas of z/OS system management.
- z/OSMF allows you to communicate with the z/OS system through a web browser, so you can access and manage your z/OS system from anywhere. Multiple users can log into z/OSMF using different computers, different browsers, or multiple instances of the same browser.

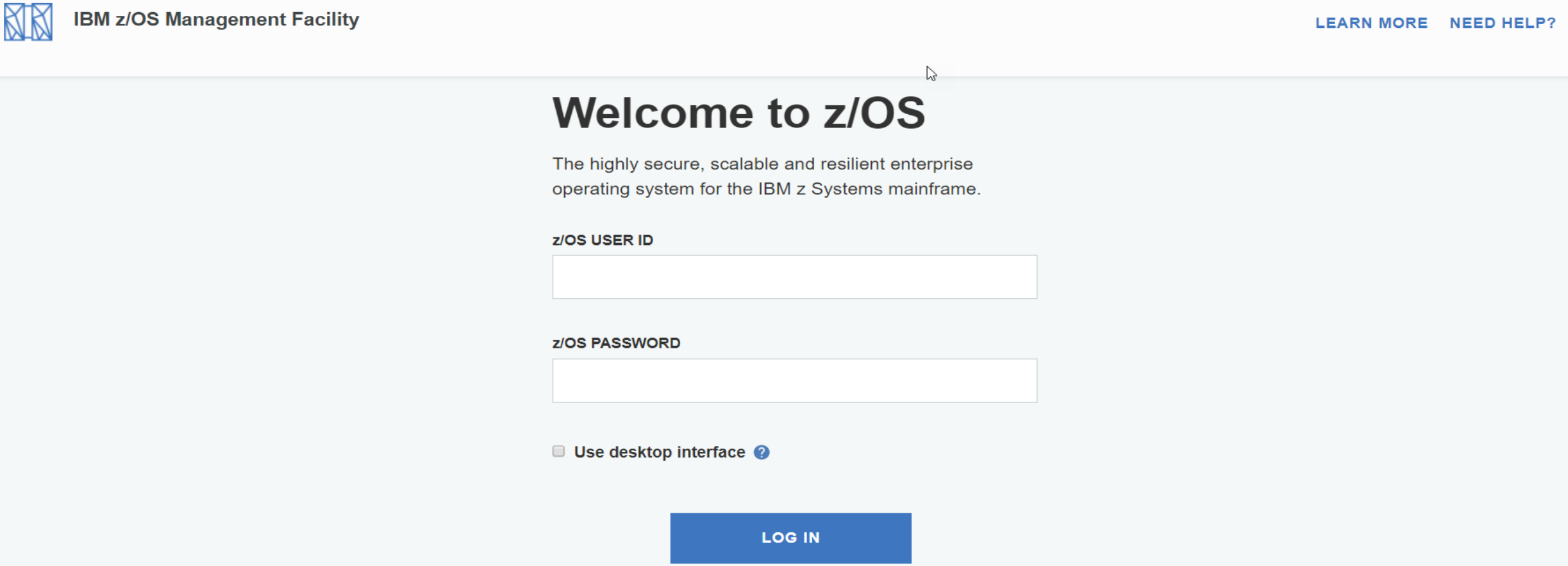
What is z/OSMF

- z/OSMF provides a framework for managing various aspects of a z/OS system through a web browser interface.
- z/OSMF provides you with a single point of control for:
  - Viewing, defining, and updating policies that affect system behavior
  - Monitoring the performance of the systems in your enterprise
  - Managing software that runs on z/OS
  - Performing problem data management tasks
  - Consolidating your z/OS management tools.

What is z/OSMF

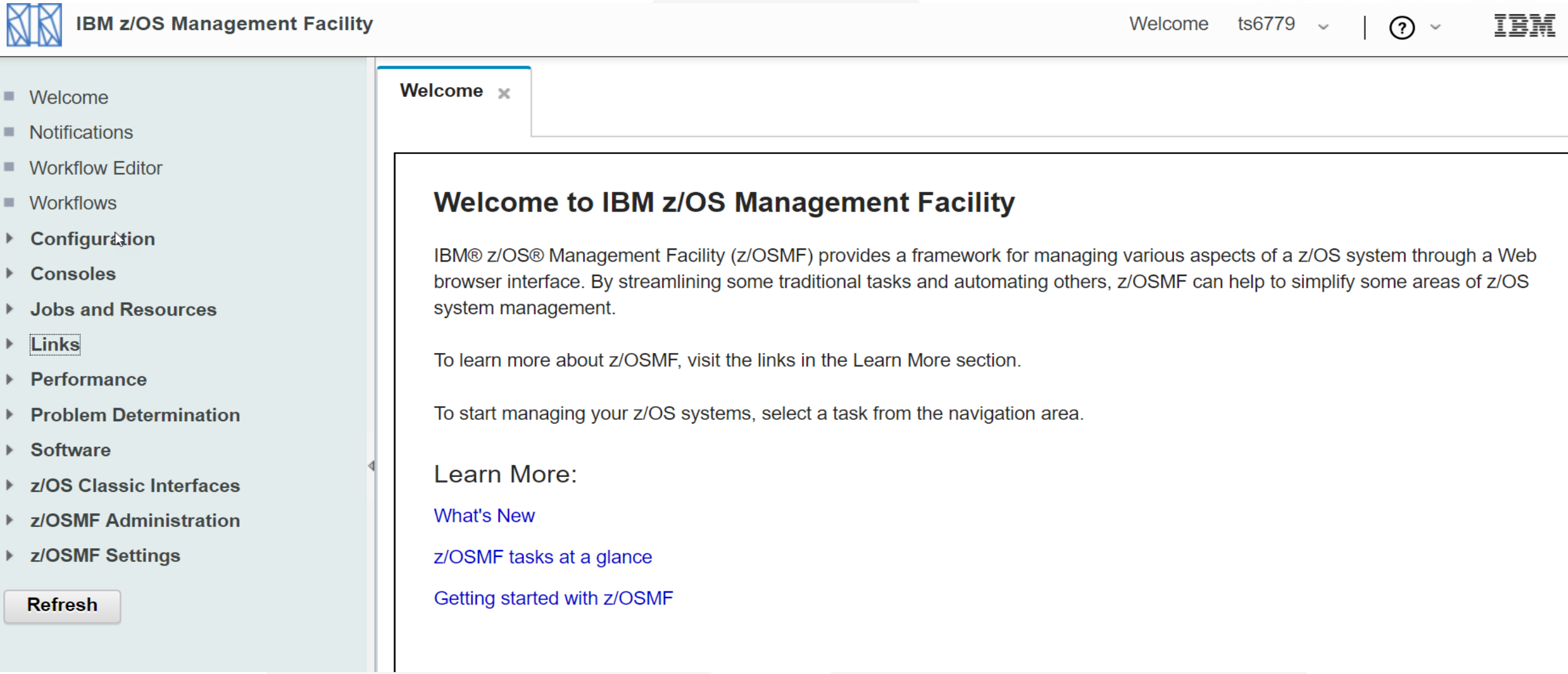
- z/OSMF includes the following software:
  - z/OSMF server.
  - WebSphere® Liberty profile, which provides an application server runtime environment for z/OSMF.
  - Set of optional, system management functions or *plug-ins*, which you can enable when you configure z/ OSMF.
  - Technologies for serving the web browser interface, such as JavaScript, Dojo, and Angular.

z/OSMF Components – Classic Interface



z/OSMF Components – Desktop User Interface

z/OSMF Components – Classic Interface



z/OSMF Components

Core Functions	Categories	Plug-ins	Menu / Sub-Menu Items (tasks)
•			Welcome
•			Notifications
•			Workflow Editor
•			Workflows
	•	•	Cloud Provisioning
			Marketplace
			Marketplace Administration
			Resource Management
			Software Services
	•		Configuration
		•	Network Configuration Assistant
	•		Consoles
			z/OS Operator Consoles
	•		Jobs & Resources
			SDSF

Core functions are those tasks which are always enabled when you initially configure the product. They are installed and can run without the need for the additional plug-ins. When the started tasks are brought up, a base configuration of z/OSMF contains only these functions. Some core functions are the Workflows task, the Resource Management task, and the Usage Statistics task.

Categories are collections of tasks and/or plug-ins with shared characteristics. An example of a category is the Performance category which contains the Capacity Provisioning, Resource Monitoring, and Workload Management plug-ins along with the System Status task.

Plug-ins are collections of one or more system management tasks that add significant functionality to z/OSMF and require additional steps to configure and deploy. Plug-ins require the creation of security profiles for the tasks that are associated with them. Examples of plug-ins are the Network Configuration Assistant, Cloud Provisioning, and the Incident Log.

z/OSMF Components

Core Functions	Categories	Plug-ins	Menu / Sub-Menu Items (tasks)
•	•		Links
		•	Shopz
		•	Support for z/OS
		•	WSC Flashes & Techdocs
		•	Z Systems
		•	z/OS Basic Information Center
		•	z/OS Home Page
		•	z/OS Internet Library
	•		Performance
		•	Capacity Provisioning
		•	Resource Monitoring
			System Status
		•	Workload Management
	•		Problem Determination
		•	Incident Log
	•		Software
		•	Software Management

z/OSMF Components

Core Functions	Categories	Plug-ins	Menu / Sub-Menu Items (tasks)
	•		Sysplex
		•	Sysplex Management
	•		z/OS Classic Interfaces
		•	ISPF
	•		z/OSMF Administration
•			Application Linking Manager
•			Import Manager
•			Links
•			Usage Statistics
	•		z/OSMF Settings
•			FTP Settings
•			General Settings
•			Notification Settings
			SDSF Settings
•			System

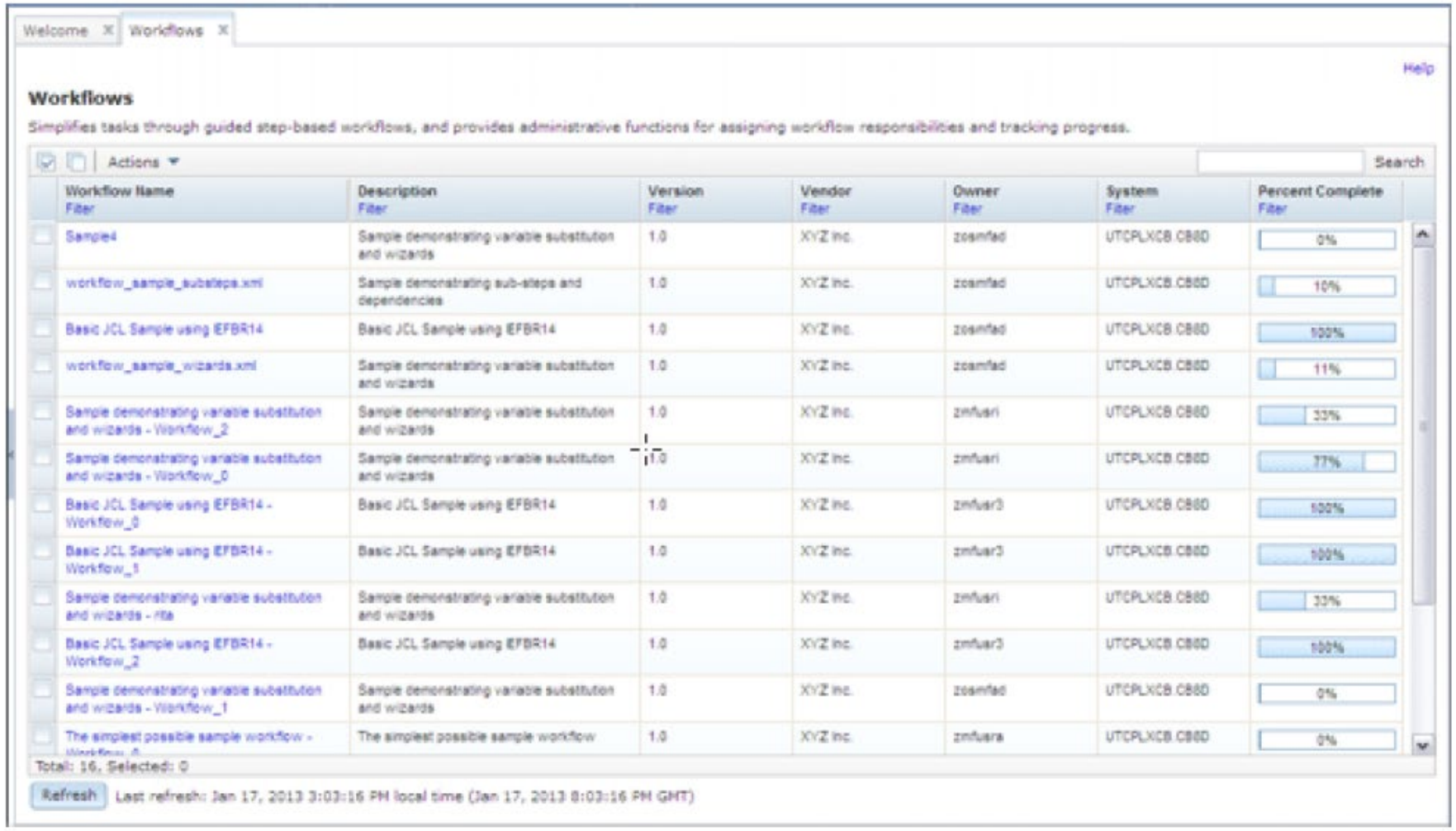
z/OSMF - Workflows

Workflows task overview

The Workflow task is installed as part of the z/OSMF core installation. No specific prerequisites must be met to use this task.

The Workflows task helps you to guide the activities of system programmers, security administrators and others at your installation who are responsible for managing the configuration of the z/OS system. The Workflows task provides a framework for these activities in the form of structured procedures known as *workflows*. The Workflows task of z/OSMF simplifies tasks through guided step-based workflows, and provides administrative functions for assigning workflow responsibilities and following progress.

z/OSMF - Workflows



z/OSMF - Workflows

SYS1.SAMPLIB (IZUSEC) to your RACF database.

RDEF ZMFAPLA IZUDFLT.ZOSMF.WORKFLOW.WORKFLOWS UACC(NONE)

RDEF ZMFAPLA IZUDFLT.ZOSMF.WORKFLOW.ADMIN UACC(NONE)

PE IZUDFLT.ZOSMF.WORKFLOW.WORKFLOWS CLASS (ZMFAPLA) ID(IZUUSER)+ ACCESS(READ)

PE IZUDFLT.ZOSMF.WORKFLOW.ADMIN CLASS(ZMFAPLA) ID(IZUADMIN) ACCESS(READ)

PE IZUDFLT.ZOSMF.WORKFLOW.WORKFLOWS CLASS(ZMFAPLA) ID(IZUSECAD) + ACCESS(READ)

SETR RACLIST(ZMFAPLA) REFRESH

For your regular workflow users, it is important to add their user IDs to RACF group IZUUSER.

z/OSMF - Workflows

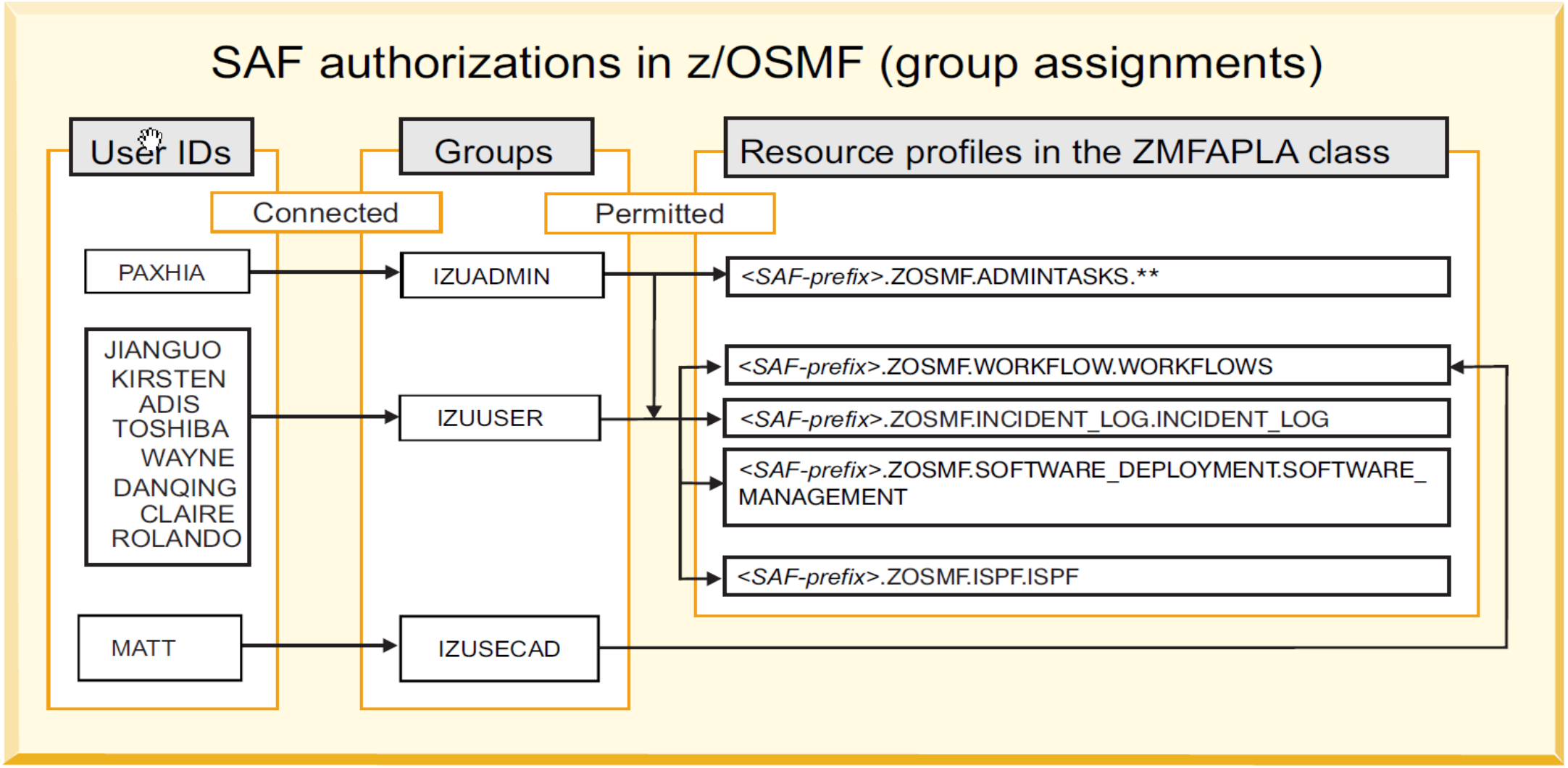
The z/OSMF Workflows task requires the following z/OSMF services to be configured:

- Common event adapter (CEA) - Usually, the CEA address space is started automatically during z/OS initialization.
- Notifications service
- z/OSMF Settings service
- z/OS jobs REST services
- z/OS data set and file REST services
- TSO/E address space services

z/OSMF Security IZUPRMxx – SYS1.PARMLIB

```
RESTAPI_FILE ACCT(IZUACCT) REGION(32768) PROC(IZUFPROC)

COMMON_TSO ACCT(IZUACCT) REGION(50000) PROC(IZUFPROC)

SAF_PREFIX('IZUDFLT')

CLOUD_SAF_PREFIX('IYU')

SEC_GROUPS USER(IZUUSER),ADMIN(IZUADMIN),SECADMIN(IZUSECAD)

SERVER_PROC('IZUSVR1')

ANGEL_PROC('IZUANG1')

AUTOSTART_GROUP('IZUDFLT')

UNAUTH_USER(IZUGUEST)

CLOUD_SEC_ADMIN(xxxxxx)
```

z/OSMF – From a Security Perspective



z/OSMF - Workflows

The z/OSMF Workflows task requires the following z/OSMF services to be configured:

- Common event adapter (CEA) - Usually, the CEA address space is started automatically during z/OS initialization.
- Notifications service
- z/OSMF Settings service
- z/OS jobs REST services
- z/OS data set and file REST services
- TSO/E address space services

z/OSMF – From a Security Perspective

MENU ITEM	MENU - SUB-ITEM (TASK)	CORE FUNCTION	PLUG-IN	RACF Profiles – For the most part ZMFAPLA class
Welcome		YES		
Notifications		YES		Saf-prefix.ZOSMF.NOTIFICATION Saf-prefix.ZOSMF.NOTIFICATION.MODIFY Saf-prefix.ZOSMF.NOTIFICATION.SETTINGS Saf-prefix.ZOSMF.NOTIFICATION.SETTINGS.ADMIN
Workflow Editor		YES		Saf-prefix.ZOSMF.WORKFLOW Saf-prefix.ZOSMF.WORKFLOW.ADMIN Saf-prefix.ZOSMF.WORKFLOW.EDITOR
Workflows		YES		Saf-prefix.ZOSMF.WORKFLOW.WORKFLOWS
Cloud Provisioning			YES	Saf-prefix.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT Saf-prefix.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT Saf-prefix.ZOSMF.PROVISIONING.RESOURCE_POOL.WLM Saf-prefix.ZOSMF.PROVISIONING.RESOURCE_POOL.NETWORK Saf-prefix.ZOSMF.TEMPLATE.APPROVERS Saf-prefix.ZOSMF.SECURITY.ADMIN
	Marketplace			
	Marketplace Administration			
	Resource Management			Saf-prefix.ZOSMF.PROVISIONING.RESOURCE_MANAGEMENT
	Software Services			Saf-prefix.ZOSMF.PROVISIONING.SOFTWARE_SERVICES

z/OSMF – From a Security Perspective

MENU ITEM	MENU - SUB-ITEM (TASK)	CORE FUNCTION	PLUG-IN	RACF Profiles – For the most part ZMFAPLA class
Configuration				Saf-prefix.ZOSMF.CONFIGURATION_ASSISTANT
	Network Configuration Assistant		YES – plug-in name COMMSERVER_CFG	Saf-prefix.ZOSMF.CONFIGURATION_ASSISTANT.CONFIGURATION_ASSISTANT
Consoles				
	z/OS Operator Consoles			Saf-prefix.ZOSMF.CONSOLES.ZOSOPER
Jobs and Resources				
	SDSF			See SDSF section in administration tasks for details
Links		YES		Saf-prefix.ZOSMF.ADMINTASKS.LINK.linkname
	Shopz			Saf-prefix.ZOSMF.LINK.SHOPZSERIES
	Support for z/OS			Saf-prefix.ZOSMF.LINK.SUPPORT_FOR_Z_OS
	WSC Flashes & Techdocs			Saf-prefix.ZOSMF.LINK.WAS_FLASHES_TECHDOCS
	z Systems			Saf-prefix.ZOSMF.LINK.SYSTEM_Z_REDBOOKS
	z/OS Basics Information Center			Saf-prefix.ZOSMF.LINK.Z_OS_BASICS_INFORMATION_CENTER
	z/OS Home Page			Saf-prefix.ZOSMF.LINK.Z_OS_HOME_PAGE
	z/OS Internet Library			Saf-prefix.ZOSMF.LINK.Z_OS_INTERNET_LIBRARY

z/OSMF – From a Security Perspective

MENU ITEM	MENU - SUB-ITEM (TASK)	CORE FUNCTION	PLUG-IN	RACF Profiles – For the most part ZMFAPLA class
Performance				
	Capacity Provisioning		YES - plug-in name CAPACITY_PROV	Saf-prefix.ZOSMF.CAPACITY_PROVISIONING Saf-prefix.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT Saf-prefix.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT.DOMAIN Saf-prefix.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.EDIT.POLICY Saf-prefix.ZOSMF.CAPACITY_PROVISIONING.CAPACITY_PROVISIONING.VIEW
	Resource Monitoring		YES – plug-in name RESOURCE_MON	Saf-prefix.ZOSMF.RESOURCE_MONITORING Saf-prefix.ZOSMF.RESOURCE_MONITORING.OVERVIEW Saf-prefix.ZOSMF.RESOURCE_MONITORING.PERFDESKS
	System Status			
	Workload Management		YES – plug-in name WORKLOAD_MGMT	Saf-prefix.ZOSMF.WORKLOAD_MANAGEMENT Saf-prefix.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.ENWRP Saf-prefix.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.INSTALL Saf-prefix.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.MODIFY Saf-prefix.ZOSMF.WORKLOAD_MANAGEMENT.WORKLOAD_MANAGEMENT.VIEW

z/OSMF – From a Security Perspective

MENU ITEM	MENU - SUB-ITEM (TASK)	CORE FUNCTION	PLUG-IN	RACF Profiles – For the most part ZMFAPLA class
Problem Determination				
	Incident Log		YES – plug-in name INCIDENT_LOG	Saf-prefix.ZOSMF.INCIDENT_LOG Saf-prefix.ZOSMF.INCIDENT_LOG.INCIDENT_LOG
Software				Saf-prefix.ZOSMF.SOFTWARE_DEPLOYMENT
	Software Management		YES – plug-in name SOFTWARE_MGMT	Saf-prefix.ZOSMF.SOFTWARE_DEPLOYMENT DATA Saf-prefix.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MAMANGEMENT Saf-prefix.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.CATEGORIES.MODIFY Saf-prefix.ZOSMF.SOFTWARE_DEPLOYMENT.SOFTWARE_MANAGEMENT.CATEGORIES.PRODUCT_INFO_FILERETRIEVE
Sysplex				Saf-prefix.ZOSMF.SYSPLEX Saf-prefix.ZOSMF.SYSPLEX.LOG Saf-prefix.ZOSMF.SYSPLEX.MODIFY
	Sysplex Management		YES – plug-in name SYSPLEX_MGMT	
z/OS Classic Interfaces				
	ISPF		YES – plug-in name ISPF	Saf-prefix.ZOSMF.ISPF.ISPF A valid account number that is defined in ACCTNUM class A valid TSOPROC defined to your system. z/OSMF provide a default of IZUFPROC.

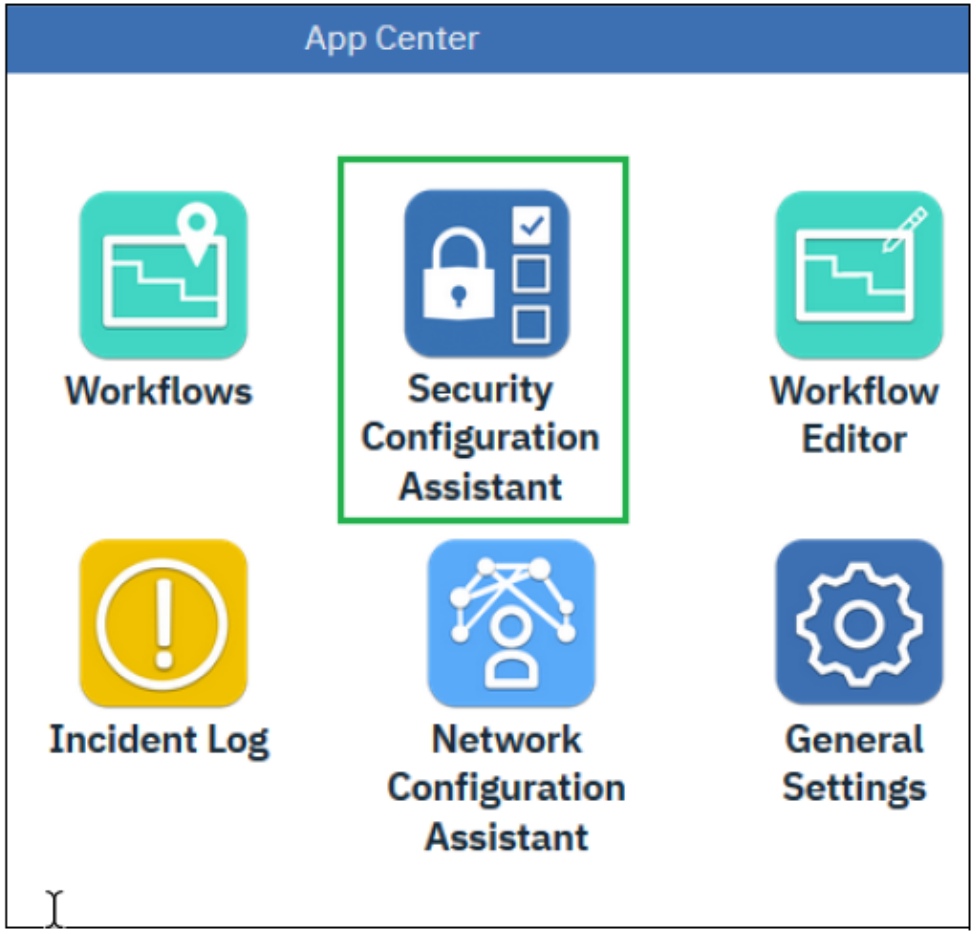
z/OSMF – From a Security Perspective

MENU ITEM	MENU - SUB-ITEM (TASK)	CORE FUNCTION	PLUG-IN	RACF Profiles – For the most part ZMFAPLA class
z/OSMF Administration				Saf-prefix.ZOSMF.ADMINTASKS Saf-prefix.ZOSMF.ADMINTASKS.LOGGER Saf-prefix.ZOSMF.ADMINTASKS.UI_LOG_MANAGMENT
	Application Linking Manager	YES		Saf-prefix.ZOSMF.ADMINTASKS.APPLINKING
	Import Manager	YES		Saf-prefix.ZOSMF.ADMINTASKS.IMPORTMANAGER
	Links	YES		Saf-prefix.ZOSMF.ADMINTASKS.LINKSTASK
	Usage Statistics	YES		Saf-prefix.ZOSMF.ADMINTASKS.USAGESTATISTICS
z/OSMF Settings				Saf-prefix.ZOSMF Saf-prefix.ZOSMF.SETTINGS
	FTP Servers	YES		Saf-prefix.ZOSMF.SETTINGS.FTP_SERVERS Saf-prefix.ZOSMF.SETTINGS.FTP_SERVERS.MODIFY Saf-prefix.ZOSMF.SETTINGS.FTP_SERVERS.VIEW
	General Settings	YES		Saf-prefix.ZOSMF.SETTINGS.SYSTEMS Saf-prefix.ZOSMF.SETTINGS.SYSTEMS.MODIFY Saf-prefix.ZOSMF.SETTINGS.SYSTEMS.VIEW
	Notification Settings	YES		

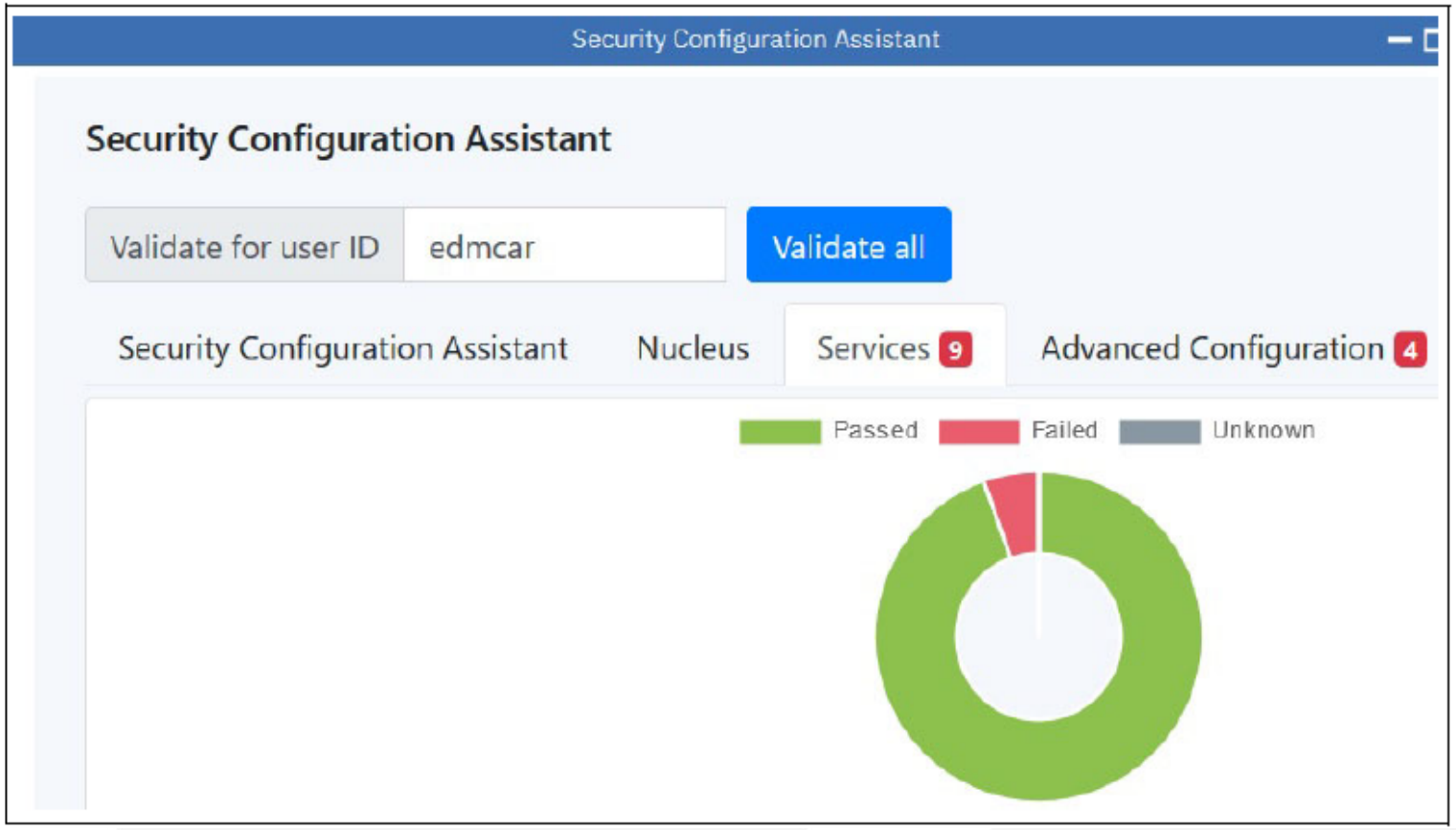
RACF Classes Used in Various Definitions

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

z/OSMF Security Configuration Assistant



z/OSMF Security Configuration Assistant

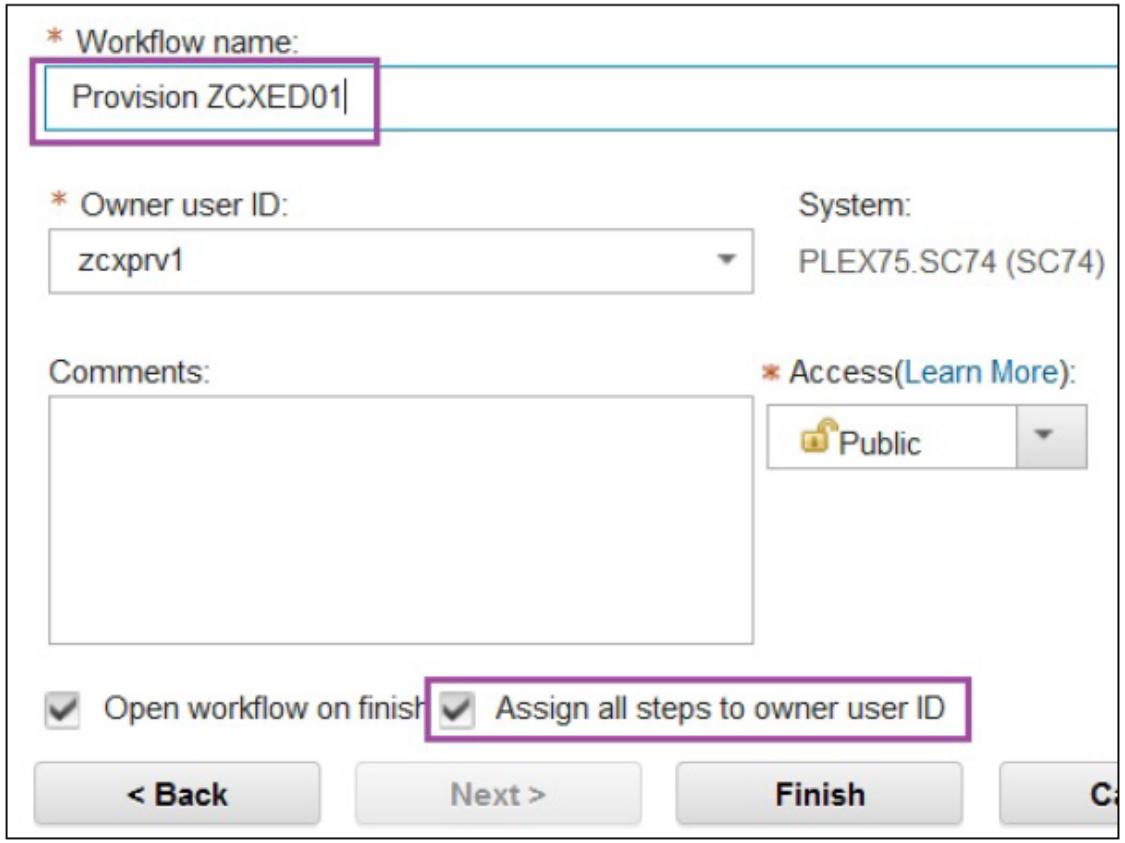


zCX - Workflow

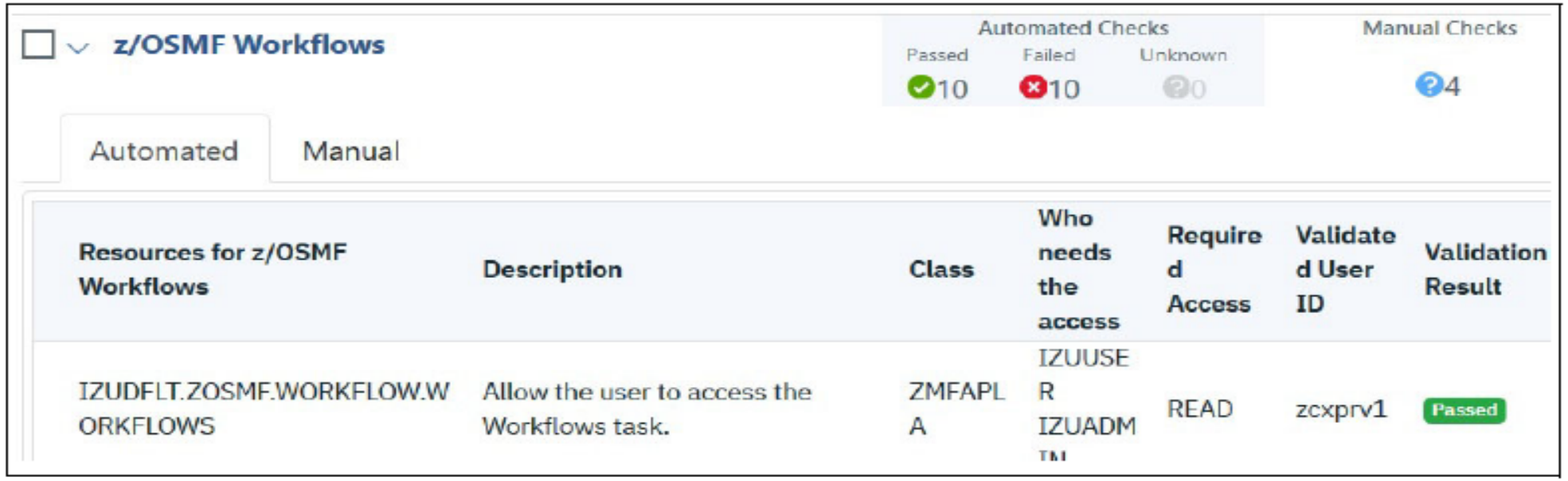
You provision zCX instances by running workflows in z/OSMF. During the running of the workflow, a single zFS file and five VSAM linear data sets are created.

You must ensure that the user ID that you use in z/OSMF has the appropriate security to create this zFS file and VSAM linear data sets. Also, you must associate RACF data set rules with these data sets to protect them.

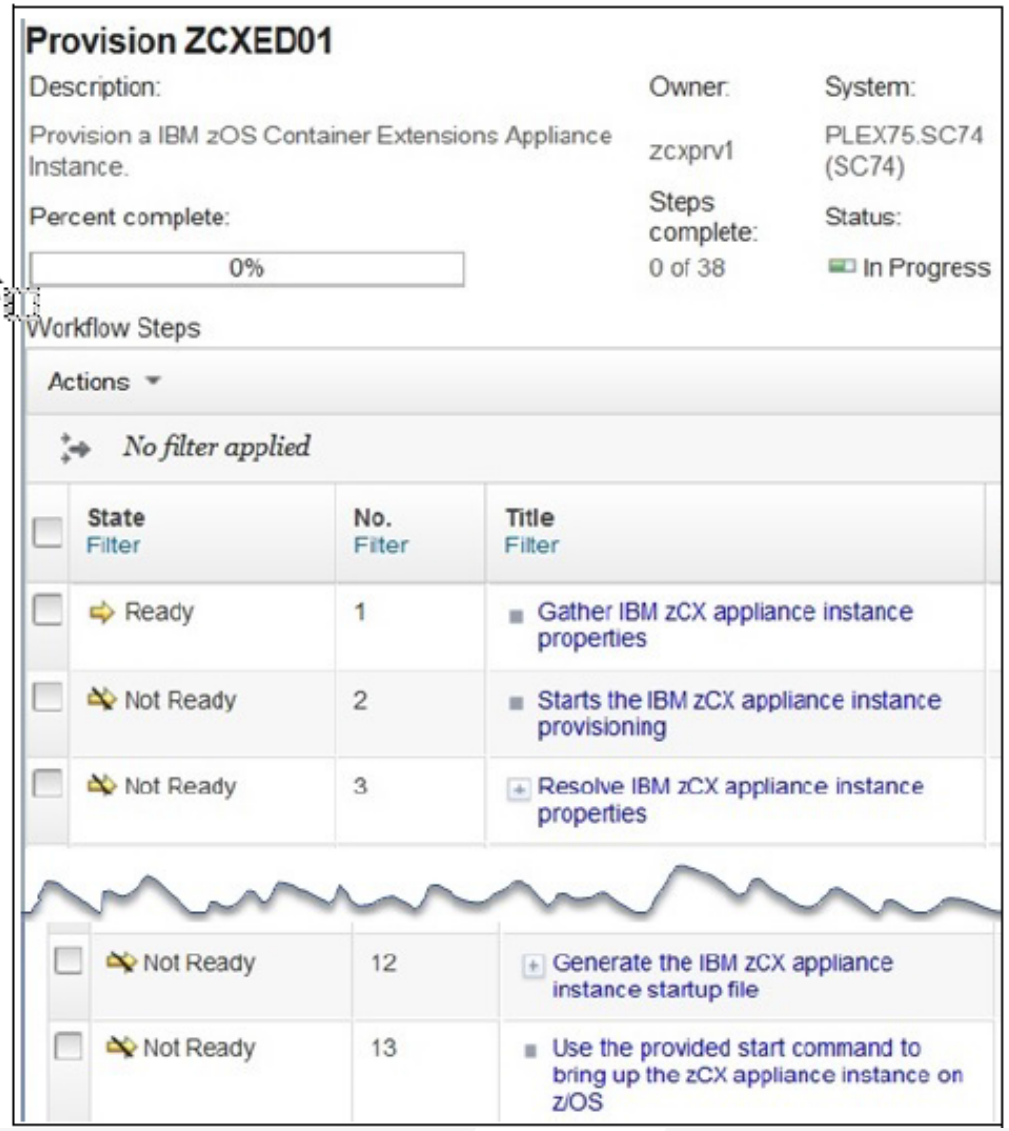
z/OSMF Security Configuration Assistant



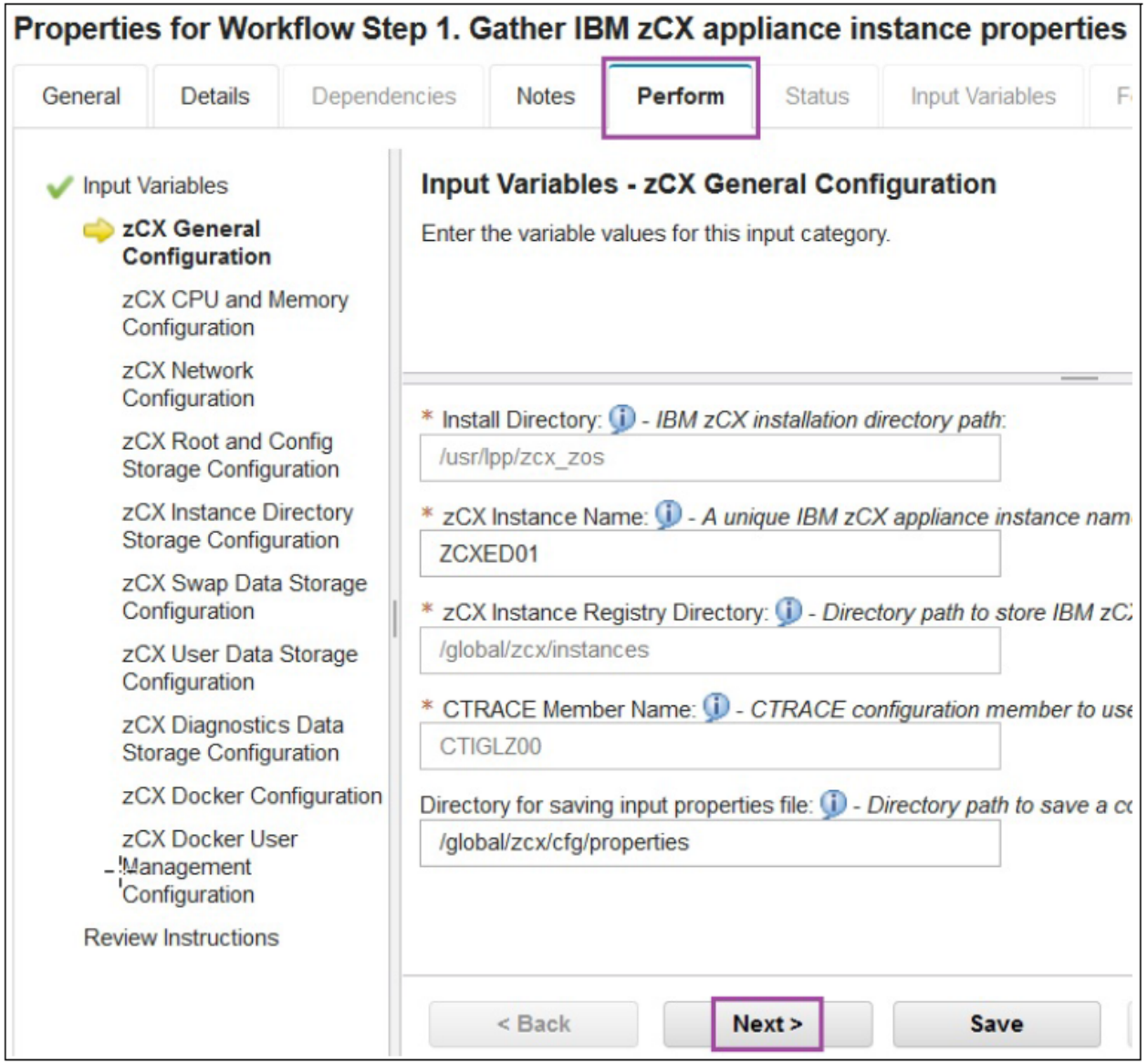
z/OSMF Security Configuration Assistant



zCX - Workflow



zCX - Workflow



zCX

zCX instances run as standard started tasks on z/OS - normal rules that apply to a started task on z/OS apply to zCX that runs as a started task.

z/OS uses mechanisms to ensure that no process running in an address space can access any other part of z/OS outside that address space unless authorized to do so.

This means that even if a process running in a Docker container in a zCX started task was running as a UNIX root user ID, that would not allow it to circumvent z/OS security controls to somehow access something else in the z/OS LPAR outside the zCX instance address space.

Access into and out of the zCX started task is done via TCPIP.

There is no capability for an application in a Docker container in a zCX started task to run a program to somehow access memory outside the started task address space.

zCX - RACF

Started Task – Recommended each instance of have own unique started task userid. Make the userid RACF 'PROTECTED'

Groups –

- zCX started tasks
- Users that would be doing the z/OSMF to run workfows
- Users that would be managing the zCX instances.

Additionally user IDs are used inside zCX instances to administer Docker containers. There are two options that can be used for these user IDs:

1. During the zCX provisioning process, specify an initial administration user ID that will be defined in the zCX instance. You can then log on to the zCX instance with this user ID and define additional user IDs, if they are required. **OR**

2. Define the zCX instance to use an LDAP server as an external user repository, and log on to the zCX instance with an LDAP user ID.

zCX - Workflow

When you run the zCX workflows in z/OSMF, a new home directory is created for the zCX instance. This directory is created either in a default directory or in a directory that you specify. This choice of directory has the following implications:

Before you run the zCX workflow, you must plan what USS directory to use. This directory serves as the parent directory in which the zCX instance directory is created.

You must consider what RACF user ID and group to define as the owner and group for these directories.

Keep these factors in mind regarding user IDs:

- The user ID the runs workflows in z/OSMF must be able to create a new directory.
- The user ID that runs the zCX started task must be able to read files from this directory and write files to a sub-directory called FFDC.

zCX - RACF

You provision a zCX instance in three main steps:

1. Use z/OSMF to run the zCX provisioning workflow.
2. Run the zCX instance as a started task on z/OS.
3. Access the zCX instance by using the admin user ID.

Before you start, you must plan what user IDs and groups to use for the different parts. You could use a single user ID for all steps of provisioning a zCX instance, but that is not recommended.

When you plan your RACF setup, it is always recommended that you define a user ID under which a started task runs on z/OS. That way, you can prevent this user ID from being used to log on to any z/OS application.

zCX - RACF

The suggested approach is as follows:

1. Define user IDs that can be used to execute the zCX workflows in z/OSMF.
2. Define user IDs that the zCX instance started tasks run under.
3. Define user IDs that are used to connect to admin user ID in the zCX instance.
4. Each of the preceding groups of user IDs would be in their own RACF groups.

zCX - RACF

The zCX Admin user ID

One concept to grasp in relation to zCX instances, is that of the zCX admin user ID.

When you provision a zCX instance, one of the properties that you specify is the admin user ID in the zCX instance. This admin user ID is defined in the zCX instance during the provisioning process and resides in the user repository of the zCX instance.

There is no connection between this admin user ID that is defined in the zCX instance and RACF.

Summary

z/OS V2.4 introduces an exciting new capability, IBM z/OS Container Extensions, to enable the ability to run almost any Linux® on IBM Z Docker container in z/OS alongside existing z/OS applications and data without a separate provisioned Linux server. This extends the strategic software stack on z/OS as developers can build new, containerized apps, using Docker and Linux skills and patterns, and deploy them on z/OS, without requiring any z/OS skills

zCX enables clients to deploy Linux on Z applications as Docker containers in a z/OS system to directly support workloads that have an affinity to z/OS. This is done without the need to provision a separate Linux server.

Summary

z/OS 2.4 announced z/OS Container Extensions (zCX). This session will talk briefly on what are the z/OS Container Extensions and how they are secured.

Due your due diligence and set up security appropriately for zCX

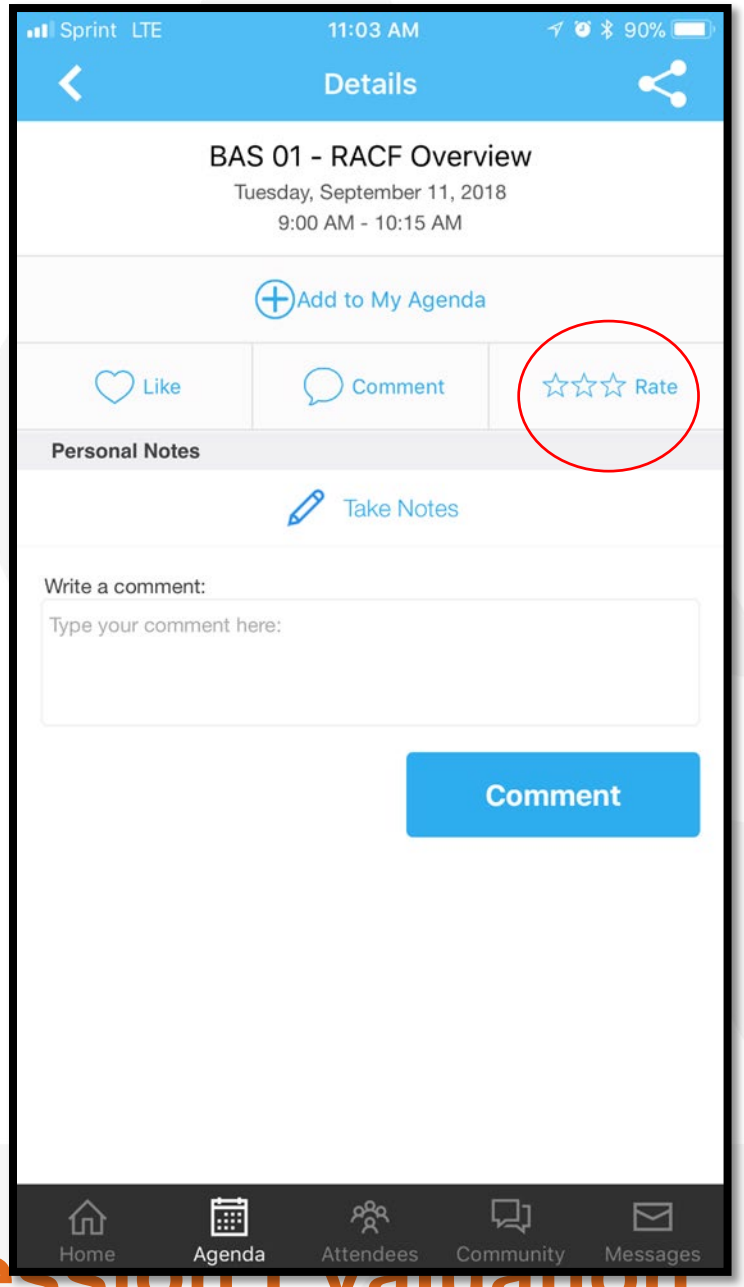
Contact Information

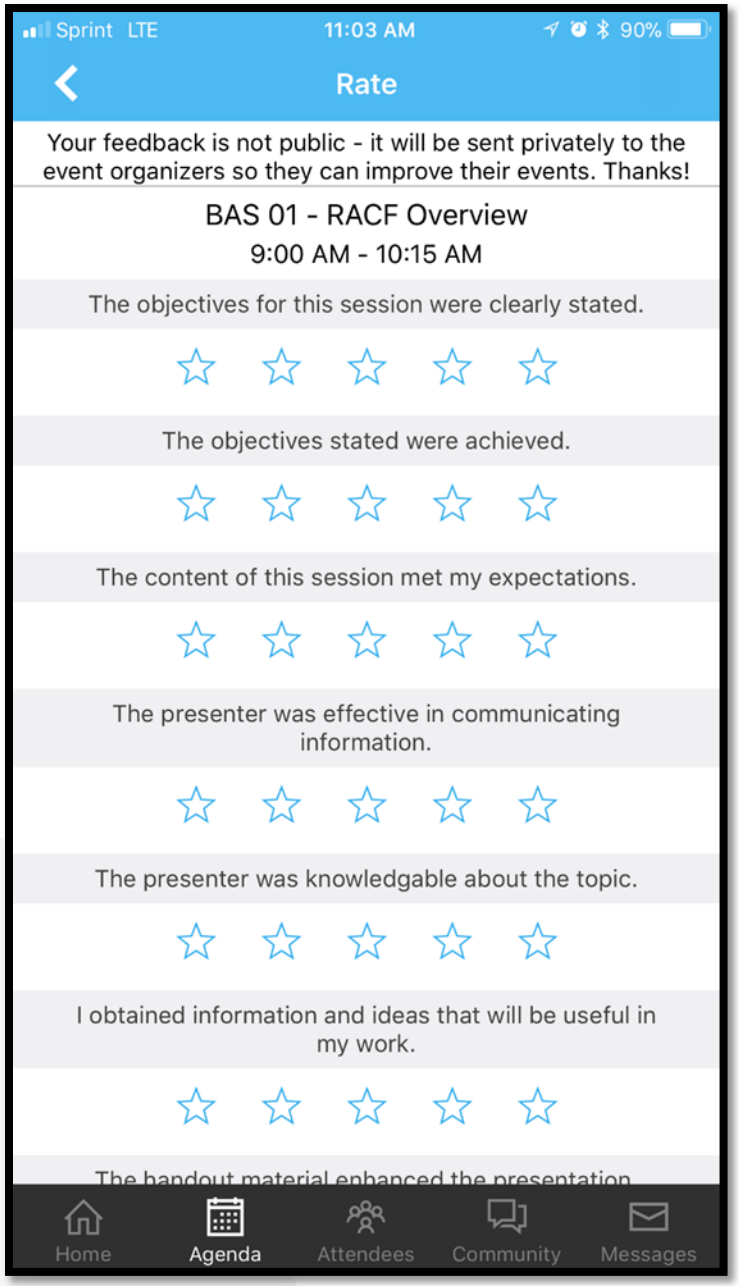
Insert contact information here.

Questions

Be sure to rate your experience using the VSC2019 app.

Your opinion helps us bring you the best experience.
Please let us know your thoughts.





Session Evaluation

Your feedback is important!

SHARE
EDUCATE ▸ NETWORK ▸ INFLUENCE

Submit a session evaluation for each session you attend:

SHARE mobile app -or- www.share.org/evaluation