CA Mainframe Security User Community Quarterly Webcast – CA ACF2 Edition

December 5, 2013

Agenda

- Save the date for CA World 2014
- CA Flips for Flipboard
- CA ACF2™ for z/OS preparation for OMVS default user removal
- DLP Poll
- Q&A

Save the date !

CA World 2014

November 9-12, 2014 ~ Las Vegas, NV

CA Technologies Information Services Flipboard

Security bookshelves internet searchable

- All CA Technologies mainframe security product bookshelves are now searchable using search engines such as Google.com
- Provides instant access to CA Product Content
- Does not require logon to support.ca.com
- **Wouldn’t it be nice to have your own content on your iOS or Android device?**

ca technologies

Bookshelf

Enter search term Search

CA ACF2 r15 for z/OS

Welcome to the CA ACF2 r15 for z/OS bookshelf. Browse the categories on this bookshelf for the information you need.

Download this Bookshelf

Release Information

Release Notes	View HTML	Download PDF

Product Documentation

▼Show All

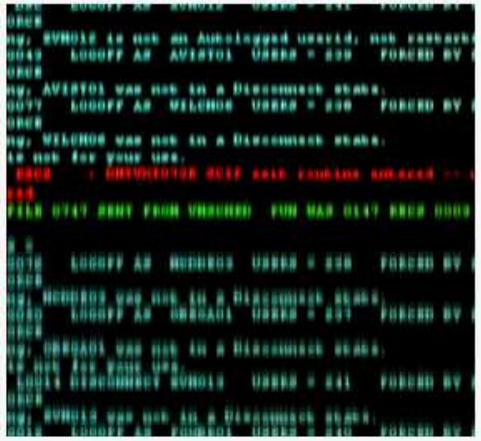
Administration Guide	View HTML	Download PDF
Auditor Guide	View HTML	Download PDF
Best Practices Guide	View HTML	Download PDF
CICS Support Guide	Restricted Deliverable	Download PDF
Compliance Information Analysis Guide	View HTML	Download PDF
Cookbook	View HTML	Download PDF
Data Model Guide	Restricted Deliverable	Download PDF
Distributed Database Support Guide	Restricted Deliverable	Download PDF
Implementation Guide	View HTML	Download PDF
IMS Batch Support Guide	View HTML	Download PDF
IMS Support Guide	View HTML	Download PDF

CA flips for Flipboard

- Flipboard enables you to review product information in a magazine style format
- CA Technologies is delivering technical content, such as tips and tricks, for many of our products
- Launched **CA System z Security Cookbook** 11/20 - includes 10 articles

IBM z/OS 2.1 Support for CA ACF2 I CA System z Security Cookbook

Compare Security Records I CA System z Security Cookbook



How to Debug in CA Compliance Manager I CA System z Security Cookbook

CA Technologies Information Services

Welcome to our cookbooks. We hope you will find them interesting and useful aids to help grow your knowledge of your CA Technologies software.

503 Articles | 2,498 Readers | 20 Magazines

Magazines by CA Technologies Information Services

How to get started

- Install the Flipboard app located in the app store on your tablet or mobile device.
- Once installed, open Flipboard and type “CA Technologies Information Services” in the search box. You will see a list of our magazines, including the CA System z Security Cookbook.
- Tap on the magazine cover and be sure to tap “Subscribe.”

Don’t have a smartphone or tablet?

- You can view cookbook content from Chrome and Firefox, Internet Explorer is not supported. We recommend using Chrome for your best viewing experience. Here's how:
  - Go to the CA Technologies Information Services landing page on Flipboard: https://flipboard.com/profile/mycagroup.
  - Flipboard opens on your desktop browser with a flipping effect similar to the mobile app. So, you don't need a mobile device!
  - The direct link to the CA System z Security Cookbook is https://flipboard.com/section/ca-system-z-security-cookbook-b3tgrr

Calling all Authors!

If you are interested in discovering your inner author and would like to write an article for a cookbook, email Laura Fletcher at Laura.Fletcher@ca.com

Q & A

CA ACF2™ for z/OS r15

Preparation for OMVS defaults removal

Dave Hrycewicz
Sr. Principal Software Engineer

Webinar series

December 5th, 2013

Agenda

- CA ACF2 r15 for z/OS 2.1 support
  - Release/Maintenance requirements
  - Related z/OS 2.1 enhancements
    - Majority applicable at z/OS 1.13 and below
- Removal of DFTUSER/DFTGROUP
  - Optional at z/OS 1.13 and below
  - Deactivated at z/OS 2.1 and above
- CA ACF2 r15 for z/OS (TEC599992)
  - Technical document available on Support Online
  - Provides extensive details related OMVS defaults removal
- Questions & Answers

CA ACF2™
Interim Enhancements – z/OS 2.1 support

- z/OS 2.1 CA ACF2 release/maintenance requirements
  - CA ACF2 r15 - Minimum required release to run z/OS 2.1.
    - Customers running CA ACF2 r14 or lower will need to upgrade to r15 across all LPARS before implementing z/OS 2.1. See Informational Solution RI61937 for a description of all requirements needed to run z/OS 2.1 with CA ACF2 r15.
    - See also RO59312 – Enhancement – z/OS 2.1 Compatibility

- Implement CA ACF2 r15 related enhancement PTF's.
  - Solutions include:
    - RO55702 – ACFRPTOM report detect users that leverage BPX.DEFAULT.USER
      - Leveraged at z/OS 1.13 and below
    - RO62727 – Introduces &LID support in HOME field of OMVS User Profile Record – allows use as a model
    - RO62039 – Add msgs for BPX.DEFAULT.USER removal
  - Use FIXCAT: CA.TargetSystem-RequiredService.z/OS.V2R1

2.1

ACF2 options OMVSUSR & OMVSGRP not supported at z/OS 2.1

Per IBM's announcement: (Feb 15th, 2011 - z/OS 1.13 preview statements of direction):

"z/OS V1.13 is planned to be the last release to support BPX.DEFAULT.USER. IBM recommends that you either use the BPX.UNIQUE.USER support that was introduced in z/OS V1.11, or assign unique UIDs to users who need them and assign GIDs for their groups."

CA ACF2 r15 GSO control UNIXOPTS record options UNIQUSER & MODLUSER can be leveraged to activate the equivalent support. Usage of both UNIQUSER and MODLUSER are detailed in the CA ACF2 Administration Guide and technical document TEC599992.

Why did IBM make this change?

Shared user ID's are never a good thing especially whenever the Auditor shows up. This is especially evident in native UNIX security when the UID (by default) is the owner of all files and directories created under that user id.

Reasons IBM made this change:

- Majority of sites still leverage defaults across the majority of their LPARs.
- RACF does not currently support externalized USS security (at the file and directory level) i.e. CA Top Secret & CA ACF2 HFSSEC security.
- Loss of Accountability
  - Difficult to enforce standards.
- Makes Data Loss Prevention difficult/impossible to enforce.
- Native Unix commands such as CHOWN can result in inadvertent circumvention of security.

CA ACF2 Tech doc: TEC599992

Preparation for removal of Default DFTUSER and DFTGROUP

Provides implementation considerations related to eliminating DFTUSER & DFTGROUP usage

- Available on CA Support Online website (TEC599992)
- Applicable at both z/OS 1.13 & z/OS 2.1
  - z/OS 1.13 and below – Remove control options DFTUSER & DFTGROUP from ACF2 UNIXOPTS GSO record.
  - z/OS 2.1 – Mandatory preparation steps.

Tech doc: TEC595035

Preparation for removal of Default DFTUSER and DFTGROUP

Identifying Logonids that leverage the defaults (z/OS 1.13 and below)

- RO55702 - DETECT USERS OF BPX.DEFAULT.USER
  - Adds the ability to turn on a BPX.DEFAULT.USER "trace"
  - To activate this support, you will need to define a FACILITY CLASS resource rule to generate the default user trace messages.
    - $KEY(TRACE.BPX.DEFAULT.USER) TYPE(FAC)
    - $USERDATA(TRACE)
  - ACFRPTOM will report on any successful initUSP callable service that has used the BPX.DEFAULT.USER values.

ACFRPTOM screen shot

```
CA Mainframe Security    - z/OS USS Event Log              - PAGE    1

   SERVICE     USERID    GROUP       UID       GID    SAF  RC   RSN
    DATE        TIME    JOBNAME   SOURCE    SYSID   CPU   SECLABEL

initUSP        USR941A  *           56050     83800  0    0    0   <--- LID USR941A will not have any OMVS segment data. (No uid/gid assigned)
12/03/13  13.337    8.38.45 USR941A              XE14
Successful - UID or GID came from BPX.DEFAULT.USER
 Home    : /u
 Program : /bin/sh

initUSP        USR941B  *             24      83800  0    0    0    <--- LID USR941B will have a UID but no GID assigned
12/03/13  13.337    8.40.06 USR941B              XE14
Successful - UID or GID came from BPX.DEFAULT.USER

initUSP        USR941C  OMVSGRP1    56050       777  0    0    0     <---- LID USR941C will have a GID but no UID assigned
12/03/13  13.337    8.40.42 USR941C              XE14
Successful - UID or GID came from BPX.DEFAULT.USER
 Home    : /u
 Program : /bin/sh

initUSP        USR941D  OMVSGRP1      25        777  0    0    0   <----   LID USR941D will have a UID and a GID assigned
12/03/13  13.337    9.05.34 USR941D              XE14
Successful - Logging active by Trace/Audit options
 Home    : /u
 Program : /bin/sh
```

Tech doc: TEC599992

Preparation for removal of Default DFTUSER and DFTGROUP

How Groups & Default Groups are handled under CA ACF2

- At sign-on ACF2 builds group list based on:
  - Assigned Groups on Logonid record
  - Allowed groups (supplemental) based on TYPE(TGR) resource rule permissions
- At sign-on ACF2 assigns the users connect group based on:
  - GROUP field from the signon (group must be in the groups list)
  - Supplemental groups if the GROUP field was not specified
- At USS initialization, the user's connect group is presented to USS. If none, then one may be assigned from MODLUSER.

Tech doc: TEC599992

Preparation for removal of Default DFTUSER and DFTGROUP

Steps to perform before using UNIQUSER & MODLUSER

- Implement ACF2MS r15 related enhancement PTF's.
- Identify Logonids that have pre-existing OE authorization assignments.
- Reconcile OMVS assignments across all applicable LPARs for these Logonids.
- Define the MODLUSER Logonid (or use the existing DFTUSER Logonid).
- Identify the highest UID that is currently assigned on each LPAR (If leveraging CPF).
- Determine/setup - related ACF2 control options

Tech doc: TEC599992

Preparation for removal of Default DFTUSER and DFTGROUP

Identify Logonids that have pre-existing OE authorization assignments

- ACF command example:

```
t terse
 LID
LIST IF(GROUP EQ ' ') SECTION(RESTRICTIONS) PROFILE(OMVS)
LIST IF(GROUP NE ' ') SECTION(RESTRICTIONS) PROFILE(OMVS)
SET PROFILE(GROUP) DIV(OMVS)
LIST LIKE(-)
END
```

Tech doc: TEC599992

Preparation for removal of Default DFTUSER and DFTGROUP

Identify Logonids that have pre-existing OE authorization assignments

- ACF command example:

```
t terse
 LID
l like(m-) prof(omvs)
  MACADMN                SHS   MACADMN   MAC ADMINITRATOR     X6625
  MASTER                 SHS   MASTER    XX
  OMVS / MASTER
  MASTERQ                SHS   MASTERQ
  MASTER1                SHS   MASTER1
  OMVS / MASTER1
  MASTER2                SHS   MASTER2
```

Tech doc: TEC599992

Preparation for removal of Default DFTUSER and DFTGROUP

Identify Logonids that have pre-existing OE authorization assignments

- ACF command example:

```
set terse
LID
list like(t-) if(group=c'         ')
  TESTGUY                    SHS   TESTGUY
  TUSER01                    TUSER01   TUSER
  TUSER02                    TUSER02   TUSER
  TUSER03                    TUSER03   TUSER
  TUSER04                    TUSER04   TUSER
```

Tech doc: TEC599992

Preparation for removal of Default DFTUSER and DFTGROUP

Identify Logonids that have pre-existing OE authorization assignments

- ACF command example:

```
LID

change if(group='        ') group(testgrp)

 ACF6C005 5  LOGONID(S) CHANGED
```

Tech doc: TEC599992

Preparation for removal of Default DFTUSER and DFTGROUP

Reconcile OMVS assignments across all applicable LPARs

- Verify Logonids have the same UID assigned across all LPARS
- Advantages:
  - Directory and file UNIX administration can be the same in all LPARs.
    - This may be required if you are sharing ZFS/HFS file systems.
  - UNIX trace will be able to distinguish activity for users by UID on any LPAR.
- Disadvantages:
  - Privileges not vary across file systems.

Tech doc: TEC599992

Preparation for removal of Default DFTUSER and DFTGROUP

Reconcile OMVS assignments Gotcha

- Changing a Logonid's UID in ACF2 (or TSS/RACF) does not change the owner of files/directories created under the previously assigned UID.
- Related UNIX commands:
  - FIND – Unix find command to locate files owned by USER or GROUP.
    - *find directory-location -user {username} -name {file-name}*
  - CHGRP – Unix command to change file/directory group.
    - *chgrp [options] group FSO* - (file system objects)
  - CHOWN – Unix command to change owner. It is important to realize that you can only change file ownership as a super-user (root). Any regular Unix user cannot change the ownership of any file (including files they own) unless they have the CHOWN.UNRESTRICTED resource in the UNIXPRIV resource class .
    - *chown user filelist*

Tech doc: TEC599992

Preparation for removal of Default DFTUSER and DFTGROUP

MODLUSER Logonid possible field assignments

- HOME – Leverage variable &LID
- OMVSPGM
- CPUTIME, MAXFILE, ASSIZE, PROCUSER, THREADS, MMAPAREA, MEMLIMIT, SHMEMMAX

Tech doc: TEC599992

Preparation for removal of Default DFTUSER and DFTGROUP

MODLUSER/UNIQUSER Gotcha – partial OMVS Segment

- MODLUSER/UNIQUSER support is not leveraged if the Logonid has any of the following OMVS User Profile Record assigned fields:
  - HOME
  - OMVSPGM
  - CPUTIME, MAXFILE, ASSIZE, PROCUSER, THREADS, MMAPAREA, MEMLIMIT, SHMEMMAX
- Attempted USS access will fail if Logonid is missing:
  - UID
  - GROUP (with a GID assigned)

Tech doc: TEC599992

Preparation for removal of Default DFTUSER and DFTGROUP

CPF processing

- When automatic UID or GID assignment is used – the actual assigned value is sent across to other CPF nodes

CPF Gotcha's – CPF'ing an ACF2 CHANGE of a UID

- Incoming CPF command CHANGE BAKER01 UID(1234):
  - Will replace an already assigned UID if it exists on the target node for Logonid BAKER01.
  - Command will fail if UID(1234) is already assigned on the targeted system.

Tech doc: TEC599992

Sample Usage cases (with CPF active)

Technical Document Sample Usage cases

- Two scenario based usage cases (with CPF implemented)
  - Both usage cases insure:
    - Same UID assigned across all CPF connected LPARs
      - Leverage the UIDSTART/UIDEND range keyword (within GSO AUTOIDOM record)
      - Eliminates possible UID collisions

SAMPLE usage: AUTOIDOM UIDSTART/UIDEND

SYS1 (via GSO AUTOIDOM) UIDSTART**(1000000) UIDEND(1999999) ASSIGNU**

SYS2 (via GSO AUTOIDOM) UIDSTART**(2000000) UIDEND(2999999) ASSIGNU**

SYS3 (via GSO AUTOIDOM) UIDSTART**(3000000) UIDEND(3999999) ASSIGNU**

SYS4 (via GSO AUTOIDOM) UIDSTART**(4000000) UIDEND(4999999) ASSIGNU**

SYS5 (via GSO AUTOIDOM) UIDSTART**(5000000) UIDEND(5999999) ASSIGNU**

In addition to setting the AUTOIDOM record fields UIDSTART and UIDEND, will also need to set in GSO UNIXOPTS the following control options on all 5 LPARs:

- UNIQUSER
- MODLUSER(logonid) – This can be the logonid that is assigned to the DFTUSER option within the GSO UNIXOPTS record.

Tech doc: TEC599992

Preparation for removal of Default DFTUSER and DFTGROUP

HFSSEC (externalize USS security) Impact

- HFSSEC – CA ACF2 control (within GSO UNIXOPTS) to externalize USS security
  - Although HFSSEC externalizes security for USS, OMVS credentials are still required to sign-on to USS related workloads.
    - HFSSEC(YES) – Still need to establish the minimum OE segment authorizations for any Logonids that leverage USS workloads.
    - UNIQUSER and MODLUSER should be considered for sites running HFSSEC that want users to be auto assigned (permanent) OMVS segment authorizations when none exists.
    - LPARS running with HFSSEC active, OE credential assignments do not determine file/directory access authorizations. That is still handled by the CA ACF2 product.

Tech doc: TEC599992

Preparation for removal of Default DFTUSER and DFTGROUP

MODLUSER/UNIQUSER rollout considerations

- Shared HFS/zFS file systems
  - **Gotcha Alert:** For non-shared security file configurations, reconcile all LPARS that share the same file system before implementing MODLUSER/UNIQUSER.

- Mixed CA ACF2 release configuration
  - **Gotcha Alert:** Before implementing MODLUSER/UNIQUSER, all LPARS should be running CA ACF2 r15 with all recommended PTFs.

Q&A

FOR INFORMATION PURPOSES ONLY

terms of this presentation

All trademarks, tradenames, servicemarks and logos referenced herein belong to their respective companies.

This presentation was based on current information and resource allocations as of November 2013 and is subject to change or withdrawal by CA at any time without notice. Notwithstanding anything in this presentation to the contrary, this presentation shall not serve to (i) affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services agreement relating to any CA software product; or (ii) amend any product documentation or specifications for any CA software product. The development, release and timing of any features or functionality described in this presentation remain at CA's sole discretion. Notwithstanding anything in this presentation to the contrary, upon the general availability of any future CA product release referenced in this presentation, CA will make such release available (i) for sale to new licensees of such product; and (ii) to existing licensees of such product on a when and if-available basis as part of CA maintenance and support, and in the form of a regularly scheduled major product release. Such releases may be made available to current licensees of such product who are current subscribers to CA maintenance and support on a when and if-available basis. In the event of a conflict between the terms of this paragraph and any other information contained in this presentation, the terms of this paragraph shall govern.

Certain information in this presentation may outline CA's general product direction. All information in this presentation is for your informational purposes only and may not be incorporated into any contract. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this presentation "as is" without warranty of any kind, including without limitation, any implied warranties or merchantability, fitness for a particular purpose, or non-infringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if CA is expressly advised in advance of the possibility of such damages. CA confidential and proprietary. No unauthorized copying or distribution permitted.