CA Mainframe Security User Community Quarterly Webcast – CA Top Secret Edition

December 5, 2013

Agenda

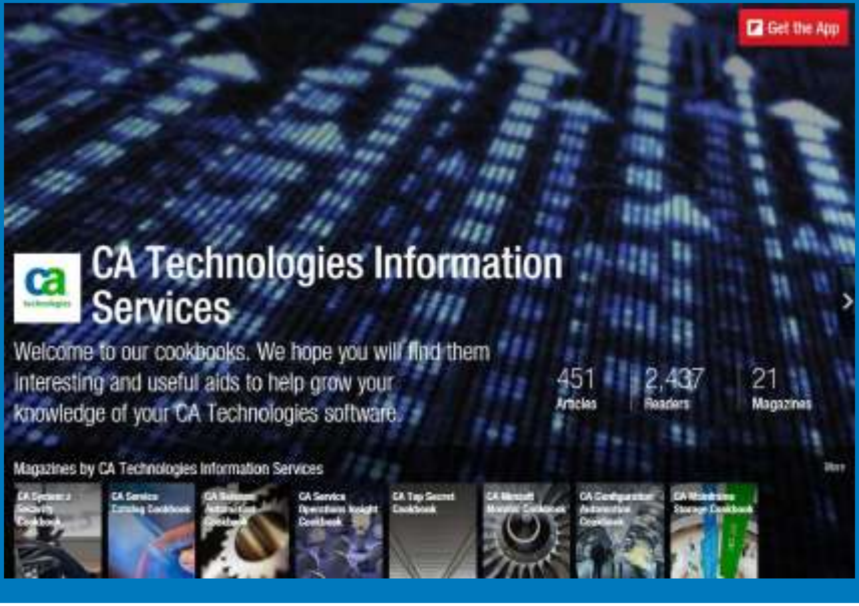
- Save the date for CA World 2014
- CA Flips for Flipboard
- CA Top Secret® for z/OS preparation for OMVS default user removal
- DLP Poll
- Q&A

Save the date !

CA World 2014

November 9-12, 2014 ~ Las Vegas, NV

CA Technologies Information Services Flipboard



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.

451 Articles | 2,437 Readers | 21 Magazines

Magazines by CA Technologies Information Services

Get the App
More
CA System z Security Cookbook
CA Service Catalog Cookbook
CA Release Automation Cookbook
CA Service Operations Insight Cookbook
CA Top Secret Cookbook
CA Nimsoft Monitor Cookbook
CA Configuration Automation Cookbook
CA Mainframe Storage Cookbook

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 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

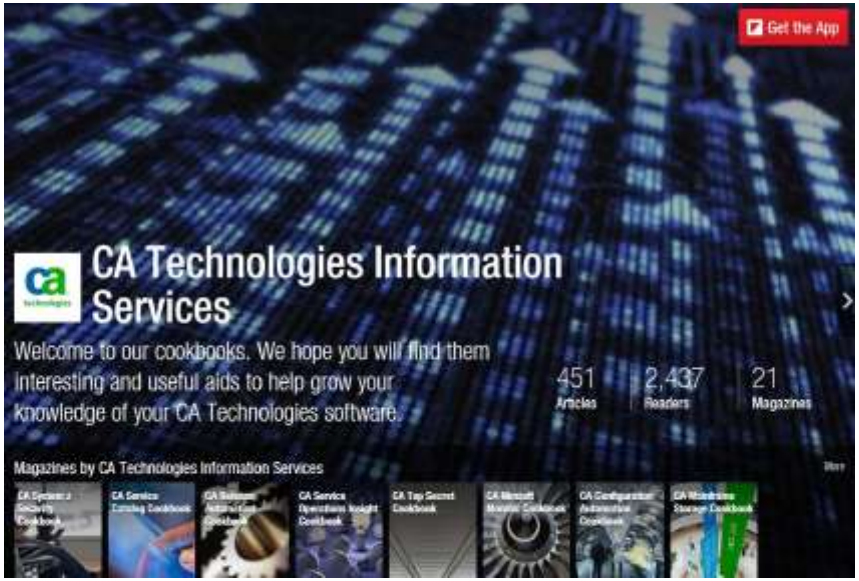
IBM z/OS 2.1 Support for CA ACF2 I CA System z Security Cookbook

Compare Security Records I CA System z Security Cookbook

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

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.”



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.

451 Articles

2,437 Readers

21 Magazines

Magazines by CA Technologies Information Services

Get the App
ca technologies
More
CA System z Security Cookbook
CA Service Catalog Cookbook
CA Release Automation Cookbook
CA Service Operations Insight Cookbook
CA Top Secret Cookbook
CA Nimsoft Monitor Cookbook
CA Configuration Automation Cookbook
CA Mainframe Storage Cookbook

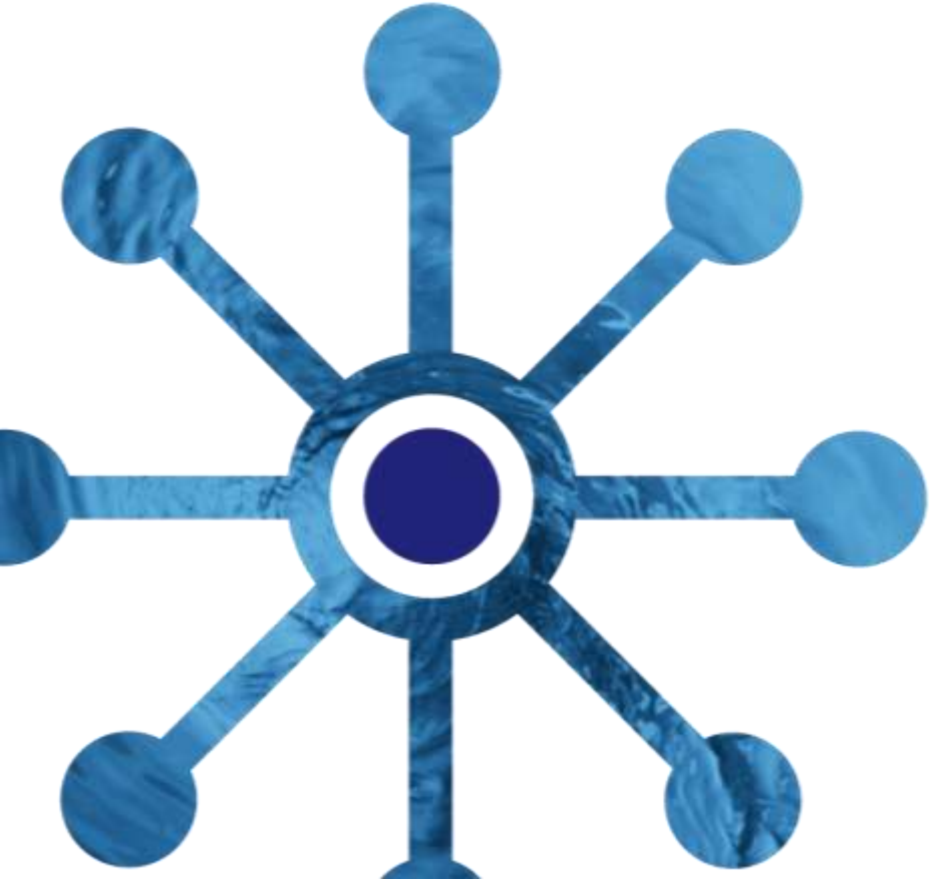
Don’t have a smartphone or tablet?

- 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 Top Secret® for z/OS r15

Preparation for OMVS defaults removal

Randy Kemmerer

Sr. Principal Software Engineer

Webinar series

December 5th, 2013

Agenda

- CA Top Secret® 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 OMVSUSR/OMVSGRP
  - Optional at z/OS 1.13 and below
  - Deactivated at z/OS 2.1 and above
- CA Top Secret® r15 for z/OS (TEC601436)
  - Technical document available on Support Online
  - Provides extensive details related OMVS defaults removal
- Questions & Answers

CA Top Secret™
Interim Enhancements – z/OS 2.1 support

2.1

- z/OS 2.1 CA Top Secret release/maintenance requirements
  - CA Top Secret r15 - Minimum required release to run z/OS 2.1

★ Customers running CA Top Secret r14 or lower will need to upgrade to r15 across all LPARS before implementing z/OS 2.1.

- Implement TSSMVS r15 related enhancement PTF's.
  - Solutions include:
    - **RO58980** – TSSOERPT report detect users that leverage BPX.DEFAULT.USER
      - Leveraged at z/OS 1.13 and below
    - **RO63150** – Adds CPF option to change UID/GID(?) to locally assigned UID/GID number.
    - **RO63740** – Support ampersand (&) in the HOME field (allows for &acid).
    - **RO61055** – Eliminate TSS9112E UNABLE TO DETERMINE JES LEVEL
  - Use FIXCAT: CA.TargetSystem-RequiredService.z/OS.V2R1

CA Top Secret™
Interim Enhancements – z/OS 2.1 support

2.1

- JES2/3 related features
  - JES2 & JES3 toleration support (RO61055)
    - TSS9112E UNABLE TO DETERMINE JES LEVEL
  - Support z/OS 2.1 JOBCLASS authorizations (RO63740)
    - In z/OS 2.1, you have the ability to grant authorization to use a specific job class to the owner or the submitter of a job.
      - PERMIT for JOBCLASS.node.class.jobname in the JESJOBS class.
      - PERMIT for IBMFAC classes to activate JESJOBS/JOBCLASS checking:
        - JES.JOBCLASS.OWNER
        - JES.JOBCLASS.SUBMITTER activate the checking

CA Top Secret™
Interim Enhancements – z/OS 2.1 support

2.1

- Certificate enhancements (RO63740)
  - Certificate verification after REPLACE command
    1. The certificate being added is a duplicate of an existing certificate and the labels of both certificates are the same or no label is specified.
    2. The existing certificate has a private key. The certificate being added is not a duplicate. The certificate being added has the same public key as the existing certificate.
    3. The existing certificate does not have a private key.
  - Display certificate chain information
    - When certificates are added with an ADD command, exported to a dataset with EXPORT command, and when LIST or CHKCERT command specifies the CHAIN parameter.
  - GENREQ modification
    - Do not allow certificate to be deleted in the database after GENREQ.

CA Top Secret™ Interim Enhancements – z/OS 2.1 support

2.1

- z/OS 2.1 compatibility and new functionality
  - Support &ACID variable in MODLUSER HOME field (RO63740)
    - HOME directory auto assigned using &acid/&ACID variables
      - Example: MODLUSER acid contains HOME(/u/&acid). BAKER01 logs on without OE credentials. BAKER01 ACID will be auto assigned : HOME(/u/baker01)
  - CHOWNURS control option removal (RO63740)
    - CHOWN_RESTRICTED authorization will now be controlled by the presence of the CHOWN.UNRESTRICTED resource in the UNIXPRIV resource class.

CA Top Secret™
Interim Enhancements – z/OS 2.1 support

z/OS 2.1

- Enhanced AUTOUID and AUTOGID (RO63150)
  - AUTOUID/AUTOGID is leveraged whenever UID(?) or GID(?) is specified on a CA Top Secret command.
    - The command generated in the RECOVERY file is modified to include the local system auto generated number. Prior to this maintenance, the command in the CA Top Secret RECOVERY FILE for both UID and GID would still contain a question mark (?)
    - Two new CA Top Secret Control Options CPFAUTOUID and CPFAUTOGID.
      - CPFAUTOUID- CPF transmits a TSS command with the locally auto assigned UID value (instead of the ? value) when you are using the Command Propagation Facility (CPF).

      TSS MODIFY(CPFAUTOUID(NO|YES))

      - CPFAUTOGID - CPF transmits a TSS command with the locally assigned GID value (instead of the ? value) when you are using the Command Propagation Facility (CPF)
      - TSS MODIFY(CPFAUTOGID(NO|YES))

CA Top Secret™
Interim Enhancements – z/OS 2.1 support

- PKCS 11 Token Support – coming
  - PKCS 11 Key support will allow private keys to be generated within a secure token.
    - Requires a Crypto Express4 co-processor
    - Command processing updated to provide support
      - GENCERT, REKEY, RENEW, LIST, CHKCERT, AND P11TOKEN
    - R_datalib enhanced as well to indicate a private key from a secure key token.

TSS Control 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 Top Secret r15 control options **UNIQUSER & MODLUSER** can be leveraged to activate the equivalent support. Usage of both UNIQUSER and MODLUSER are detailed in the CA Top Secret Control Options Guide and technical document TEC601436.

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 Top Secret **tech docs** you care about….

CA Top Secret Tech doc: TEC601436

Preparation for removal of Default OMVSUSR and OMVSGRP

Provides implementation considerations related to eliminating OMVSUSR & OMVSGRP usage

- Available on CA Support Online website (TEC601436)
- Applicable at both z/OS 1.13 & z/OS 2.1
  - z/OS 1.13 and below – Remove control options OMVSUSR & OMVSGRP from TSS PARMS file.
  - z/OS 2.1 – Mandatory preparation steps.

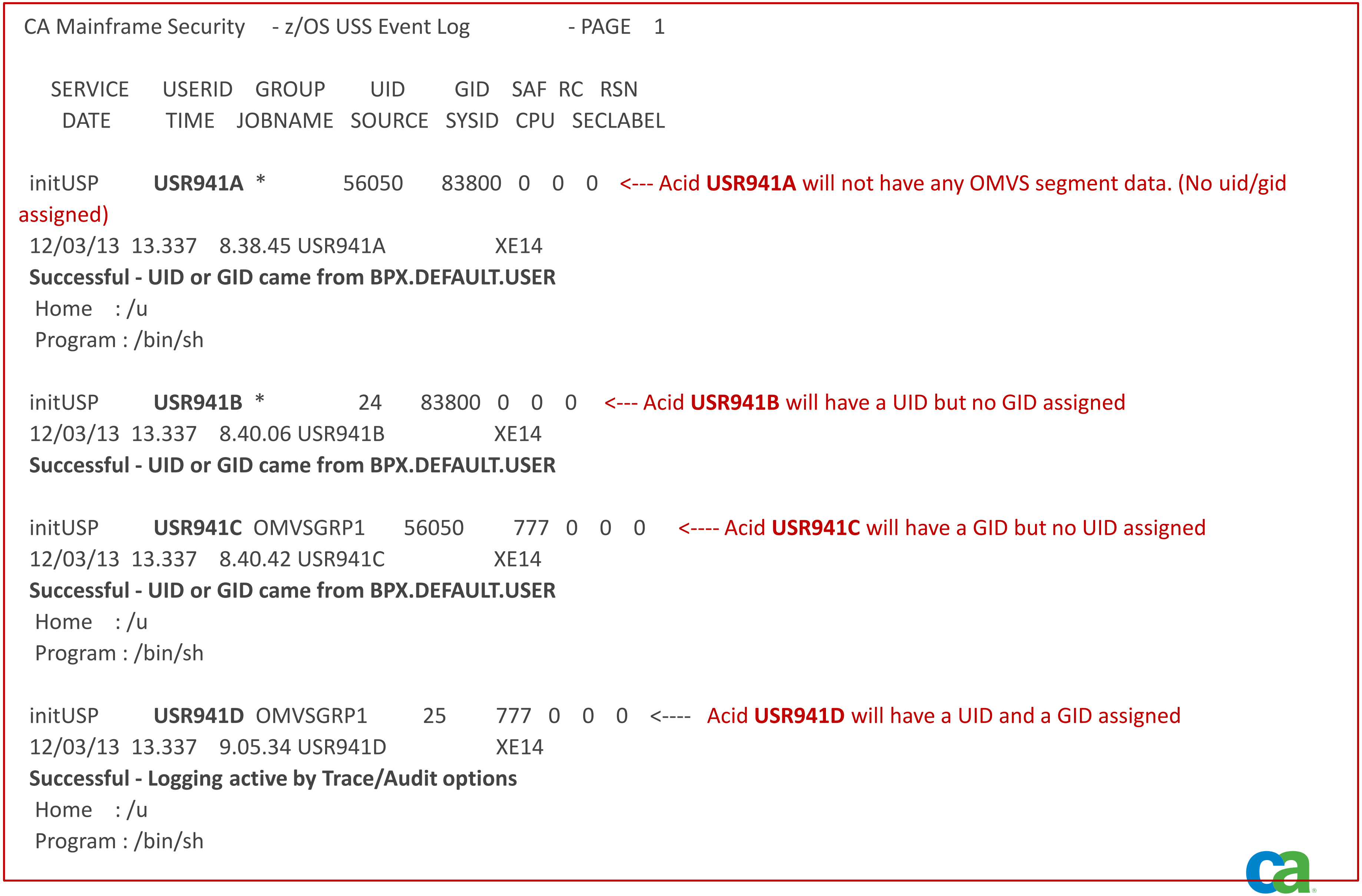
Tech doc: TEC601436

Preparation for removal of Default OMVSUSR and OMVSGRP

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

- RO58980 - 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 set CA Top Secret Control Option OPTIONS(32) to enable the USS logging feature and OPTIONS(85) to generate the default use trace messages.
  - TSSOERPT will report on any successful initUSP callable service that has used the BPX.DEFAULT.USER values.

TSSOERPT 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   <--- Acid 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   <--- Acid 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      <---- Acid 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   <----   Acid 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: TEC601436

Preparation for removal of Default OMVSUSR and OMVSGRP

How Groups & Default Groups are handled under CA Top Secret

- At sign-on TSS builds group list based on:
  - Assigned Groups on ACID record
  - Any IBMGROUP permissions on ACID (via profile or ALL record)

- At sign-on TSS assigns the users connect group based on:
  - GROUP field from the signon (group must be in the groups list)
  - DFLTGRP 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: TEC601436

Preparation for removal of Default OMVSUSR and OMVSGRP

Steps to perform before using UNIQUSER & MODLUSER

- Implement TSSMVS r15 related enhancement PTF’s.
- Identify ACIDs that have pre-existing OE authorization assignments.
- Reconcile OMVS assignments across all applicable LPARs for these ACIDs.
- Define the MODLUSER acid (or use the existing OMVSUSR acid).
- Identify the highest UID that is currently assigned on each LPAR (If leveraging CPF).
- Determine/setup - related TSS control options

Tech doc: TEC601436

Preparation for removal of Default OMVSUSR and OMVSGRP

Identify ACIDs that have pre-existing OE authorization assignments

- TSSCFILE – TSS LIST(ACIDS) SEGMENT(OMVS)
- TSS OMVS related CFILE record ID's

4401 – UID
4402 – GID
4403 – HOME
4404 – OMVSPGM
4405 – DLFTGRP

TSS OMVS related USER LIMITS CFILE record ID's
4406 – ASSIZE
4407 – MMAPAREA
4408 – OECPUTM
4409 – OEFILEP
4410 – PROCUSER
4411 – THREADS

Tech doc: TEC601436

Preparation for removal of Default OMVSUSR and OMVSGRP

Reconcile OMVS assignments across all applicable LPARs

- Verify ACIDs 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: TEC601436

Preparation for removal of Default OMVSUSR and OMVSGRP

Reconcile OMVS assignments Gotcha

- Changing an ACID’s UID in Top Secret (or ACF2/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: TEC601436

Preparation for removal of Default OMVSUSR and OMVSGRP

MODLUSER ACID possible field assignments

- HOME – Leverage variable &acid or &ACID
- OMVSPGM
- OECPUTM, OEFILEP, ASSIZE, PROCUSER, THREADS, MMAPAREA, MEMLIMIT, SHMEMMAX
- Default Group (DFLTGRP) – auto assigned only if ACID does not have a default group.

Tech doc: TEC601436

Preparation for removal of Default OMVSUSR and OMVSGRP

MODLUSER/UNIQUSER Gotcha – partial OMVS Segment

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

Tech doc: TEC601436

Preparation for removal of Default OMVSUSR and OMVSGRP

CPF enhancements

- CPFAUTOUID –
  - NO- propagates UID(?) on outbound commands
    - Leverages DFLTRNGU range on remote LPAR(s)
  - YES- propagates the generated UID (local LPAR)
    - Does not leverage DFLTRNGU range on remote LPAR(s)
- CPFAUTOGID –
  - NO- propagates GID(?) on outbound commands
    - Leverages DFLTRNGG range on remote LPAR(s)
  - YES- propagates the generated GID (local LPAR)
    - Does not leverage DFLTRNGG range on remote LPAR(s)

Tech doc: TEC601436

Preparation for removal of Default OMVSUSR and OMVSGRP

CPF Gotcha’s – CPF’ing a TSS ADD of a UID

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

Tech doc: TEC601436

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 DFLTRNGU range keyword
      - Eliminates possible UID collisions

SAMPLE usage: DFLTRNGU

SYS1 (via TSS PARMS) **DFLTRNGU(1000000,1999999)**

SYS2 (via TSS PARMS) **DFLTRNGU(2000000,2999999)**

SYS3 (via TSS PARMS) **DFLTRNGU(3000000,3999999)**

SYS4 (via TSS PARMS) **DFLTRNGU(4000000,4999999)**

SYS5 (via TSS PARMS) **DFLTRNGU(5000000,5999999)**

In addition to setting control option DFLTRNGU, you will also need to set in TSS PARMS the following control options on all 5 LPARs:

- UNIQUSER(ON)
- MODLUSER(acid) – This can be the acid that is assigned to the OMVSUSRP control option
- CPFAUTOUID(YES)

Tech doc: TEC601436

Preparation for removal of Default OMVSUSR and OMVSGRP

HFSSEC (externalize USS security) Impact

- HFSSEC – CA Top Secret control option 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 ACIDS 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 Top Secret product.

Tech doc: TEC601436

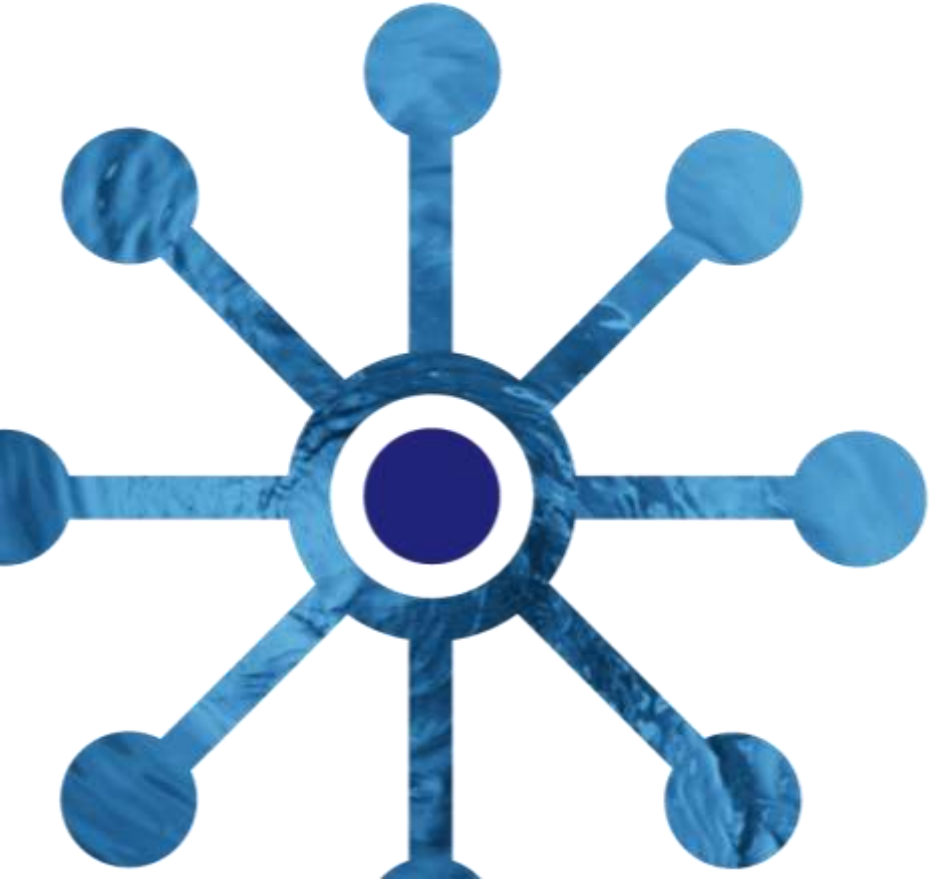
Preparation for removal of Default OMVSUSR and OMVSGRP

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 Top Secret release configuration
  - **Gotcha Alert:** Before implementing MODLUSER/UNIQUSER, all LPARS should be running Top Secret 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.