

CA Top Secret® for z/OS

The Road Leading to r16 and a Sneak Peek into What's Coming to Better Protect your Enterprise



Jeff Cherrington ~ Portfolio Manager
Jeffrey.Cherrington@ca.com



Paul Rauchet ~ Director, Software Engineering
Paul.Rauchet@ca.com

Agenda

1

WHAT HAVE WE BEEN UP TO? WE ARE AGILE!

2

POST CA TOP SECRET R15 GA ENHANCEMENTS

3

CA TOP SECRET R16 – RELEASE CHARTER & PLAN

4

R16 ENHANCEMENTS – THINGS YOU NEED TO CONSIDER

5

Q & A

Many changes – all for the good!



Source: <http://dilbert.com/strip/2003-01-10>

CA Top Secret is now Agile

ag·ile

/'ajəl/

Adjective

Relating to or denoting a method of project management, used especially for software development, that is characterized by the division of tasks into **short phases of work** and **frequent reassessment** and **adaptation of plans**.

"agile methods replace high-level design with frequent redesign"

Is it too late to join the CA Top
Secret r16 Beta Program?

A Big Fat NO!!!!!!!!!!

How to Join the TSS r16 Beta Program

- Go to validate.ca.com
- Register and sign CA's Beta Agreement
- Once accepted, you will have access to the code and documentation for TSS r16
- Next, create a sandbox in your environment if you haven't already
 - r16 is not GA and should NOT be brought into a production environment at this time
- From validate.ca.com, download and IPL the PAX file and latest cumulative PTF file into your sandbox
- Schedule a test plan call with TSS Product Owner, kimberly.hatch@ca.com

What have we been up to?

CA TOP Secret® for z/OS
r15 post GA enhancements

CA Top Secret r15 post GA enhancements

- Mirror Feature. Creates a mirror of the security file for immediate restart in case of file device/channel failure.
- Enforce security administrators to follow NEWPW rules when issuing password related Top Secret commands.
- JES2/JES3 shutdown/restart improvements.
- Performance improvements as a result of reduced storage obtains.
- Enhanced restricted password list.
- Expansion of COMPARE command to include other ACID types.
- Refinement of WHOHAS command.
- All TSS MODIFY commands checked as CASECAUT resources.
- FACILITY tracking added to CA Cleanup interface.
- Utility improvements to TSSUTIL, LDAP, TSSAUDIT, TSSSIM.
- CHKCERT and Certificate Utility display Public/Private key size and type.
- ECC keys can be stored and retrieved for ICSF.
- Eliminate need for superuser privilege for user mount and unmounts.

Addresses Customer Compliance Requirement



Post TSS r15 GA enhancement details

Security File Mirror support

- TSS Control option: **MIRROR(ON)**
 - Mirror copy of primary security file maintained.
 - Provides up-to-the-minute alternate security file.
 - Available only when SHRFILE(NO) and MIRROR(ON) are both set.
 - Designed to have no impact on primary security file performance.

Benefits:

- Can eliminate the need to perform forward recover processing when Mirror file is used as primary file.
- Use emergency startup PROC to recycle Top Secret with the Mirror file as primary file
- Note: Top Secret Backup processing can be done once per week

Post TSS r15 GA enhancement details



Compliance
Assist

NEW Password Admin change restrictions

- TSS Control option: **PWADMIN(YES)**
 - Security administrators:
 - Forced to follow NEWPW rules
 - Be restricted from changing the password expiration interval for individual users

Benefits:

- Centralized and decentralized administrators can no longer:
 - Bypass NEWPW requirements
- Or**
- Change PSWD EXPIRE interval for individual users

Post TSS r15 GA enhancement details

z/OS 2.1 – Updates

- Default USER no longer supported
 - USS access requires unique OE Credentials.
- CHOWNURS control option removal
 - UNIXPRIV(CHOWN.UNRESTRICTED)
 - Per ACID basis as needed.
- JES2/3 related features
 - JES2 & JES3 toleration support
 - Support z/OS 2.1 JOBCLASS authorizations
 - Now grant authorization to use a specific job class to Owner or job submitter:
 - 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 – to activate checking



Post TSS r15 GA enhancement details



Compliance
Assist

Support &ACID variable in MODLUSER HOME field

- **HOME directory auto assigned using &acid/&ACID variables**
 - MODLUSER acid contains HOME(/u/&acid). Fred01 logs on without OE credentials. Fred's ACID will be auto assigned : HOME(/u/fred01)
- **Enhanced AUTOUID and AUTOGID**
 - UID(?) or GID(?) is specified on a CA Top Secret command:
 - RECOVERY file command to include the local system auto generated number instead of a question mark(?).
- **CPFAUTOUID and CPFAUTOGID (newly added)**
 - CPF transmits a TSS command with the locally auto assigned UID value (instead of the question mark (?) value) when you are using the Command Propagation Facility (CPF).

Post TSS r15 GA enhancement details



Compliance
Assist

Certificate enhancements

- **Certificate REPLACE command improved:**
 - Duplicate certificate checking
 - Labels the same
 - Label not specified
 - Public and Private key checking
 - Existing certificate has a private key and certificate being added is not a duplicate.
The certificate being added has the same public key as the existing certificate.
 - The existing certificate does not have a private key.
- **Display certificate chain information**
 - ADD, LIST, EXPORT and CHKCERT commands
- **GENREQ modification**
 - Retain private key when old certificate is deleted.

Post TSS r15 GA enhancement details



Compliance
Assist

- **Datacom A/D support for CIA and Compliance Manager**
 - Added CA Datacom A/D support for both CIA and Compliance Manager.
 - Datacom A/D Black-box installs with base products
- **Expand the interface with JES2**
 - Provide additional ability to improve shutdown process
 - CA Top Secret can now be the very last task shutdown
 - Spool files dynamically allocated and de-allocated
 - JES2/3 monitored for normal or abnormal shutdown
- **Reduced Storage Obtains**
 - Grouped storage usage
 - Reduced the number of calls
 - Reduces CPU utilization per every RACROUTE call
 - Improved performance of high volume CPU bound calls

Post TSS r15 GA enhancement details



Compliance
Assist

- **Enhanced RPW (restricted password list)**
 - Enforce RPW for any position in new password
 - Requires new control option NEWPW(RT) to be set.
- **Expand TSS COMPARE**
 - Allows for other ACID types to be compared including type: Zone, Division, Department and Profiles
- **TSS WHOHAS updates**
 - Reflects only those resources that match a specific ownership
 - Removed any duplicates from list
- **TSS MODIFY control by CASECAUT**
 - All TSS Modify commands now under CASECAUT
 - Console Bit checked first
 - If bit off then do resource check
 - Prefixing and masking **NOT** allowed.

Post TSS r15 GA enhancement details



Compliance
Assist

- **Facility usage tracked via CA Cleanup for Top Secret**
 - Allows for cleanup of profiles that only include a Facility.
- **Tracking TRANID Bypassed Transactions Used**
 - TSSUTIL report shows transactions leveraged in the TRANID Bypass list.
 - The Resource (TYPE & NAME) will specify a '+' followed by the transaction id.
 - Allows for easy identification of TRANID bypassed transaction usage.
- **CA LDAP and TSSSIM**
 - TSSSIM now a service to CA LDAP
 - Allows for Logging in the TSSSIM process
 - Allows CA LDAP to make external calls and create logged events
- **TSSUTIL updates**
 - Allow for specific name on resource & Multi-line support on input
- **TSSAUDIT updates** - Search by Date and Time (like TSSUTIL)
- **INACTIVE support extended**
 - INACTIVE control option max interval extended from 255 days to 999 days.

Post TSS r15 GA enhancement details



Compliance
Assist

- **Department ACID maximum size Increased**
 - Supported size increased to 1024
- **DB2 V11 support**
 - Support for DB2 v11 added.
- **IMS 13.1 support**
 - Support for IMS 13.1 added.
- **User Defined Fields enhanced to support**
 - Compliance Information Analysis (CIA) component
 - batch load and real-time processes.
- **FSACCESS control option**
 - Performance improvement - Newly added control option setting allows customers to disable security calls related to FSACCESS checks.
- **CTS 4.2 support – CTS 4.2 support**

Post TSS r15 GA enhancement details



Compliance
Assist

z/OS 1.13 compatibility and new functionality

- New R_usermap function return Userid from DN or Realm name
- Password Phrase support
 - CESL transaction supports sign-on with password or password phrase
- Idle time-outs (locktime)
- **Certificate Key display changes**
 - CHKCERT command now displays Public/Private key size and type
 - Certificate Utility (SAFCRRPT) displays key size and type in header
- **ECC (Elliptic Curve Cryptography) Keys and ICSF**
 - Certificate commands allow for ECC key to be stored and retrieved from ICSF
- **Kerberos address checking**
 - New CHKADDRS field in REALM record
 - Allows ticket address checking in Kerberos server
- **User mount and unmount**
 - Privilege checking accomplished by resource checks
 - No need for all users to have superuser privilege

CA TOP Secret r16 enhancements

Completed - In progress - Planned

CA Top Secret r16 Release Charter

Agile

VISION

Our customers entrust CA Top Secret with the protection of their critical business assets. As we want to continue to earn that trust, we intend to maintain the currency of the product, improve the security protection it affords and improve its efficiency, both in valuable system resources and the time and effort it takes for our customers to exploit its features.

GOALS

Reduce installation time:

Application of maintenance will occur within a single day, reducing upgrade time by 20-80%.

Improve productivity:

Top Secret will support a 1024K ACID size in support of larger structures, increasing ownership sizes and number of users attached to departments and profiles.

Improve security and compliance:

Password encryption will be improved dramatically. The new AES256 password encryption key length will be at least 100% larger than the earlier password keys. This will allow customers to provide proof to auditors that CA Top Secret helps them achieve compliance with regard to password encryption.

FOR INFORMATION PURPOSES ONLY

terms of this presentation

Copyright © 2015 CA. All rights reserved. IBM, System z, zEnterprise, zSeries, z/OS, z/VM, RACF, CICS, IMS and DB2 are trademarks of International Business Machines Corporation in the United States, other countries, or both. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

This presentation was based on current information and resource allocations as of July 2015 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.

CA Top Secret r16 Release Plan

(as of July 14th)

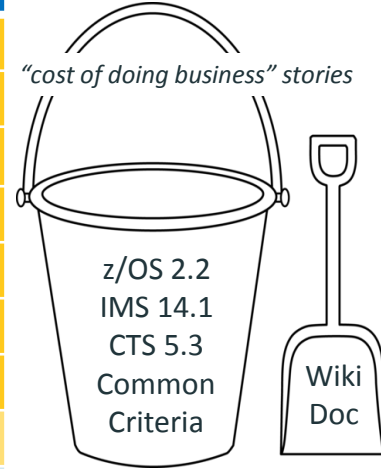
Delivered



= Customer Ideation

(# votes) = Ideation votes

(#) = Beta call votes



r16



Popular Ideas
trending on CA
Communities

V 1/Ideas	P	Deliverable / Feature / Epic	Beta 7/8/15		Status
n/a	1	Post Top Secret r15 GA Enhancements			Delivered
n/a	2	z/NEXT Certification (z13)			Completed
B-66394	3	Increased User Record Size (ACID) to 1024K	(2)		Delivered
B-32821	4	Improve WHOHAS UID(0) Reporting	(3)		Delivered
B-76252	5	Option to Disable CICS Bypass Processing			Delivered
E-11835	6	Store FACILITY Parameters On Security File	(6)	10	Delivered
B-55474	7	Restrict UID 0 Assignment To Specific Admins	(4)	5	Delivered
B-66429	8	AES 256-Bit Password Encryption	(5)		In Progress
B-83470	9	Allow TSSCFIL to run against the backup file	(10)	6	Planned
B-83469	10	Enhance OMVS admin when adding DFLTGRP	(5)	17	Planned
B-28494	11	Allow ADMIN Suspend for PWOnly Nodes in CPF	(5)		Under Review
B-57739	12	Allow Suspension of Users in Cross Memory			Under Review
235715703	13	Modify Facility should display % used for PRFT & MAXUSER	(7)	9	Under Review
235713617	14	Retire IDs leaving them on database	(5)	5	Under Review
235718336	15	NEWPHRASE support for LC, UC & TS	(4)	12	Under Review
235718112	16	CIA updated to include "Profile name" field	(4)	6	Under Review
235719395	17	Write protect TSS7003W – PSWD WILL EXPIRE ON mm/dd/yy	(3)	5	Under Review
235717117	18	Enforce Passphrase only for validation	(2)	6	Under Review
235717791	19	Extend TSS-Command by change-identifier-operand	(2)	7	Under Review
235722192	20	NOSUBCHK Granularity		5	New

r16 enhancement details



Compliance
Assist

Store FACILITY Parameters On Security File

- TSS Control option: **FACSTOR(YES|NO)**
- Store facility matrix entries on the security file (instead of the parameter file).
 - When you specify FACSTOR(YES):
 - Entries are hardened to the security file after the product is restarted.
 - Any changes to the entries are:
 - automatically stored on the security file
 - logged to the recovery file.

Benefits:

- Facility definitions protected from view (no longer in TSS PARMS file).
- Easier to administer and maintain multiple LPAR complexes.
- Size of the TSS PARMS FILE greatly reduced.

r16 enhancement details



Compliance
Assist

Restrict UID 0 Assignment To Specific Admins

- MSCA exempt from UID(0) restriction
- Restriction performed via CASECAUT(TSSCMD.ADMIN.UID0) authority checking, when:
 - Admin (all types) has ACID(MAINTAIN) authority
 - UID(0) is present within a TSS ADD or REPLACE command string
 - If an ACID already has UID 0, no restriction is enforced to remove it, or replace it with non-zero value.
 - Only if the intent is to give an ACID UID 0 does restriction occur.

Benefits:

- Further restricts who can assign authorization for UID(0).
- Satisfy compliance requirements

r16 enhancement details



Compliance
Assist

AES 256-Bit Password Encryption (underway)

- CA Top Secret currently supports 128-bit AES encryption for passwords and phrases. It requires a 16 byte encryption key and can be done via software or hardware. IBM has provided 256-bit AES encryption for RACF passwords/phrases in z/OS 2.1. This enhancement will provide the same for TSS.

Benefits:

- Adds advanced password encryption algorithm which satisfies current corporate as well as government compliance requirements.

r16 enhancement details

Increased User & Profile Record Size (ACID) to 1024K

- You can now assign a maximum value of 1024 using the MAXACIDSIZE Control Option parameter.

Benefits:

- Reduce complexity and cost to maintain security related updates.
 - Help to reduce security administration complexity for sites running with:
AUTH(OVERRIDE,ALLOVER)
 - Eliminate/delay need to add new Profiles
 - Allow for profile consolidation where possible
- Role based security improved
 - Reduce the number of profiles required to build role bases security profiles.

r16 enhancement details



Compliance
Assist

Option to Disable CICS Bypass Processing

- CA Top Secret CICS Facility sub option: (BYPLIST=NO|YES|AUDIT)
 - BYPLIST=NO Disables bypass list by facility
 - BYPLIST=YES Enables bypass list by facility – this is the default
 - BYPLIST=AUDIT Works similar to **Tracking TRANID Bypassed Transactions Used** feature without the need to add +A to transactions in the TRANID bypass list.

Benefits:

- Option to enforce defined security authorizations eliminating use of the BYPASS list.

Improve WHOHAS UID(0) Reporting

- Prevents false positives from UID persistence after ACID deletion

r16 enhancement details – Status : Planned

Execute TSSCFE against the Top Secret Backup File

- Leverage the TSS Backup file for TSSCFE execution

Benefits:

- Eliminates the overhead of executing TSSCFE against the live (Primary) CA Top Secret security file.
 - Removes inadvertent performance impact when TSSCFE is run during busy workloads.
 - Expand TSSCFE execution window to include prime time processing periods.
 - Establishes a point in time snapshot:
 - Eliminates output anomalies caused by Top Secret commands processed during TSSCFE execution.

r16 enhancement details – Status : Planned

Enhance USS administration when adding DFLTGRP

- Cross check to verify that the GROUP name used in the DFTLGRP field:
 - Is an existing valid GROUP
 - that is assigned to target ACID's GROUP list.
 - Has a GID assigned to it.

Benefits:

- Ease of administration.
- Ensures valid O/E credentials are set.

Why should CA Top Secret r16 be on your radar?



CA Top Secret r16 Benefits



- **All existing CA Top Secret r15 corrective solutions incorporated into the r16 release.**
 - Sourced through the last week of the Beta!
 - Get current and level set on maintenance as you rollout the new release
- **45 (and counting) new features available**
 - Majority of the features generated from customer requests
 - Many tied to **compliance requirements** (breach protection)
- **z/OS 2.2 new feature exploitation**
 - Get LPARs staged and ready to IPL and exploit the newly introduced z/OS 2.2 related security features.
- **IBM z13 hardware certified**
- **Common Criteria certified**

**More info and getting
involved....**

Where will we be showing up?

The CA Mainframe Security R&D security teams currently sponsor 4 user groups. The next set of meetings are scheduled to take place in the Fall.

Mid Atlantic Security User Group – This user group, established in Nov, 2013, is targeted for customers that reside in: NJ, DEL, Eastern PA, NY & CT areas. Next meeting Location/Date: Hosted by user group member site in **Manhattan, NY – Date Mid Oct, 2015**

DC Area Security User Group – This user group, established in May, 2015, is targeted for customers that reside in: DC, VA, MD & South Central PA Next meeting Location/Date: **CA Technologies Inc. Herndon, VA – Date To Be Determined**

North Central Security User Group – This user group, established in March, 2014, is targeted for customers that reside in: IL, WIS, IND and Iowa. Next meeting Location/Date: **CA Technologies Inc. Lisle, Illinois – – Date To Be Determined**

South Central Security User Group – This user group, established in Sept, 2014, is targeted for customers that reside in: Northeast TX, OK, AK and LS. Next meeting Location/Date: **CA Technologies Inc. Plano, TX – – Date To Be Determined**

Other participation:

SHARE Conference - Orlando, FL: 8/9-8/13/2015 www.share.org

Bob Hansel and Stu Henderson RACF User Groups – Fall dates being planned – details forthcoming

Vanguard Security and Compliance Conference – Las Vegas, NV: 9/28 – 10/1/2015 www.go2vanguard.com

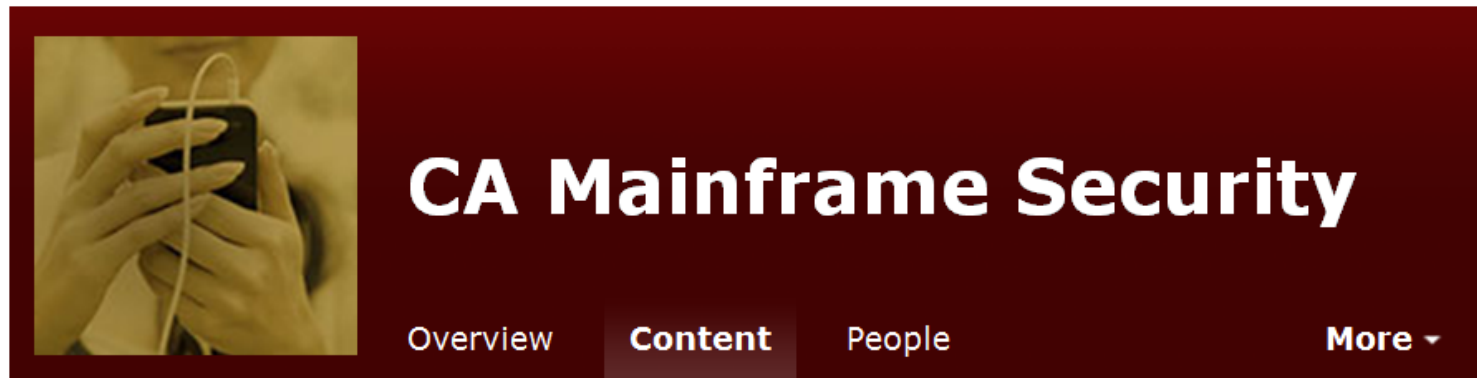
CA World 2015 - Las Vegas, NV: 11/16-11/20/2015 www.ca.com/caworld

CA World 2015: Mainframe Highlights



- 1.5 Days with 25+ Pre-Conference Education Sessions for IT Operations professionals that cover a wide range of topics for the Mainframe platform: Data Management, **Security**, Application Development, Workload Automation, Big Data Management, Performance & Monitoring, Storage Management and Output Management
- Meet and hear from customers and partners to learn how they are taking advantage of the Mainframe in the Application Economy at 15+ Theater Sessions, 20 Off the Floor Sessions, 15+ Demo Stations and Meet the Experts Stations. Sessions cover strategic themes, roadmap, strategy and specific business and technical challenges.

Get involved! Communities & Ideation



WELCOME TO THE CA MAINFRAME SECURITY COMMUNITY

New to the CA Mainframe Security Community?

[Get started here](#)

[Find another CA Mainframe community](#)

PRODUCTS COVERED

- [CA ACF2](#)
- [CA Auditor](#)
- [CA Cleanup](#)
- [CA Compliance Manager](#)
- [CA Top Secret](#)

ASK THE CA MAINFRAME SECURITY COMMUNITY

Ask it

FEATURED CONTENT

[Getting Started in the CA Mainframe Security Community](#)
1 month ago

by Lenn Thompson

[Goodbye Bookshelves.... Hello Wiki \(#DocOps!\)](#)
1 month ago

by Laura Fletcher

[CA ACF2 Webcast Today on z Exchange \(7/21 @ 2pm ET\)](#)
2 hours ago

by CARLA FLORES

CA WORLD '15



Register today and get special community member pricing.

UPCOMING EVENTS

[CA ACF2 Webcast Today on z Exchange \(7/21 @ 2pm ET\)](#)
7/21/15 2:00 PM

[CA Top Secret update on z Exchange \(7/22 @ 2pm ET\)](#)
7/22/15 2:00 PM

<https://communities.ca.com/welcome>




Q & A



Paul Rauchet

Director, Software Engineering

Paul.Rauchet@ca.com

 [@raupa01](https://twitter.com/raupa01)



[in](#)