#SHAREorg

SHARE
Technology · Connections · Results

CA Security Update & Hidden Gems

Carla A. Flores

ca technologies

Tuesday – August 13, 2013

Session # 13649

Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project

SHARE in Boston

Voting SHARE

- Our own Jerry Seefeldt from NewEra Software

Agenda

CA ACF2™ for z/OS Update

CA Top Secret® for z/OS Update

Hidden Gems

Open Discussion/Questions

CA ACF2™ for z/OS r15 Incremental Enhancements (CY2013)

#SHAREorg

SHARE in Boston

CA ACF2 r15 GA recap

Restricted Administration

- Targets Passwords and related fields and Digital Certificate administration

New Administrative commands

- User comparison, user modeling, and user archiving

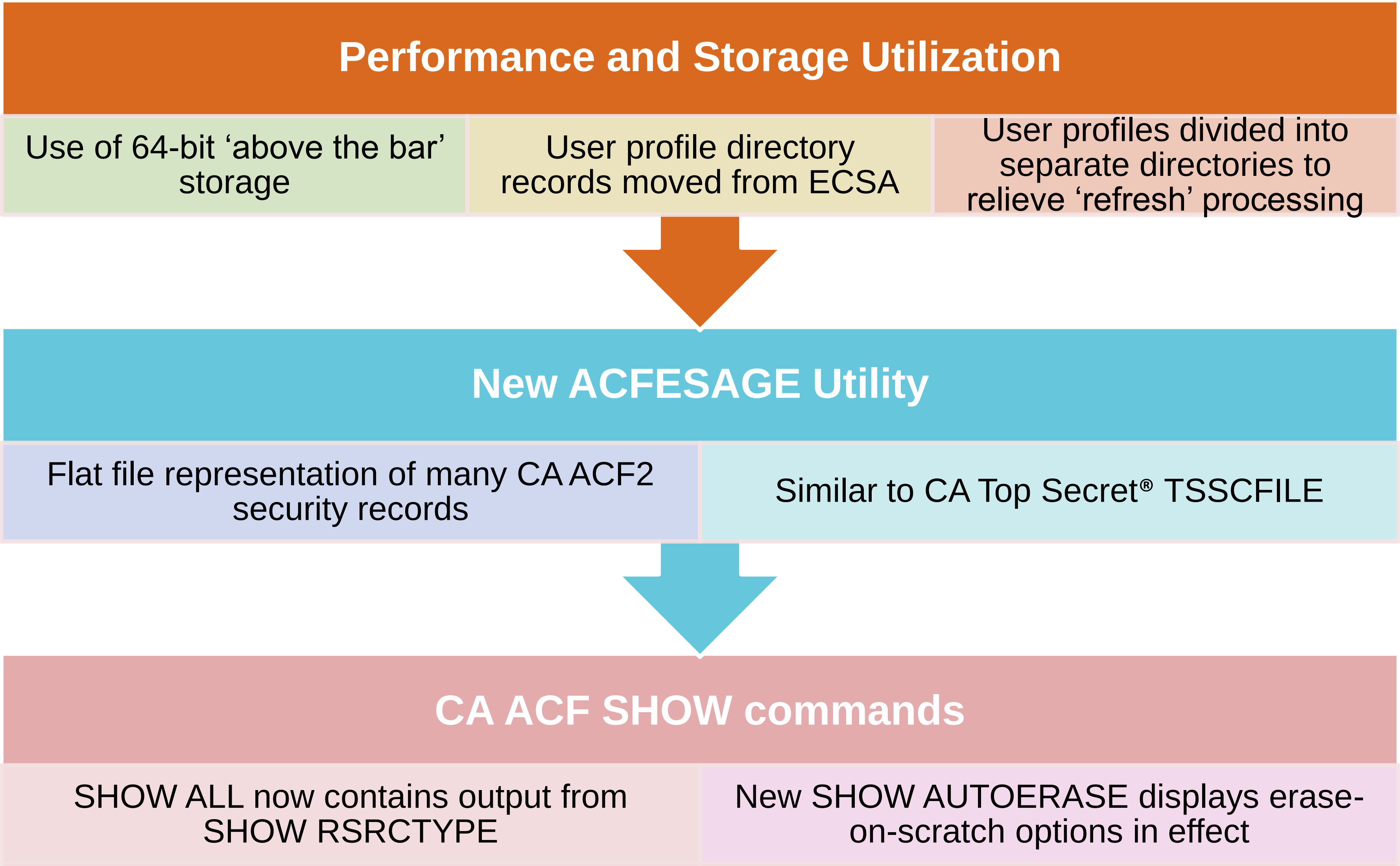
Certificate related enhancements

- New RENEW command, Large IDN/SDN support, Expanded Keyrings
- Expiring Certificate warnings, Password prompting
- Certificate utility: additional fields displayed, summary totals

Role reporting

- ACFXREF inclusion of XROLs to identify users that no longer exist
- New CMDS and BACKOUT files

CA ACF2 r15 GA recap



Performance and Storage Utilization

Use of 64-bit ‘above the bar’ storage

User profile directory records moved from ECSA

User profiles divided into separate directories to relieve ‘refresh’ processing

New ACFESAGE Utility

Flat file representation of many CA ACF2 security records

Similar to CA Top Secret® TSSCFILE

CA ACF SHOW commands

SHOW ALL now contains output from SHOW RSRCTYPE

New SHOW AUTOERASE displays erase-on-scratch options in effect

CA ACF2 r15 interim enhancements since GA

z/OS 1.13 compatibility and new functionality	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 GSO 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
	New R_ usermap function to return Userid from DN or Realm name	

CA ACF2 r15 interim enhancements since GA

- IDMAP user profiles used during system entry
  - Maps distributed user information to an ACF2 logonid
- Identifies invalid distinguished names (IDMAPDN values)
- Complements new z/OS 1.3 R_usermap Identity Propagation functions

- Password Phrase support
  - CESL transaction supports sign-on with password or password phrase
  - ACFM UL function updated to support password phrase
  - Idle time-outs (locktime)

CA ACF2 r15 interim enhancements since GA

Role Based API (ACF00RBS) enhanced

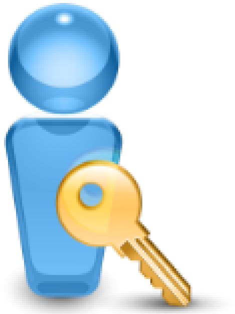
- Returns list of roles and group of roles for a given user
- Returns list of users for a given role - *New*
- New SYSID parameter to go after all role record types defined on the security database - *New*

CA Datacom®/AD support for CIA and CA Compliance Manager

- Added value for customers: removes DB2 restriction
- Black-box delivered with base product
- Delivered as part of CA Chorus™ for Security and Compliance Management 2.0 maintenance
- Available to non-CA Chorus customers

CA ACF2 Incremental Enhancements – CY2013

- Role-based Security
  - Enhanced Model and Archive commands
    - Role records now included
    - Builds ACF commands to generate a modeled user
    - Builds ACF commands to re-add an Archived user to role records
  - Clean-up X-ROL Role records when a user account is deleted
    - Role Include/Exclude fields updated for non-masked values
  - Incorporate Role rule sets in CA ACF ACCESS command
    - Previously only supported UID based Rule sets
  - Prevention of changing Role record type
    - X(ROL) records defined as ‘role’ or ‘group’ record type
    - Enhancement prevents modifying record type



CA ACF2 Incremental Enhancements – CY2013

Cross-Reference record expansion

- X(ROL), X(RGP) and X(SGP) from 4K to 16k
- Numerous customer requests to ease administration
- Must be running with larger Info-storage database

GSO INFODIR expanded

- Limitation of 256 entries doubled to 512
- New GSO INFODIR field TYPESX (expansion) used for additional entries

Digital Certificates

- Movement of internal certificate table to 64-bit storage
- Due to increased usage of certificates
- Unsupported Signature Algorithm checking

CA ACF2 Incremental Enhancements – CY2013

Symbolic substitution in Dataset Rules

- Reduces rule administration by allowing &LID as substitution string
- The &LID is used on the rule line within the dataset rule set

GSO LINKLIST enhancements

- System Symbolic substitution allowed as defined in SYS1.PARMLIB (IEASYM)
- Masking capabilities now permitted for Datasets

Optional use of Cancelled LID for RACROUTE EXTRACTS

- Equivalent support for all ESM's
- Prevents Processes from not working

CA ACF2 Incremental Enhancements – CY2013

ACFVSAM Reserve Enqueue Name	Allows the minor name for ACFVSAM ENQ/RESERVE name to be associated with dataset name instead of ddname
	Better granularity for users with multiple security files in same Sysplex
	Reduces contention on ACF2 VSAM usage
Logonid exclusion from Password / Passphrase Violations	Password violation counters will not be incremented for defined userids
	Prevents application outages due to violations
	Controlled through new resource class and resource rules
Unique UID and GID values	Helps make sure each user is accountable using a unique UID or GID value

CA ACF2 Incremental Enhancements – CY2013

IMS for z/OS Enhancements

- Security for the IMS DBCTL Environment
  - CA ACF2 IMS security for the IMS DBCTL (database only) environment
  - Security for PSBs and AOI commands
  - /ACF command available
- /ACF command in IMS OM environment
  - Support for the /ACF command entered from IMS OM environment
- Removal of CA ACF2 IMS requirement for IMS Security Macro
  - IBM is eliminating the SECURITY macro from IMS system definition

CA Top Secret® for z/OS r15 Incremental Enhancements (CY2013)

CA Top Secret r15 GA recap

Restricted administration

- Targets Passwords and related fields and Digital Certificate administration

New administrative commands

- User comparison
- User/Profile modeling
  - Allows permissions to be modeled
- User/Profile archiving
  - Allows permissions to be archived

CA Top Secret r15 GA recap

Certificate related enhancements

- New RENEW command, Large IDN/SDN support, Expanded Keyrings
- Expiring Certificate warnings, Password prompting
- Certificate utility: additional fields displayed, summary totals

Performance and Storage Utilization

- Use of 64-bit ‘above the bar’ storage
- User profile directory records moved from ECSA
- User profiles divided into separate directories to relieve ‘refresh’ processing

CA Top Secret r15 GA recap

Auditing Limits

- New match limit on Audit records
- Users
- Resources

Performance and Storage Utilization

- Use of 64-bit ‘above the bar’ storage
- Reduce and combine storage areas

CA Top Secret R15 interim enhancements since GA

z/OS 1.13 compatibility and new functionality

- 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
- New R_ usermap function to return Userid from DN or Realm name

CA Top Secret R15 interim enhancements since GA

CTS 4.2 compatibility and new functionality

- Password Phrase support
  - CESL transaction supports sign-on with password or password phrase
  - Idle time-outs (locktime)

CA Datacom/AD support for CIA and Compliance Manager

- CA Datacom/AD Black-box installs with base products

CA Top Secret R15 interim enhancements since GA

Expand the interface with JES2

- Provide additional ability to improve shutdown process
- CA Top Secret can now be the very last task shut down
- 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

CA Top Secret incremental enhancements – CY2013

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 ACIDS types to be compared
  - Zone
  - Division
  - Department
  - Profile

CA Top Secret incremental enhancements – CY2013

WHOHAS

- 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.

CA Top Secret incremental enhancements – CY2013

Facility and IBMGROUP usage

- Now tracked via CA Cleanup for CA Top Secret
- Allows for cleanup of profiles that only include one or both

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.
- See CA Top Secret Implementation: CICS Guide for details.

CA Top Secret incremental enhancements – CY2013

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 loggings

TSSUTIL

- Specific name on resource
- Multi-line support on input

TSSAUDIT

- Search by Date and Time (like TSSUTIL)

What are You Doing About BPX.DEFAULT.USER?

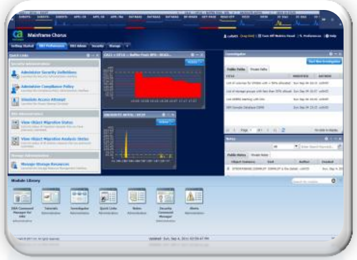
- Many of us use a FACILITY class rule named **BPX.DEFAULT.USER** which provides a default USS identity (UID and GID) for users that don’t have an OMVS segment.
- IBM plans to stop supporting **BPX.DEFAULT.USER** after Release 1.13
- You will need to use the BPX.UNIQUE.USER

- CA will be releasing a technical document on this topic and conducting a webcast
  - Email carla.flores@ca.com if you want this notification

CA Mainframe Chorus for Security and Compliance Management

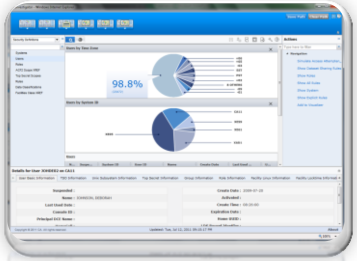
CA Mainframe Chorus

an overview…



Integrated Workspace

- Singular interaction model
- Fast Learning Curve



Role-Based Navigation

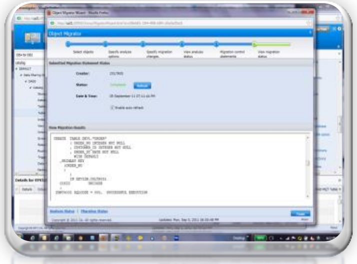
- Matches Job Functions
- Leverage resources across platforms

Graphical Diagnostics

- Data in human readable formats
- Solve problems faster

Knowledge Management

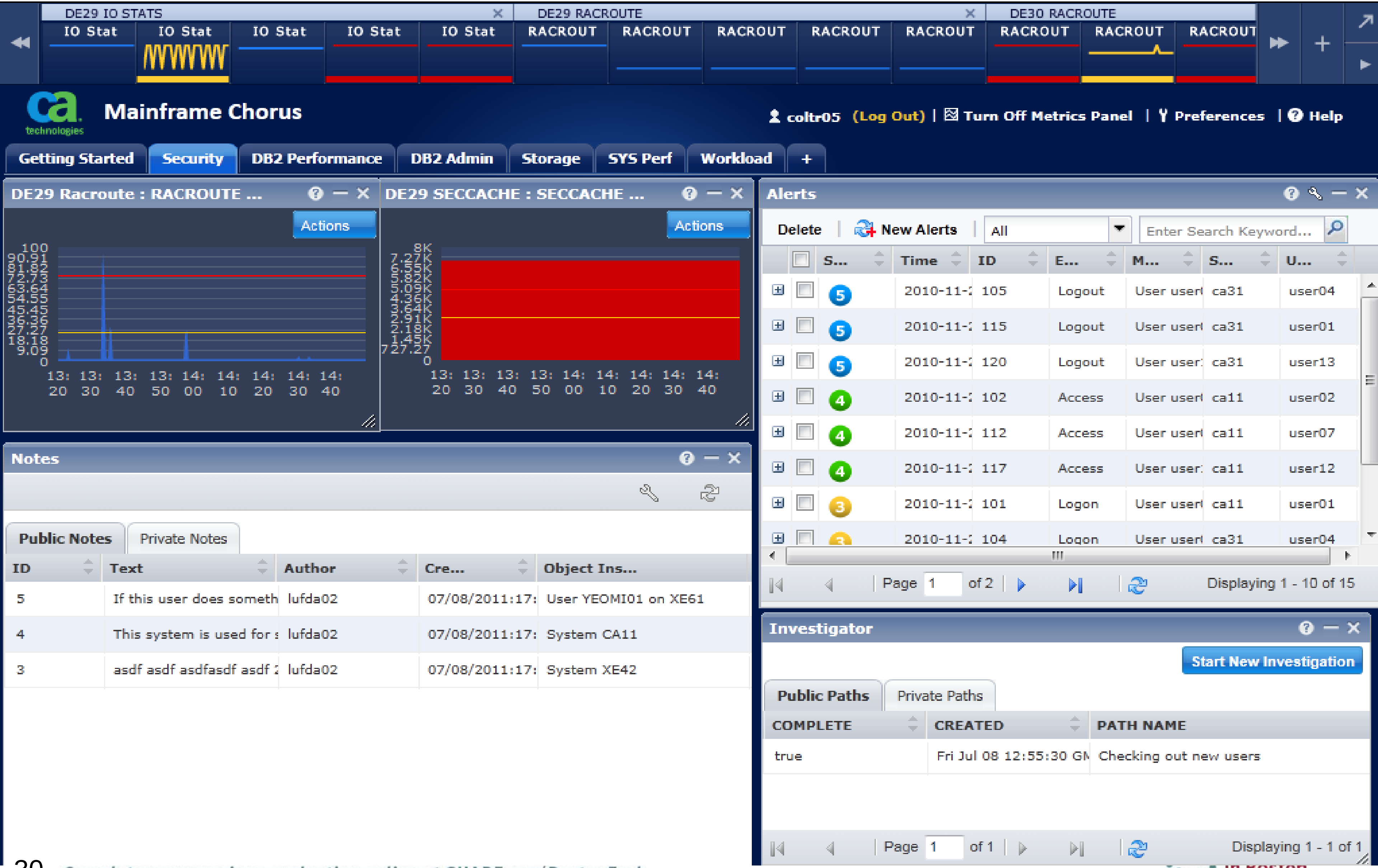
- Community knowledge and expertise at users fingertips
- Increases the whole team’s efficiency



Process Automation

- Wizard-like process tools
- Reduces possibility of errors

CA Mainframe Chorus ~ Security Workspace



Alerts

	S...	Time	ID	E...	M...	S...	U...
⊞ □	5	2010-11-:	105	Logout	User useri	ca31	user04
⊞ □	5	2010-11-:	115	Logout	User useri	ca31	user01
⊞ □	5	2010-11-:	120	Logout	User user:	ca31	user13
⊞ □	4	2010-11-:	102	Access	User useri	ca11	user02
⊞ □	4	2010-11-:	112	Access	User useri	ca11	user07
⊞ □	4	2010-11-:	117	Access	User user:	ca11	user12
⊞ □	3	2010-11-:	101	Logon	User useri	ca11	user01
⊞ □	3	2010-11-:	104	Logon	User useri	ca31	user04

Page 1 of 2 | Displaying 1 - 10 of 15

Notes

ID	Text	Author	Cre...	Object Ins...
5	If this user does someth	lufda02	07/08/2011:17:	User YEOMI01 on XE61
4	This system is used for :	lufda02	07/08/2011:17:	System CA11
3	asdf asdf asdfasdf asdf :	lufda02	07/08/2011:17:	System XE42

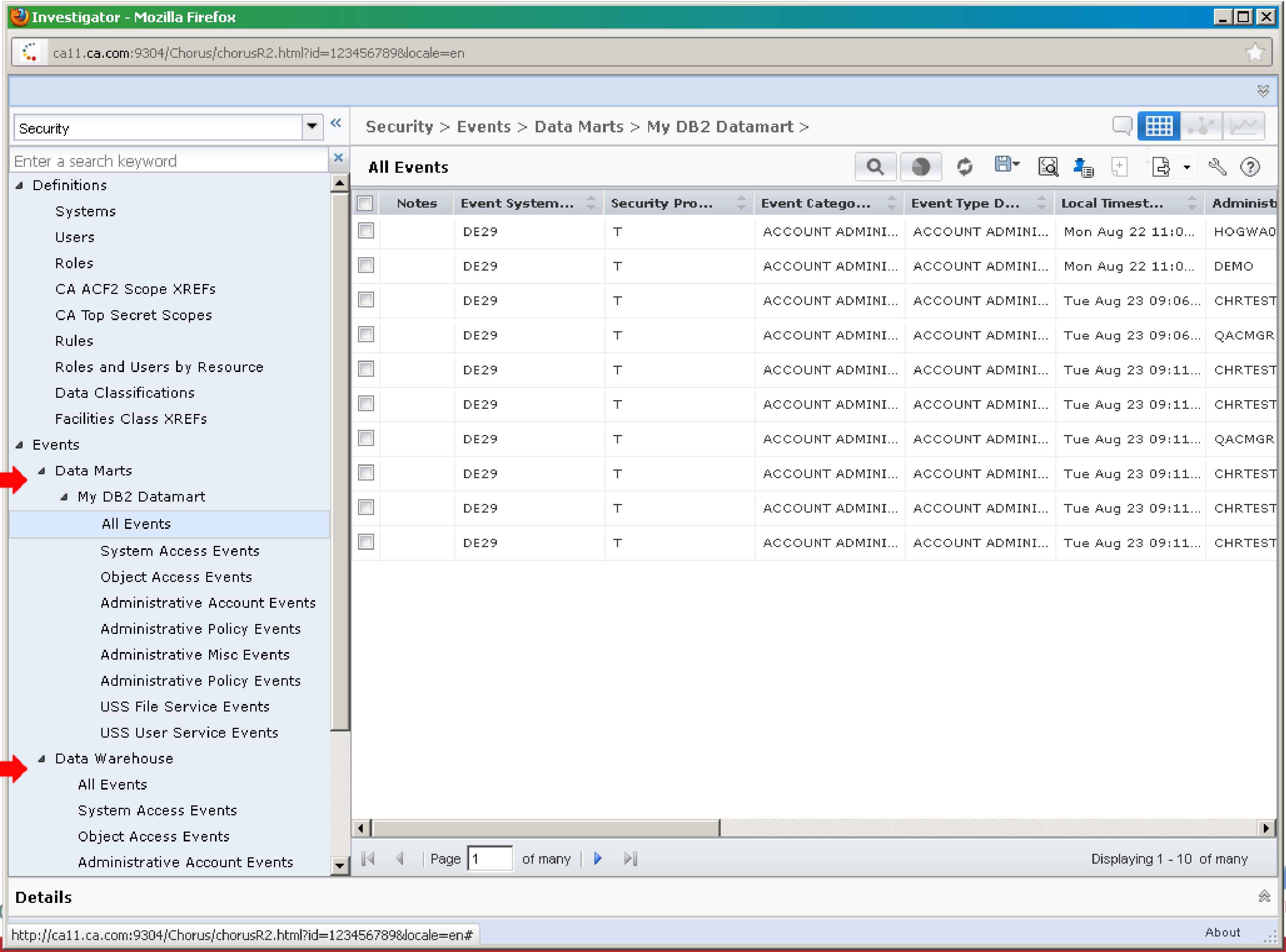
Investigator

COMPLETE	CREATED	PATH NAME
true	Fri Jul 08 12:55:30 GM	Checking out new users

Page 1 of 1 | Displaying 1 - 1 of 1

Complete your sessions evaluation online at SHARE.org/BostonEval

Datacom CIA, Data mart(s), and Warehouse



Investigator - Mozilla Firefox

ca11.ca.com:9304/Chorus/chorusR2.html?id=12345678&locale=en

Security

Enter a search keyword

- Definitions
  - Systems
  - Users
  - Roles
  - CA ACF2 Scope XREFs
  - CA Top Secret Scopes
  - Rules
  - Roles and Users by Resource
  - Data Classifications
  - Facilities Class XREFs
- Events
  - Data Marts
    - My DB2 Datamart
      - All Events
      - System Access Events
      - Object Access Events
      - Administrative Account Events
      - Administrative Policy Events
      - Administrative Misc Events
      - Administrative Policy Events
      - USS File Service Events
      - USS User Service Events
  - Data Warehouse
    - All Events
    - System Access Events
    - Object Access Events
    - Administrative Account Events

Security > Events > Data Marts > My DB2 Datamart >

All Events

□	Notes	Event System...	Security Pro...	Event Catego...	Event Type D...	Local Timest...	Administ
□		DE29	T	ACCOUNT ADMINI...	ACCOUNT ADMINI...	Mon Aug 22 11:0...	HOGWA0
□		DE29	T	ACCOUNT ADMINI...	ACCOUNT ADMINI...	Mon Aug 22 11:0...	DEMO
□		DE29	T	ACCOUNT ADMINI...	ACCOUNT ADMINI...	Tue Aug 23 09:06...	CHRTEST
□		DE29	T	ACCOUNT ADMINI...	ACCOUNT ADMINI...	Tue Aug 23 09:06...	QACMGR
□		DE29	T	ACCOUNT ADMINI...	ACCOUNT ADMINI...	Tue Aug 23 09:11...	CHRTEST
□		DE29	T	ACCOUNT ADMINI...	ACCOUNT ADMINI...	Tue Aug 23 09:11...	CHRTEST
□		DE29	T	ACCOUNT ADMINI...	ACCOUNT ADMINI...	Tue Aug 23 09:11...	QACMGR
□		DE29	T	ACCOUNT ADMINI...	ACCOUNT ADMINI...	Tue Aug 23 09:11...	CHRTEST
□		DE29	T	ACCOUNT ADMINI...	ACCOUNT ADMINI...	Tue Aug 23 09:11...	CHRTEST
□		DE29	T	ACCOUNT ADMINI...	ACCOUNT ADMINI...	Tue Aug 23 09:11...	CHRTEST

Page 1 of many

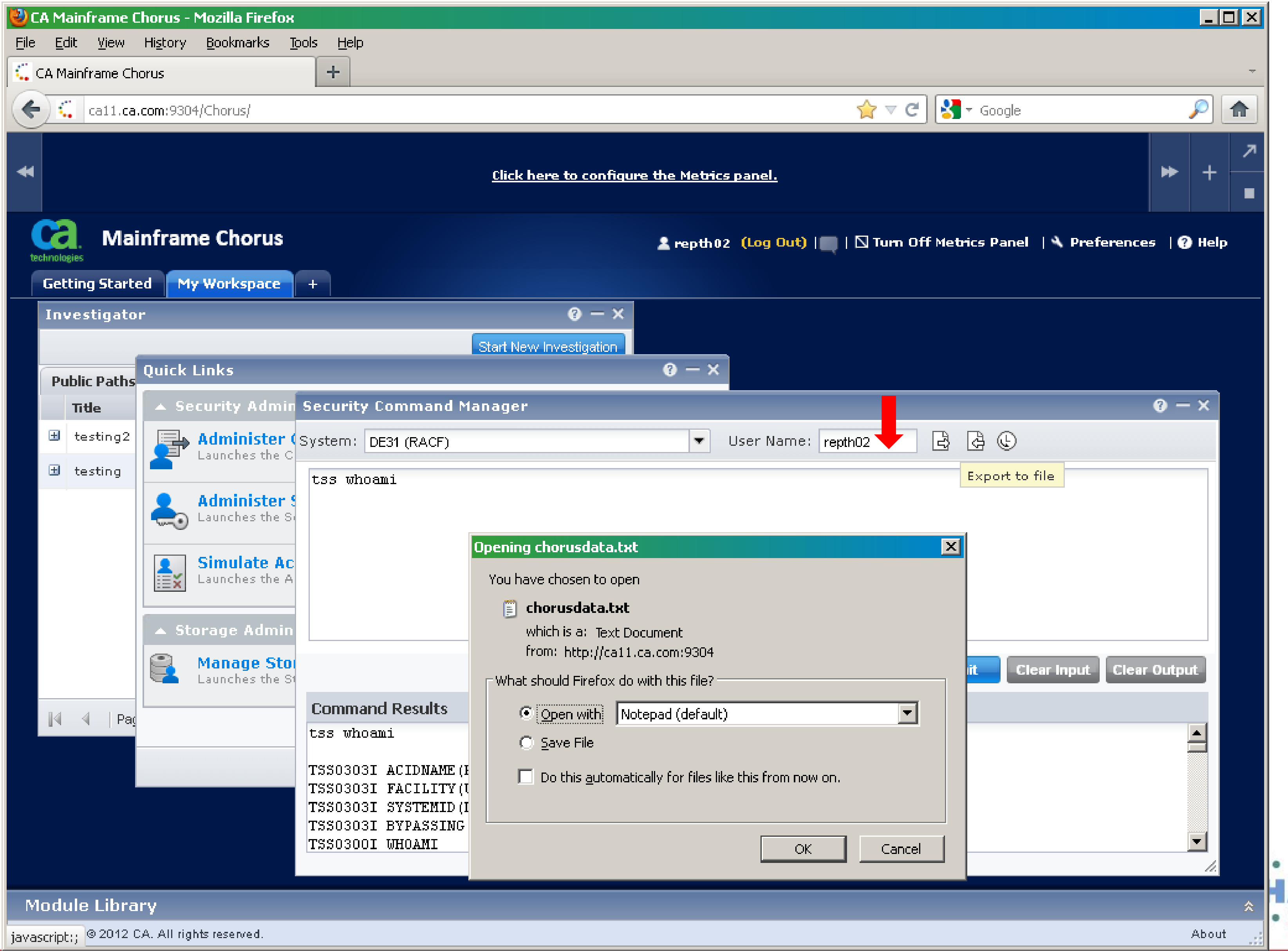
Displaying 1 - 10 of many

Details

http://ca11.ca.com:9304/Chorus/chorusR2.html?id=12345678&locale=en#

About

Export from Security Command Manager



System: DE31 (RACF)

User Name: repth02

```
tss whoami
```

Command Results

```
tss whoami

TSS0303I ACIDNAME(I
TSS0303I FACILITY(U
TSS0303I SYSTEMID(I
TSS0303I BYPASSING
TSS0300I WHOAMI
```

Opening chorusdata.txt

You have chosen to open

chorusdata.txt

which is a: Text Document

from: http://ca11.ca.com:9304

What should Firefox do with this file?

● Open with Notepad (default)

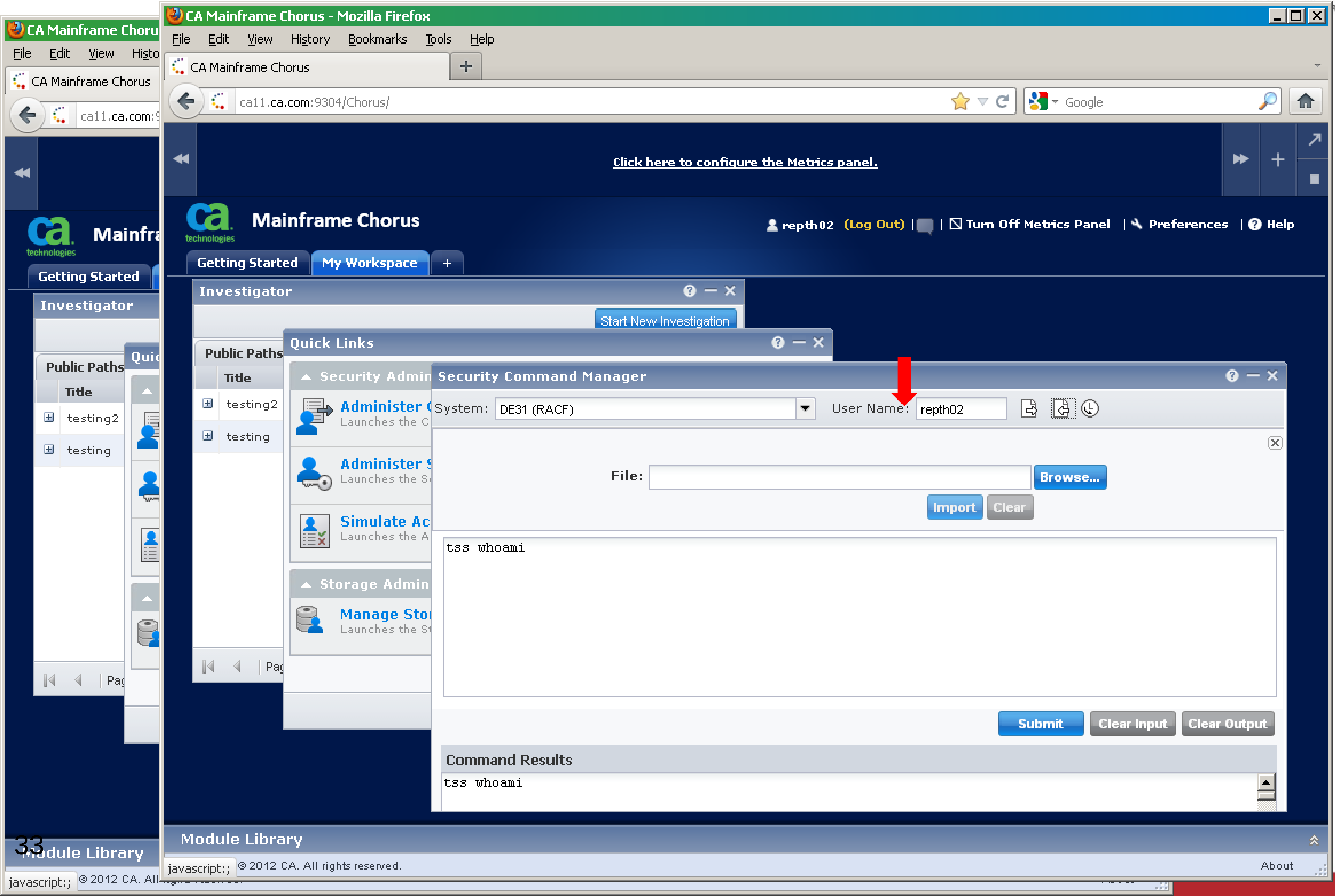
○ Save File

□ Do this automatically for files like this from now on.

OK Cancel

© 2012 CA. All rights reserved.

Import Into Security Command Manager



System: DE31 (RACF)

User Name: repth02

File:

```
tss whoami
```

Command Results

```
tss whoami
```

Hidden Gems:

CA ACF2 for z/OS &
CA Top Secret for z/OS

Compliance Information Analysis (CIA)

- Compliance Information Analysis
  - Common Regulatory Requirements
    - Security Policy: Definition, Assessment, Enforcement, and Remediation of Security incidents
    - Auditing and Reporting, Periodic reviews, and Independent reviews
  - What it provides?
    - Provides flexible compliance reports
    - Aids and supports ad-hoc queries to the security policy
    - Alleviates impact to Security Database
    - Provide information from multiple images
    - Data unloaded into a DB2 Relational Database or CA Datacom/AD
    - Supply distributed reports, sample SQL Ad-hoc reports

Data Classification

- Data Classification / Resource Ownership
  - Provides a way to group resources based on defined requirements (SOX, HIPAA, GLBA, site defined, etc)
    - Define as many Classification records as necessary
    - Assign resources within the Data Classification record
    - Resources can be overlapped in multiple classifications
  - New ACF2 DCO set of Records
  - New parameter on ACF2 reports for independent classification
  - New *DATACLS record for Top Secret
  - Available in Compliance Information Analysis (CIA) for both ACF2 and Top Secret

LDS (LDAP Directory Services)

- CA LDAP Server is a great way of integrating other applications and platforms with ACF2 & Top Secret on the mainframe. Can I sync ACF2 & Top Secret user information with other LDAP based directories?
    - Yes you can!
- LDS stands for LDAP Directory Services and is similar in nature to Command Propagation Facility (CPF)
- ACF2 & Top Secret have the ability to configure user changes to be sent via the LDAP protocol to any URL
- A feature of the base ACF2 & Top Secret - configure and start it up
- Configure at the operation level (CREATE, MODIFY, DELETE) and by individual field
- ACF2 & Top Secret r12 added the ability to change passwords in Microsoft Active Directory (AD)

Distributed Security Integrator (DSI)

- New Certificate Distribution API’s
  - Ideal when administering digital certificates from one central location to multiple systems
  - Configure API to ‘administer’ Certificates from Distributed Application through Distributed Security Integrator (DSI)
  - DSI can now:
    - NewRing – create a new KeyRing
    - PurgeRing – remove all certificates from an existing KeyRing
    - DataPut – add a certificate to the Security database and connect it to a KeyRing
    - DataRemove – remove a certificate from a KeyRing and delete it from the Security DB
    - DelRing – delete a KeyRing

Certificate Utility

- SAFCRRPT
  - Ability to list information about certificates defined in the security sub-system
- Display features:
  - List of expiring certificates
  - List of expired certificates
  - List of certificates by key ring
  - Identifies signer of certificate
- Input parameters:
  - Detail, Summary, Dump, EXT, Ringname, Trust, ICSF, PCICC,EDAYS, RSA, DSA

Statistics

- Statistical Analysis (ACFRPTSG / TSSRPTSG)
  - New STATS Control Options
    - Stats record controls which statistical records are to be cut
      - *ALL, CACHE, CPF, RACROUTE, SYSPLEX*
      - *Statistics will be accumulate for all types*
    - Stats Log controls where cut records are to be logged
      - *SMF or MVS dataset (SEQ,PDS,etc)*

```
SYS1 / OPTS    LAST CHANGED BY ADMIN ON 02/16/07-12:28
               ACCESS BLPLOG CACHE CONSOLE(ROLL) CPF DATE(MDY) NODDB
               NOLDS MAXVIO(10) STATSRECD(CACHE CPF RACROUTE)
               STATSLOG(SYS1.ACF2.STATS) STC NOSYSPLEX
```

```
TSS MODIFY(STATUS(STATG))
  STATG(ON) STATGINT(15)
STATREC(CACHE,RACROUTE,SYSPLEX,COMMAND,WORKLOAD,IOSTATS)
   STATSLOG(SYS1.TSS.STATS)
```

Open Discussion – Q&A

Thank you!

Session #13649

Visit www.SHARE-SEC.com
for more information on
the SHARE Security &
Compliance Project

Disclaimer

Certain information in this presentation may outline CA's general product direction. This presentation shall not serve to (i) affect the rights and/or obligations of CA or its licensees under any existing or future license agreement or services agreement relating to any CA software product; or (ii) amend any product documentation or specifications for any CA software product. This presentation is based on current information and resource allocations as of August 13, 2013 and **is subject to change or withdrawal by CA at any time without notice**. **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 may make such release available to new licensees in the form of a regularly scheduled major product release. Such release may be made available to licensees of the product who are active subscribers to CA maintenance and support, on a when and if-available basis. The information in this presentation is not deemed to be incorporated into any contract.

*CA does not provide legal advice. Neither this document nor any CA software product referenced herein shall serve as a substitute for your compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, policy, standard, guideline, measure, requirement, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. You should consult with competent legal counsel regarding any Laws referenced herein.

THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY. CA assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. **In n**o event will CA be liable for any loss or damage, direct or indirect, in connection with this presentation, 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.