

CA Mainframe Security Update and Hidden Gems

Carla A. Flores



Session # 11585

August 7, 2012 – 1:30pm



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

Session Evaluations

- QR codes



- Online for up to 72 hours after the session
 - www.SHARE.org/AnaheimEval
- Paper forms will also be available for all sessions (***last SHARE for paper evaluations***)

Voting SHARE

- Our own Jerry Seefeldt from NewEra Software



Legal notice

© Copyright CA 2012. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. No unauthorized use, copying or distribution permitted.

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 no 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 of the possibility of such damages.

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 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 may make such release available (i) for sale to new licensees of such product; and (ii) 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.

Agenda

- CA Mainframe Security Release Status
- CA Mainframe Security What's New
- CA ACF2™ for z/OS & CA Top Secret® for z/OS r15 update
- Hidden Gems
- Open Discussion/Questions

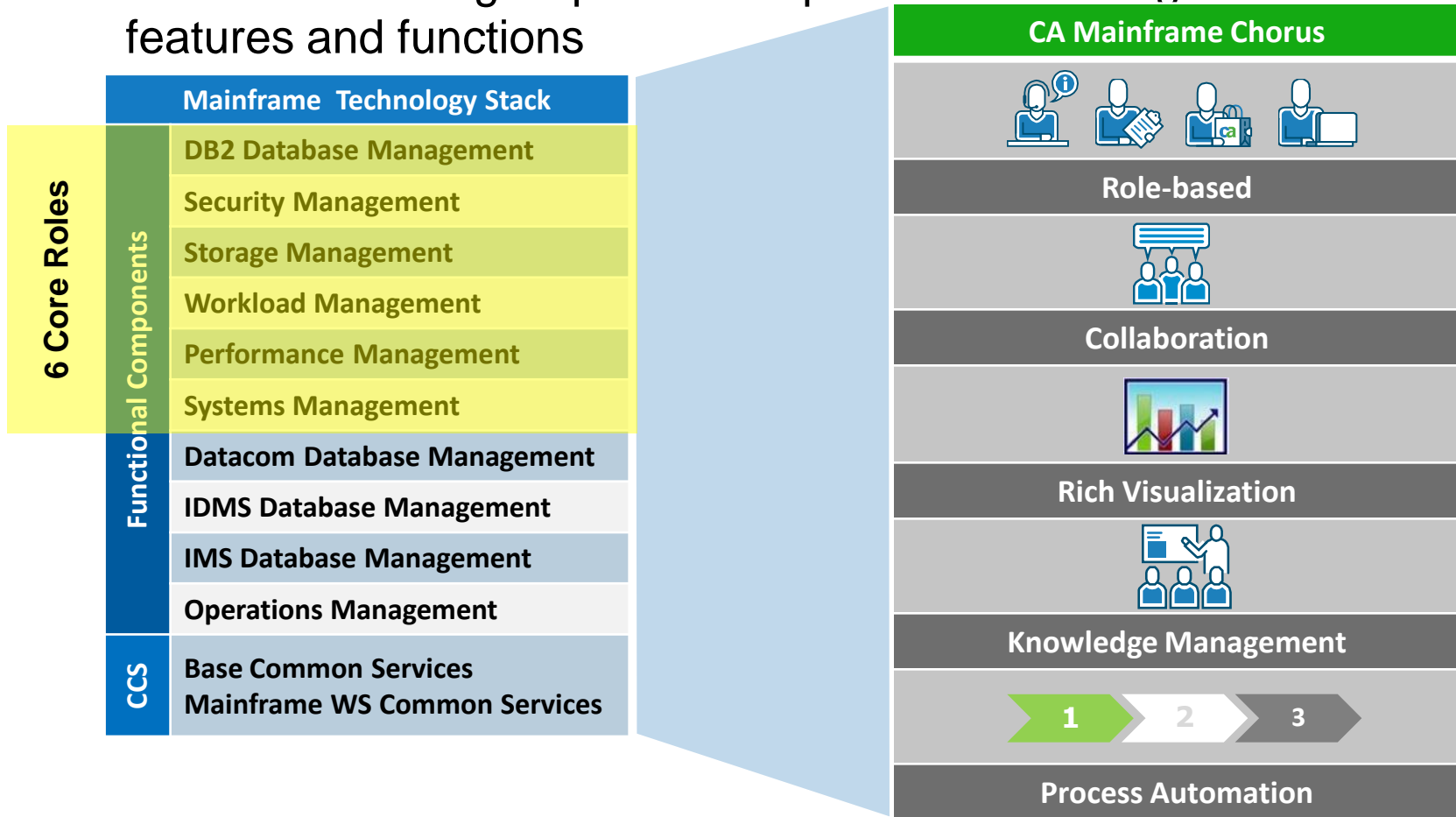
Note: Specific examples of some features are in an Appendix section at the end of this presentation

Release status – new dates

- CA ACF2 / CA Top Secret for z/OS r12 – **End of Service 3/1/2011**
- CA ACF2 / CA Top Secret for z/VM r12 **sp3** – 01/2012
- CA Compliance Manager **r2** – 11/2011
- CA Mainframe Chorus for Security and Compliance Management **r2.5** – 06/2012
- EAL4+ Certification
- <http://www.ca.com/us/Support/mainframe-compatibilites/z196-Compatibility-Matrix.aspx>

What is CA Mainframe Chorus?


- Object-oriented workspace, with a new role-based interaction model that incorporates rich features and data visualization and leverages the CA Technologies portfolio of products as a single bank of features and functions



CA Mainframe Chorus

DE29 IO STATS
DE29 RACROUTE
DE30 RACROUTE

IO Stat
IO Stat
IO Stat
IO Stat
IO Stat
RACROUT
RACROUT
RACROUT
RACROUT
RACROUT
RACROUT
RACROUT

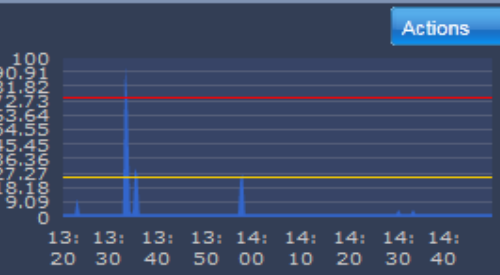


Mainframe Chorus

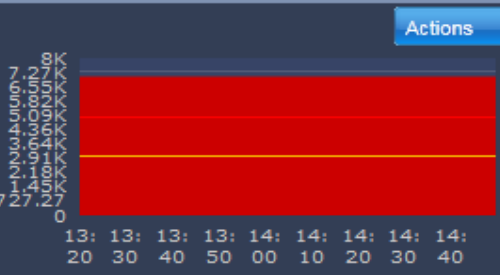
coltr05 (Log Out) |
 [Turn Off Metrics Panel](#) |
 [Preferences](#) |
 [Help](#)

Getting Started
Security
DB2 Performance
DB2 Admin
Storage
SYS Perf
Workload

DE29 Racroute : RACROUTE ...



DE29 SECCACHE : SECCACHE ...



Alerts

Delete |
 New Alerts |
 All |

<input type="checkbox"/>	S...	Time	ID	E...	M...	S...	U...
<input type="checkbox"/>	5	2010-11-17 13:20	105	Logout	User user:	ca31	user04
<input type="checkbox"/>	5	2010-11-17 13:30	115	Logout	User user:	ca31	user01
<input type="checkbox"/>	5	2010-11-17 13:40	120	Logout	User user:	ca31	user13
<input type="checkbox"/>	4	2010-11-17 13:27	102	Access	User user:	ca11	user02
<input type="checkbox"/>	4	2010-11-17 13:27	112	Access	User user:	ca11	user07
<input type="checkbox"/>	4	2010-11-17 13:27	117	Access	User user:	ca11	user12
<input type="checkbox"/>	3	2010-11-17 13:27	101	Logon	User user:	ca11	user01
<input type="checkbox"/>	3	2010-11-17 13:27	104	Logon	User user:	ca31	user04

Page 1 of 2 | Displaying 1 - 10 of 15

Notes

Public Notes | Private 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

Start New Investigation

Public Paths | Private Paths

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

Design goals and architecture

- Enable the converging workforce
- Provide shortened on ramp for less experienced users
- Increase productivity for experienced users

	<i>Knowledge Center</i>	<i>Investigator</i>	<i>Metrics Panel</i>	<i>Security Command Manager</i>	<i>Quick Links</i>	<i>Notes</i>	<i>Security Alerts</i>
ACF2 and Top Secret							
CIA database	x	x				x	
Admin	x				x		
Security command line*	x			x			
ACFTTEST/TSSSIM	x				x		
Statg	x	x	x				
Compliance Manager							
Policy*	x				x		
Events*	x	x				x	
Alerts*	x						x

* Includes support for RACF

CA Compliance Manager 2.0 features ease of use

Administration

- CA31 Compliance Manager Shared Policy
 - Policy Administration
 - Actions
 - DSN Lists
 - Policy Set
 - Policy Statement
 - Create a Policy Statement
 - Modify a Policy Statement
 - Delete a Policy Statement
 - Configuration
 - Policy Disclosure
 - Event Reports
 - Summary Reports
 - Change Approvals
 - Node Information

- Data Classification support
- DSN lists for event policy
- Multiple events in a single policy statement
- CONTAINS operator in event policy

Create a Policy Statement

Policy Statement

Type • Description

Events

Available Events	Selected Events
<ul style="list-style-type: none"> Security System Start Security System Stop Security System Stop Violation Security System Modify Security System Modify Violation Successful Signon 	

Test Conditions

Maximum of 10 test conditions per Policy Statement. NOTE: All time values will be converted to UTC.

Test Conditions

Field	Operator	Value
Date	=	09/23/2011

Actions

Email WTO Service Desk Chorus Alert

Email actions Attached

Email actions currently attached to policy statement.

Actions

From	To	CC	BCC	Subject

CA Compliance Manager 2.0 features ease of use

- Summary Reports
- Change Approvals
- Node Information

Test Conditions

Field	Operator	Value
Date	=	09/23/2011

Actions

Email | WTO | Service Desk | Chorus Alert

Email actions Attached

Email actions currently attached to policy statement.

Actions

From	To	CC	BCC	Subject

Logger Actions

Include
Include/Exclude Exclude
 Not Applicable

Data Warehouse Actions

Include
Include/Exclude Exclude
 Not Applicable

Data Mart Actions

Include
Include/Exclude Exclude
 Not Applicable

- Policy statements for multiple components
- SDATE and EDATE relative to TODAY
- Chorus Alerts

CA Compliance Manager 2.0 features

CA Mainframe Chorus integration

The screenshot displays the CA Mainframe Chorus interface with several key components:

- Top Navigation:** Includes the CA Technologies logo, the text "Mainframe Chorus", and user information for "lufda02" with options for "Log Out", "Turn Off Metrics Panel", "Preferences", and "Help".
- Notes Panel:** A sidebar on the left for managing notes, with tabs for "Public Notes" and "Private Notes". It includes a search bar and a table of notes.
- Security Alerts Panel:** A central panel displaying a table of alerts. A red box highlights the word "Alerts" over the table.
- Security Command Manager Panel:** A panel at the bottom right for executing commands. It shows the system "DE29 (TSS) (CA Top Secret-15.0 150SP0AK003)" and user "lufda02". The command "tss list" is entered and executed, resulting in the message: "TSS0202E YOU ARE NOT AUTHORIZED TO USE THE TSS COMMAND".
- Investigator Panel:** A panel at the bottom left for event analysis. A red box highlights the text "Event analysis" over the panel's content.

Seve...	Time	Message	System	UserId
1	Wed, Sep 07, 2011	DE30 OBJECTACCESS Alert test	DE30	SYSVIEW
1	Wed, Sep 07, 2011	DE30 OBJECTACCESS Alert test	DE30	SYSVIEW
1	Wed, Sep 07, 2011	DE30 OBJECTACCESS Alert test	DE30	SYSVIEW
1	Wed, Sep 07, 2011	DE30 SIGNON Alert test	DE30	HOGWA01
1	Wed, Sep 07, 2011	DE30 SIGNOFF Alert test	DE30	HOGWA01
1	Wed, Sep 07, 2011	DE30 SIGNON Alert test	DE30	HOGWA01
1	Wed, Sep 07, 2011	DE30 SIGNON Alert test	DE30	DEFAULTU

TITLE	MODIFIED	AUTHOR
15344 Path	Wed Sep 07 03:38:25	yasra01

CA Mainframe Chorus New Features in r2.5

Investigator cross-role actions (Storage to Security shown)

The screenshot shows the Investigator application interface. The main window displays a table titled "Datasets not used last year SMD and MOTM". The table has columns for Notes, Nodes, Count, Pct, and TOTA-Trks. The "Nodes" column is highlighted, and the row for "ADKST01" is selected. The "Actions" sidebar on the right contains a search bar and a "Navigation" section with three links: "Add to Visualizer", "Show users of selected dataset", and "Show violation on selected data". Two red arrows point to the "Show users of selected dataset" and "Show violation on selected data" links.

Notes	Nodes	Count	Pct	TOTA-Trks
	ABEBR01	2	0	3
	ADKST01	1	0	2
	AD1DEV	1	0	1
	ALMVI02	1	0	2
	ASM	8	0	10
	ASMDSK	5	0	7
	ASMQADAL	85	0	143
	ASMTAP	70	0	86
	ASTX280	640	0	1439
	ATTE001	0	0	11

Details for Datasets not used last year SMD and MOTM (ADKST01)

Datasets not used last year SMD and MOTM Information

Nodes	ADKST01	Count	1
Pct	0	TOTA-Trks	2
TOTI-Trks	0	SysplexVan	PLEXC1
LparVan	CA11	SubsystemVan	QCV6

Copyright © 2012 CA. All rights reserved. About

Paths and their descriptions are now searchable

The screenshot displays the CA Mainframe Chorus interface, which is a web-based management tool. The main window shows a search for 'SMS Management Class DBA' with 88 matches found. The search results are displayed in a table with columns for 'Notes', 'MC-Name', 'Last Mod Uid', 'Last Mod Dt', and 'Last Mod'. The table lists several entries, including 'CUT', 'DBA', 'DBB', 'DBMIG', 'DBPERM', and 'DBPROD'. The 'DBA' entry is highlighted. The interface also includes a navigation pane on the left with categories like 'Storage Engine Information', 'All Storage Solutions', and 'Allocation Control'. A 'Module Library' is visible at the bottom left, and a 'Details for SMS-MC (Management Class) (DBA)' section is at the bottom right.

CA Mainframe Chorus - Microsoft Internet Explorer provided by CA

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

Click here to configure the Metrics panel.

CA Knowledge Center - Microsoft Internet Explorer provided by CA

Knowledge Center

SMS Management [Advanced Search](#)

Total 88 matches found

[Path:SMS Management Class DBA](#)
Storage > DFSMS Constructs > SMS-MC (Management Class) MC-Name DBA

[Standards and data](#)

[Transit organization](#)

[MGMTC Management class. T](#)

Investigator - Microsoft Internet Explorer provided by CA

File Edit View Favorites Tools Help

SMS Management Class DBA

Storage > DFSMS Constructs > SMS-MC (Management Class) MC-Name DBA

Storage > DFSMS Constructs >

Enter a search keyword

Notes	MC-Name	Last Mod Uid	Last Mod Dt	Last Mod
	CUT	DOWTI01	2002/11/15	10:38
	DBA	BEHMA01	1999/12/11	02:02
	DBB	MCPJA01	2003/04/15	17:18
	DBMIG	BEHMA01	2000/07/24	14:01
	DBPERM	DOWTI01	2003/03/26	16:57
	DBPROD	DOWTI01	2004/11/01	13:51

Additional

- CA Main
- CA Data
- CA ACF
- CA Top
- CA Vant

Copyright © 2012 CA. All rights reserved.

Module Library

Copyright © 2012 CA. All rights reserved.

Done

Storage > DFSMS Constructs >

Enter a search keyword

Administrative Actions

- Send Chorus Alert

Navigation

- Add to Visualizer
- Show Data Sets For System (All)

Details for SMS-MC (Management Class) (DBA)

Page 1 of 1

Displaying 1 - 100 of 100

Alerts Module

Severity Count summary and Hide-able filter

CA Mainframe Chorus - Microsoft Internet Explorer provided by CA

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

File Edit View Favorites Tools Help

CA Mainframe Chorus

Click here to configure the Metrics panel.

ca Mainframe Chorus technologies

repth02 (Log Out) Turn Off Metrics Panel Preferences Help

Getting Started My Workspace +

Security Alerts

1 2 0 3 4 0 4 0 5 2

All Enter Search Keyword... Search Reset

Message	Severity	Time
limittest1	1	Sat, Apr 24, 2010 03:42:08 PM
limittesting6	1	Sat, Apr 24, 2010 03:42:08 PM
limittesting2	3	Thu, Nov 25, 2010 01:32:08 PM
limittesting3	3	Wed, Feb 23, 2011 04:44:14 AM
limittesting7	3	Thu, Nov 25, 2010 02:42:08 PM
limittesting8	3	Wed, Feb 23, 2011 04:44:14 AM

Module Library

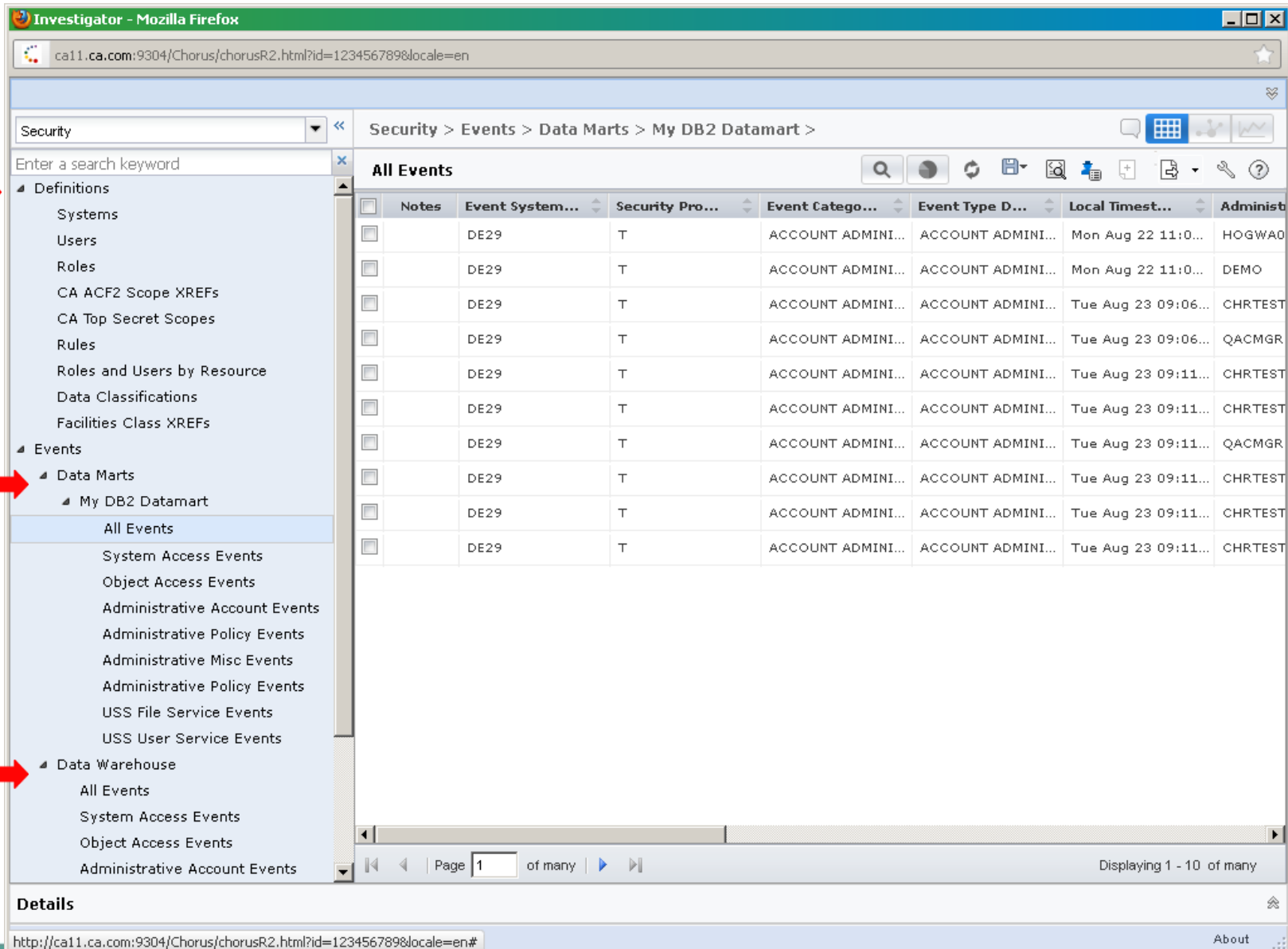
Copyright © 2012 CA. All rights reserved. About

Done Local intranet 100%

CA Mainframe Chorus

Security and Compliance Role Improvements in 2.5

Datacom CIA, Data mart(s), and Warehouse



Investigator - Mozilla Firefox
ca11.ca.com:9304/Chorus/chorusR2.html?id=123456789&locale=en

Security > Events > Data Marts > My DB2 Datamart >

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

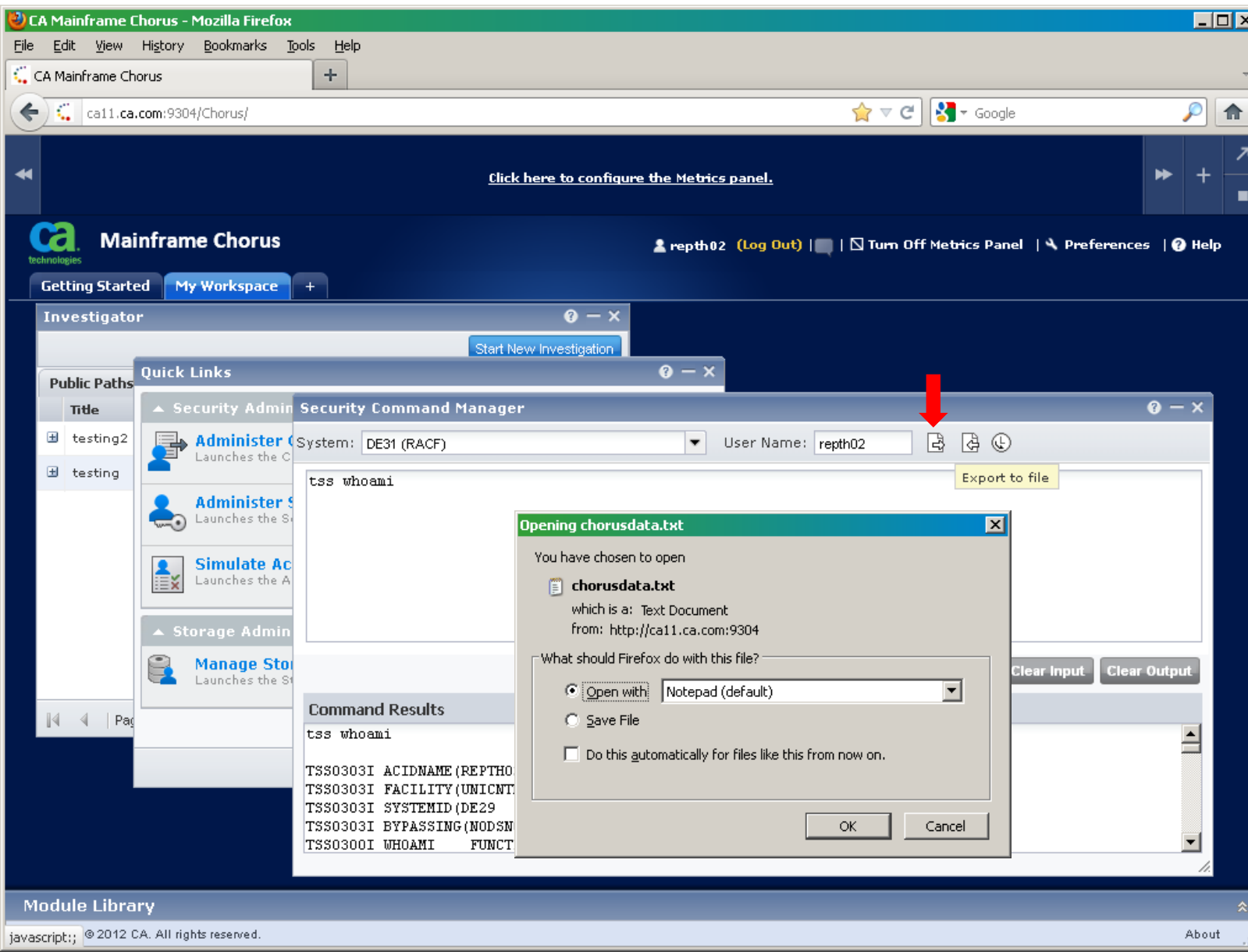
Notes	Event System...	Security Pro...	Event Catego...	Event Type D...	Local Timest...	Administ
	DE29	T	ACCOUNT ADMINI...	ACCOUNT ADMINI...	Mon Aug 22 11:0...	HOGWA0
	DE29	T	ACCOUNT ADMINI...	ACCOUNT ADMINI...	Mon Aug 22 11:0...	DEMO
	DE29	T	ACCOUNT ADMINI...	ACCOUNT ADMINI...	Tue Aug 23 09:06...	CHRTEST
	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=123456789&locale=en#

Export from Security Command Manager



CA Mainframe Chorus - Mozilla Firefox

File Edit View History Bookmarks Tools Help

CA Mainframe Chorus

ca11.ca.com:9304/Chorus/

Click here to configure the Metrics panel.

Mainframe Chorus

repth02 (Log Out) Turn Off Metrics Panel Preferences Help

Getting Started My Workspace

Investigator

Quick Links

Public Paths

Security Admin Security Command Manager

System: DE31 (RACF) User Name: repth02

tss whoami

Export to file

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

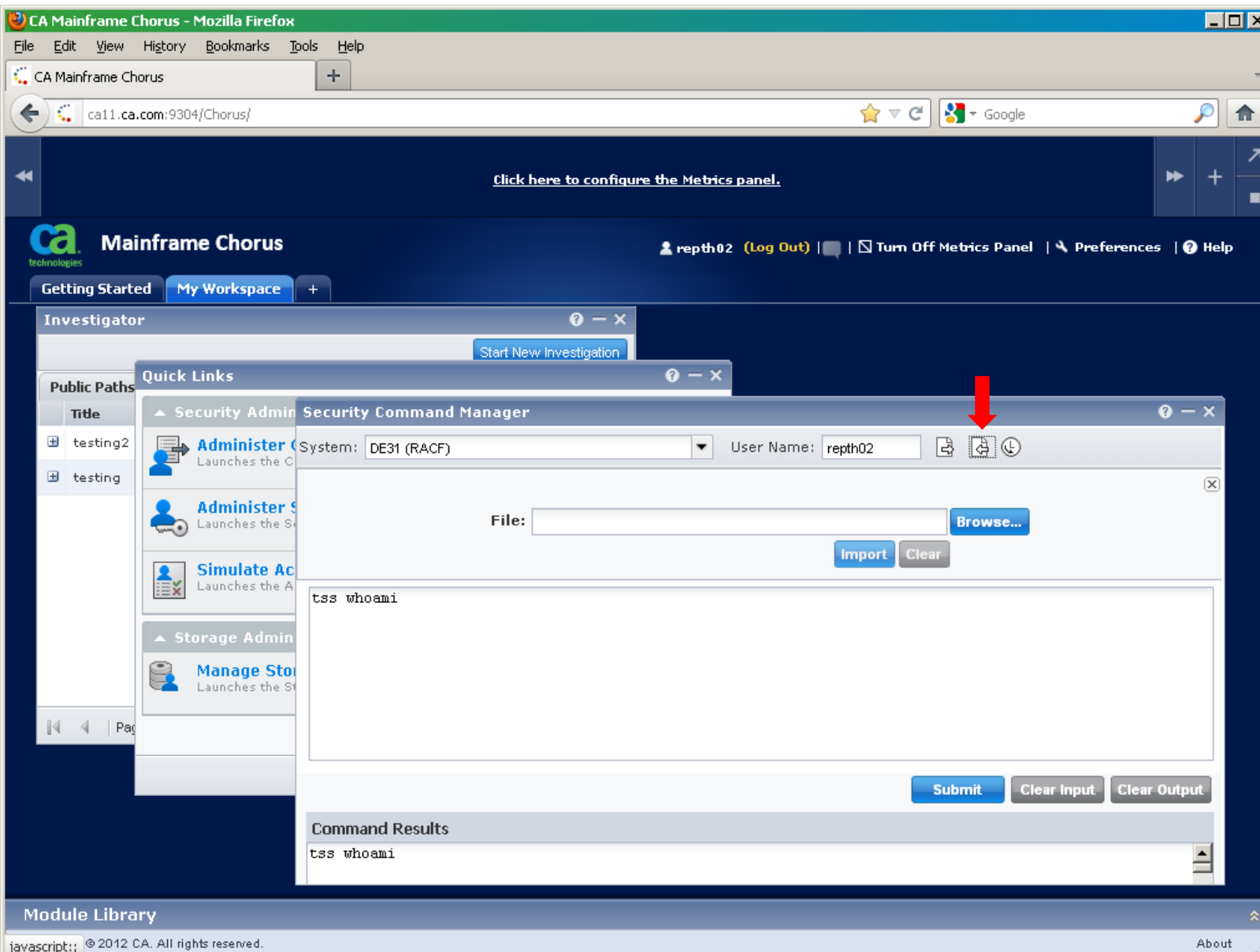
Do this automatically for files like this from now on.

OK Cancel

Command Results

```
tss whoami
TSS0303I ACIDNAME (REPTH0
TSS0303I FACILITY (UNICNT
TSS0303I SYSTEMID (DE29
TSS0303I BYPASSING (NODSN
TSS0300I WHOAMI FUNCT
```

Import Into Security Command Manager



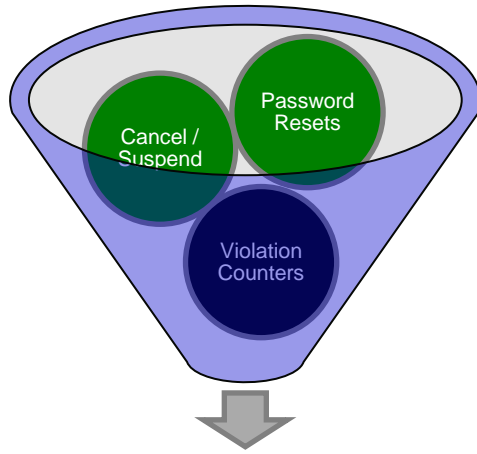
The screenshot shows the Mainframe Chorus web application interface. At the top, there is a navigation bar with the CA logo and the text "Mainframe Chorus". Below this, there are tabs for "Getting Started" and "My Workspace". The main content area is divided into several sections:

- Investigator**: A section with a "Start New Investigation" button.
- Quick Links**: A sidebar with several links, including "Security Admin" (highlighted), "Storage Admin", and "Manage Storage".
- Security Command Manager**: A central window with a "System" dropdown set to "DE31 (RACF)" and a "User Name" field set to "repth02". It features a "File:" input field with a "Browse..." button, and "Import" and "Clear" buttons. Below this is a text area containing the command "tss whoami". At the bottom of this window are "Submit", "Clear Input", and "Clear Output" buttons.
- Command Results**: A section at the bottom of the Security Command Manager window showing the output of the command: "tss whoami".

A red arrow points to the "Import" button in the Security Command Manager window.

CA ACF2 & CA Top Secret r15

Restricted administration controls



You can now control administration capabilities without high-level privileges being given (ie. Security, Account, Audit, MSCA, SCA, etc.)

- Initial target:
 - Passwords and password related fields
 - Administration of certificate commands
- New pre-defined resource class: CASECAUT
 - Internal CLASSMAP record with TYPE=AUT (CA ACF2)
 - NORESCHK not honored for CASECAUT class (CA Top Secret)
- Provide administration access through resource authorization
 - Cannot perform Administration on a higher-level user

Restricted administration controls (CA Top Secret)



- Allows a user other than MSCA to run TSSXTEND and TSSFAR
- Allows a user with no admin authorities to run utilities

New administration commands

- **User Comparison**
- **User Modeling**
- **User Archival**



Automated user comparison (CA ACF2)

- New ACF COMPARE command
 - Single command compares two users and displays differences
 - Compares logonids
 - Compares associated roles
 - Compares user profile segments
 - *CICS, EIM, LANGUAGE, NETVIEW, OPERPARM, SECLABEL, WORKATTR*
 - Syntax: COMPARE userid1 USING(userid2)
- Requirements
 - User must have SECURITY or AUDIT privileges
 - Logonids being compared must be within administrator's scope

Automated user modeling (CA ACF2)

- New ACF MODEL command
 - Copies subset of logonid fields, profiles, and roles from existing user
 - Builds commands to insert new user modeling existing user
 - Syntax: MODEL logonid(newuser) USING(modelid) INTO('pds(member)')
 - If INTO not specified, command output displayed to terminal
 - Administrators can MODEL any logonids within their scope

Automated user archiving (CA ACF2)

- NEW ACF2 ARCHIVE subcommand for LIST and DELETE commands
 - Builds ACF commands that recreate a user (Logonid and User Profiles)
 - Re-adds user to roles they were previously assigned to
 - Syntax: {LIST | DELETE} logonid ARCHIVE INTO('output.work.user(member)')
 - *If INTO not specified, command output displayed to terminal*
 - *Administrators can ARCHIVE any logonid within their scope*

Compare command enhancements (CA Top Secret)

- Description
 - New TSS COMPARE(ACID) USING(ACID) command will compare the two ACIDS and then display the differences to the screen.
- This command is treated like a list command
 - Administrators must have explicit authority via the ADMIN - DATA command
 - The compare command will only display output for the ACIDS within their scope

Administration user modeling (CA Top Secret)

- Description
 - MODEL command
 - Models permissions for datasets/resources from existing user acid to another user acid
 - Generates list of TSS commands
 - First record in output is comment, which contains:
 - *Command*
 - *User acid being modeled*
 - *Date and time of model*
 - *TSS administrator who issued command*
 - *System on which command was executed*
 - *User acid used as a model*

Administration archival (CA Top Secret)

- Description

- Archival allows user's permissions and resources to be archived into form of TSS commands
- Generated TSS commands can be stored in PDS dataset and used to restore a user
- First record in output is a comment, which contains:
 - Command
 - User acid being modeled
 - Date and time of the archive
 - TSS administrator who issued command
 - System on which command was executed



Administration archival (CA Top Secret)



- Requirements
 - Specify ARCHIVE keyword on LIST or DELETE command
 - Administrator must have DATA(ALL) authority and scope over ACID being archived
 - Specify keyword INTO to have TSS commands written out to PDS
 - During archive processing, most of user's security record information is archived, but some fields are not copied during archive process (e.g., digital certificates)
 - Use EXPORT command
 - If user being archived has digital certificates

Certificate enhancements

- **Renew Command**
- **IDN/SDN Extensions**
- **Certificate Utility Enhanced**

Certificate RENEW command (CA ACF2)

- Renews digital certificate with one command
 - Provide certificate and new 'expire' date
 - Eases the administration from up to a six step process to one
 - Syntax: RENEW user.cert EXPIRE(12/31/11)
SIGNWITH(my.ca)
- Requirements
 - Certificate & Signer of cert being renewed must have private key in CA ACF2 Info-Storage database or in ICSF (PKDS)



Certificate DN support (CA ACF2)

- Distinguished Name (DN) max sizes increased to accommodate larger CA certificate SDNs/IDNs
- GSO CERTMAP fields SDNFILTR and IDNFILTR increased to allow larger values up to 1024 bytes
- Notes:
 - Do not share INFOSTG database between systems without support
 - Specify SDNSIZE(1024) to activate large DN support only after ALL systems sharing INFOSTG have been upgraded

Certificate enhancements (CA ACF2)

- Expanded Key Ring Support
 - Limitation due to size of INFO-STORAGE Database
 - New User parameter on CONNECT or REMOVE “logically” connects or removes ALL certificates from a user keyring
- Password Prompt
 - Prompt for password if missing from CHKCERT, INSERT, or EXPORT command
- Expiring Certificate Warning
 - New GSO OPTS CERTEXP(days)
 - ACF79468 Certificate xxx.yyy is expiring in xx days



Certificate RENEW command (CA Top Secret)



- Renews digital certificate with one command
 - Provide certificate and new 'expire' date
 - Eases the administration from up to a six step process to one
 - Syntax: `TSS RENEW(JOE1) DIGICERT(cert1)
NADATE(12/31/10)`
- Requirements
 - Certificate being renewed must have private key in CA Top Secret database or in ICSF
 - Signer of certificate being renewed must have private key in CA Top Secret database or in ICSF

Large DN support (CA Top Secret)

Requirements

- New maximum DN size is 1024 for Subject DN, 1007 for Issuer DN
- SDNFILTR and IDNFILTR have also been increased
- Large DN feature is incompatible with operating systems that do not have the support
- Sharing a security file between incompatible systems is not supported
- New SDNSIZE(255|1024) parameter will allow migration of all systems to the new support before allowing certificates with large DNs to be inserted or gencerted

Certificate utility enhanced (CA ACF2 & CA Top Secret)

- New fields displayed in Utility output

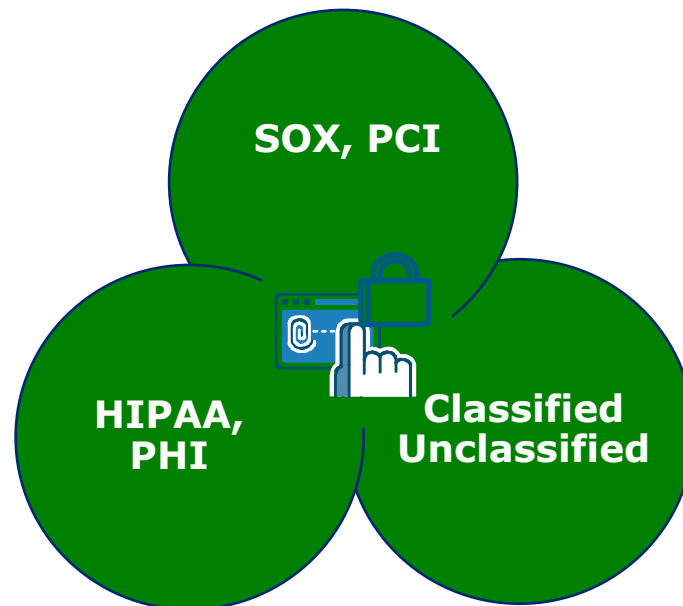
Field	Field Value Description
Algorithm	Signing algorithm
Trusted	Trust status (Yes or No)
Cert Length	Certificate length
Extensions	Contents of certificate extensions (Hex dump, if not common)

- New Totals displayed in Utility output

Totals Field	Totals Field Value Description
Trusted Certificates	Total number of trusted certificates
High Trust Certificates	Total number of high trusted certificates

Data classification enhancement

- Data Classification Enhancement
 - Add Data Classification and Ownerships to CA Compliance Manager Event Records and CA Mainframe Chorus for Security and Compliance Management



CA ACF2™ for z/OS Only

Role based security

- ACFXREF Utility changed to include XROL records
 - Manipulates Cross-reference XROL records and identifies invalid values on INCLUDE and EXCLUDE statements
 - Facilitates removal or restoration of roles and users that no longer exist from role definitions
- New output CMDS and BACKOUT files
 - Valid for all ACFXREF processing types (XROL, XSGP, XRGP)
 - CMDS output file
 - BACKOUT output file



Auto erase enhancements

- Erase-on-Scratch (EOS) support
- “Existing” method (ACF2 intercepts-based)
 - Erase processing done out of ACF2 ERASE intercepts
 - If using existing EOS method, ACF2 does the manual scratching
- “New” method (SAF-based)
 - Controlled by GSO AUTOERAS record – new PROCESS(SAF|ACF2)
 - Better control for user
 - Can control EOS centrally against all data sets via AUTOERAS record - at individual HLQ level & SECLEVEL for data classification records

TSO options

- New BYPPAUSE field
 - Bypasses CA ACF2 message prompt and pause during TSO SIGNON
 - Limits display of CA ACF2 informational messages during TSO logon
 - Incorporation of User Mod UM75289
 - Requirement: Must use CA ACF2 TSO Logon Routine
- New LOGHERE field
 - Allows TSO/E user who has a session on one terminal to log on to another terminal with the RECONNECT option and "steal" the session from the original terminal
 - Requirement: Must be at z/OS 1.11 or above

Misc enhancements

- DSERV Exit Support
 - PDSE support for PDS Member Level Protection and Program Pathing
- SHOW RSRCTYPE
 - Incorporated in Show All output

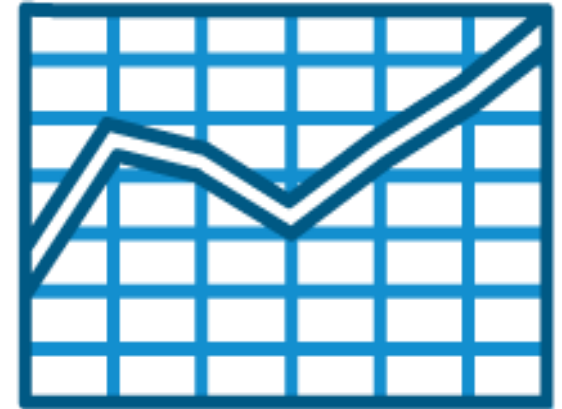
CA Top Secret® for z/OS Only

Virtual storage constraint relief (VSCR)

- Use of 64-bit storage above the bar

Auto Start

- Support auto starting TSS as Subsystem
- Requirements
 - Support START/NOSTART in CAISECxx parmlib member
 - Allow control options overrides via CAITSSxx
 - Set subsystem name via SUBSYS= keyword
 - VERIFY issued by AXR is suspended by TSSSFR00
-



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

CA LDAP Server

- Used to integrate to ACF2 & Top Secret by CA and other vendor software
- Some examples other software:
 - CA Identity Manager r12
 - IBM WebSphere
 - User authentication & group authorization
 - Novell eDir via dirXML
 - Clients are using with LDS to perform two way password sync
 - **Any LDAP compliant directory structure**
- No charge component of CA ACF2 & CA Top Secret

LDS

- 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

- SAFCCRPT
 - 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

Linux on System z

- Leverage PAM (Pluggable Authentication Module) to validate AUTHENTICATE from z/OS database
- Configure for round robin support with other LDAP structures for high availability
- Could leverage DSI to AUTHORIZE access to Linux apps
 - Requires a re-write of the app if existing
- Leverage CA Access Control to get more granular level controls on platform

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 (SFQ, 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)

CA ACF2 Only

Role based security

- Role-based Security
 - Usage
 - Easy approach to defining Roles
 - Easy approach of defining users to roles
 - Easy approach of defining what data sets and resources the roles have access to
 - Benefits
 - Simplifies administration of dataset/resource rules
 - Savings on storage usage on rules
 - Easy implementation
 - Create Roles based on business need
 - Ensures defined role has only the access needed to perform role
 - Eases compliance and risk management
 - Auditing and Reporting identifies roles

Commands

- **RECKEY Command Enhanced**
 - Customer requested enhancement to provide additional support for rule sets
 - Pre-r14 only able to ‘add’ or ‘delete’ individual rule lines
 - Enhanced support in r14 for Control Cards (\$ cards,% cards)
 - New MOD sub-command to ‘modify’ existing rule lines
- **ACCESS Command Enhanced**
 - Customers using command for compliancy reporting and accountability
 - Requested addition of Date/Time Stamp for historical purposes; saving output to PDS library
- **RULELONG and COMPDYN Option**

Reporting

- ACFRPTDS: Use MASK or NMASK to limit output
- ACFRPTRX (Run with NOACF2 option)
 - Logonid Access Report showing all rule sets that apply to a specific logonid (LID) mask or user identification string mask
- ACFRPTXR (Run with NOACF2 option)
 - Cross reference report showing access to a specified data set or resource
 - NOUIDALL option to suppress UID(*) reporting
- NEWXREF: X(SGP) Cleanup report
- ACFRPTSL: Modified to leverage current date
 - LSTACCD(nn)

CA Top Secret® for z/OS

Control Option

- **INACTIVE Control Option**
 - Will cause a user to be suspended upon completion of the interval
 - **INACTIVE(0|nnn/LASTUSED)**
 - 0-nnn sets normal inactive processing as functions in prior releases
 - **LASTUSED**
 - *Checks Last Used date and Password change date*
 - *If both are passed INACTIVE setting user suspended*
 - **INACTIVE(5)**
 - User logs on 6 days after password expired, user suspended
 - **INACTIVE(5, LASTUSED)**
 - User logs on 6 days after last time logged on and password was changed 6 days or more ago, user suspended

Utilities

- TSSUTIL
 - New JCL stream to handle sorting of data in date time order
 - New Options
 - EXCLJOB
 - *Use to suppress job names from the report output*
 - EXCLACID
 - *Use to suppress ACID information from the report output*
 - JOBID
 - *Use to run reports based on specific job IDs*
 - PROGRAM
 - *Use to run reports based on specific program names*
- TSSBRWZ: Writes TSS command output to a dataset

Where else can you find info that might help?



- RACF Translation Guides
- Knowledge documents
- Support.ca.com
- Releasing Latent Value Book

Review

- Release Status
- CA ACF2 & CA Top Secret Enhancements
 - Compliancy Considerations
 - Administration Capabilities
 - Performance Enhancements
 - Incorporated DARs
- CA Mainframe Security Products
 - CA Cleanup
 - CA Auditor
 - CA Mainframe Chorus for Security and Compliance Management

Open Discussion – Q&A

Thank you!

Session #11585



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

Appendix

Sample output

CA ACF2 sample health check – expiring certificates

CHECK(CA_ACF2,ACF2_CHECK_EXPIRING_CERTS)
START TIME: 03/15/2010 12:19:07.557056
CHECK DATE: 20100101 CHECK SEVERITY: MEDIUM

CA ACF2 CHECK FOR EXPIRING DIGITAL CERTIFICATES

LIST OF DIGITAL CERTIFICATES EXPIRING WITHIN 30 DAYS

CERTNAME=CERTAUTH.P11BND
CERTNAME=CERTAUTH.P11DEL

* Medium Severity Exception *

ACFHC051E At least one ACF2 Digital Certificate will expire in the next 30 days.

Explanation: There is one or more ACF2 Digital Certificate which will expire in the next 30 days.

System Action: ACF2 continues processing.

Operator Response: Report this problem to the Security Administrator.

System Programmer Response: Have the security administrator review the ACF2 Digital Certificates.

Problem Determination: N/A

Source: ACF2

Reference Documentation: Please refer to chapter Digital Certificate Support in the ACF2 Administrator Guide on the use of Certificates.

CA ACF2 sample – restricted administration controls

. Example: help desk admin

```
ACF75052 RESOURCE RULE ACFCMD STORED BY SECADM01 ON 03/22/10-09:00
```

```
$KEY(ACFCMD) TYPE(AUT) ROLESET
```

```
- USER.PASSWORD ROL(HLPDSK1) ALLOW
```

```
- USER.PASSPHRASE ROL(HLPDSK1) ALLOW
```

```
- USER.- ROL(HLPDSK2) ALLOW
```

```
ACF75051 TOTAL RECORD LENGTH= 236 BYTES, 5 PERCENT UTILIZED
```

```
change user01 password(user01) passphrase(new passphrase)
```

```
ACF6C004 LOGONID USER01 CHANGED
```

```
ACF6D070 PWPHRASE / USER01 RECORD CHANGED
```

```
change secadm password(secadm)
```

```
ACF00103 NOT AUTHORIZED TO CHANGE FIELD PASSWORD
```

CA ACF2 sample - restricted administration controls

- Example: certificate administration
 - Note: User DCADM1 is “unscoped” and can administer all certificate-related objects for any user

```
set r(aut)
RESOURCE
comp * store
ACF70010 ACF COMPILER ENTERED

. $KEY(ACFCMD) TYPE(AUT)
. DIGTCERT.- UID(DCADM1) SERVICE(READ,UPDATE,DELETE) LOG
.
ACF70051 TOTAL RECORD LENGTH= 158 BYTES, 3 PERCENT UTILIZED
ACF60029 RESOURCE ACFCMD STORED
RESOURCE

f acf2,rebuild(aut),c(r)
ACF8A037 DIRECTORY RAUT ADDED TO RESIDENT CHAIN
```

CA ACF2 sample – compare

ACF

Compare JPETERS USING(JSMITH)

LID SECTION

LID	JPETERS	JSMITH
NAME	JAMES PETERS	JOHN SMITH

TSO SECTION

TSOPROC	CATSO	XXTSO
DFT-PFX	PETERS	SMITH

RESTRICTIONS SECTION

PREFIX	PETERS	SMITH
GROUP	DEFGRPA	DEFAULTG

ROLES SECTION

GRUPE	GROUPA
GROUPH	GROUPC

CICS PROFILES

OPCLASS		Y
OPPTY	0	255
TIMEOUT VALUE	0	15

CA ACF2 sample – archive

```
ACF
model logonid(newuser) using(ACFUSER) into('MYPDS.FILE(OUTPUT)')

SET LID
INSERT NEWUSER -
  PASSWORD(NEWUSER) -
  ACCOUNT -
  ACCTPRIV -
  ALLCMDS -
  TSOFSRN -
  GROUP(DEFAULTG)-

SET PROFILE(USER) DIV(CICS)
INSERT NEWUSER -
  OPIDENT(CHI)-
  OPPRTY(255)-
  TIMEOUT(60)-

F ACF2,REBUILD(USR),CLASS(PROFILE)

SET X(ROL)
CHANGE GROUPA -
INCLUDE(NEWUSER)

F ACF2,NEWXREF,TYPE(ROL)
END
```

CA ACF2 sample - archive

```
ACF
delete newuser archive into('mypds.out(listarch)')
```

```
ACF
SET LID
INSERT NEWUSER -
  PASSWORD(NEWUSER) -
  ACCOUNT -
  ACCTPRIV -
  ALLCMDS -
  AUDIT -
  CICS -
  GROUP(DEFAULTG)-
```

```
SET PROFILE(USER) DIV(CICS)
INSERT NEWUSER -
  OPIDENT(CHI)-
  OPPRTY(255)-
  TIMEOUT(60)-
```

```
F ACF2,REBUILD(USR),CLASS(PROFILE)
```

```
SET X(ROL)
CHANGE GROUPA -
INCLUDE(NEWUSER)
CHANGE GROUPC -
INCLUDE(NEWUSER)
F ACF2,NEWXREF,TYPE(ROL)
END
```


CA ACF2 sample - role based security

CA ACF2 - XREF CLEANUP REPORT

DATE 02/24/10 (10.055) TIME 18.32

PAGE 1

RESOURCE(XROL) GROUP SYSID(LONG) RECID - USERGRP

DESCRIPT(USER GROUP ROLE)

LIST OF INCLUDE VALUES:

USER-

LIST OF EXCLUDE VALUES:

PGMR04

PGMR03

PGMRJ02 -- VALUE NOT FOUND

LIST OF VALUES THAT MATCHED MASK: USER-

USER4 USER1

USER3 USERSC

USER2 USERGRP

CA Top Secret sample - restricted administrative authorities

- User DCA01 is allowed to change passwords

```
tss add(sysdept) casecaut(tsscmod.user)
TSS0300I ADD    FUNCTION SUCCESSFUL

tss per(DCA01) casecaut(tsscmod.user.replace.password) access(update)
TSS0300I PERMIT FUNCTION SUCCESSFUL

tss list(DCA01) data(admin)

ACCESSORID = DCA01    NAME    = DCA
----- ADMINISTRATION AUTHORITIES

LIST DATA = BASIC,NAMES

----- RESTRICTED ADMINISTRATION AUTHORITIES

XA CASECAUT= TSSCMD.USER.REPLACE.PASSWORD          OWNER(SYSDEPT )
ACCESS = UPDATE
```

CA Top Secret sample - restricted administrative authorities

- User DCA01 is allowed to run TSSUTIL

```
tss add(sysdept) casecaut(tssutility)
TSS0300I ADD    FUNCTION SUCCESSFUL

tss per(DCA01) casecaut(tssutility.tssutil) access(use)
TSS0300I PERMIT FUNCTION SUCCESSFUL

tss list(DCA01) data(xauth)

ACCESSORID = DCA01   NAME      = DCA
XA CASECAUT= TSSUTILITY.TSSUTIL          OWNER(SYSDEPT )
ACCESS = USE

ADMIN BY= BY(MASTER )  SMFID(XE05) ON(02/18/2010) AT(11:03:38)
```

CA Top Secret sample – compare

TSS COMPARE(CMPACD2) USING(CMPACDB)

```

ACID    CMPACD2          | CMPACDB
DEPTMENT COMPDEP2      | COMPDEPT
DIVISION          | COMPDIVI
ZONE             | COMPZONE
----- Profiles are different or in a different order starting with.
      KRACPROF          |
LANGUAGE          | F
----- SOURCE
      ANOTHER8          |
      CHAR5             |
      C2                |
      FOUR              |
----- OPERCLAS
      02                |
      05                |
      06                |
PHYSKEY          | ADDINGTOACHARACTER
----- DEFNODES
      LA                |
      PHI               |
----- SEGMENT OMVS -----
ASIZE          | 2147483647
  
```

CA Top Secret sample – compare

- Example (TSS COMPARE COMMAND)

```
----- Facility differences for Acid CMPACDB  
FACILITY = MQM  
DAYS = TUE THU SATSUN TIME =ANY  
ACTIONS = FAIL
```

```
----- Permit Differences for ACID CMPACD2  
XA DATASET CMPACD1.WORK  
EXPIRE(04/12/10 )  
ACCESS=UPDATE  
XA DATASET = KAUGE01.BOZO  
ACCESS=READ
```

CA Top Secret sample – archive

- Example (implementation)

TSS LIST(Rachael) ARCHIVE

TSS LIST(Cassie) ARCHIVE INTO(KOTPA01.ARCHIVE.CASSIE)

TSS LIST(Jonathan) ARCHIVE INTO(KOTPA01.ARCHIVE.DATASET(JONATHAN))

CA Top Secret example - archive

- Example (results/output)

```
/*ARCHIVE RACHAEL STORED 03/08/10-15.25.37 BY MASTER1 ON XE15
/*Please edit any CREATE commands by adding a PASSWORD keyword to the command
TSS CREATE(RACHAEL) NAME('RACHAEL E. KOT') TYPE(USER) DEPT(DEPTLORD)
TSS ADD(RACHAEL) GROUP(OMVSGRP)
TSS ADMIN(RACHAEL) MISC4(CERTAUTH CERTUSER CERTGEN CERTEXPO CERTCHEK)
TSS ADD(RACHAEL) FAC(BATCH)
TSS ADD(RACHAEL) FAC(CICSPROD)
TSS ADD(RACHAEL) FAC(TSO)
TSS ADD(RACHAEL) UID(0000000004)
TSS ADD(RACHAEL) HOME(/U)
TSS ADD(RACHAEL) DFLTGRP(OMVSGRP)
TSS PER(RACHAEL) DSN(SYS1.) ACCESS(READ)
TSS1594I ARCHIVE FUNCTION SUCCESSFUL
TSS0300I LIST FUNCTION SUCCESSFUL
```

CA Top Secret example - model

- Example (implementation)

```
TSS MODEL USING(Rachael) ACID(Cassie)
```

```
TSS MODEL USING(Jonathan) ACID(Ronald) INTO(KOTPA01.MODEL.RONALD)
```

```
TSS MODEL(Jonathan) ACID(Jason) INTO(KOTPA01.MODEL.DATASET(JASON))
```


CA Top Secret - model

- Example (results/output)

```
/*MODEL CASSIE STORED 03/08/10-16.29.03 BY MASTER1 ON XE15 USING RACHAEL
/*Please edit any CREATE commands by adding a PASSWORD keyword to the command
TSS CREATE(CASSIE) NAME('RACHAEL E. KOT') TYPE(USER) DEPT(DEPTLORD)
TSS ADD(CASSIE) GROUP(OMVSGRP)
TSS ADMIN(CASSIE) MISC4(CERTAUTH CERTUSER CERTGEN CERTEXPO CERTCHEK)
TSS ADD(CASSIE) FAC(BATCH)
TSS ADD(CASSIE) FAC(CICSPROD)
TSS ADD(CASSIE) FAC(TSO)
TSS ADD(CASSIE) HOME(/U)
TSS ADD(CASSIE) DFLTGRP(OMVSGRP)
TSS PER(CASSIE) DSN(SYS1.) ACCESS(READ)
TSS0300I MODEL FUNCTION SUCCESSFUL
```