CA Mainframe Security Update and Hidden Gems

Carla A. Flores

Session # 11585

August 7, 2012 – 1:30pm
Session Evaluations

• QR codes

• Online for up to 72 hours after the session
  • [www.SHARE.org/AnaheimEval](http://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
© 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
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

Mainframe Chorus

DE29 racroute: RACROUTE

DE29 SECCACHE: SECCACHE

Alerts

Delete  New Alerts  All

Public Notes  Private Notes

Public Paths  Private Paths

Start New Investigation
## Design goals and architecture

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

### ACF2 and Top Secret

<table>
<thead>
<tr>
<th>Feature</th>
<th>Knowledge Center</th>
<th>Investigator</th>
<th>Metrics Panel</th>
<th>Security Command Managers</th>
<th>Quick Links</th>
<th>Notes</th>
<th>Security Alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIA database</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Admin</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Security command line*</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>ACFTEST/TSSSIM</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Statg</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

### Compliance Manager

<table>
<thead>
<tr>
<th>Feature</th>
<th>Knowledge Center</th>
<th>Investigator</th>
<th>Metrics Panel</th>
<th>Security Command Managers</th>
<th>Quick Links</th>
<th>Notes</th>
<th>Security Alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy*</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Events*</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Alerts*</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

* Includes support for RACF
CA Compliance Manager 2.0 features ease of use

- Data Classification support
- DSN lists for event policy
- Multiple events in a single policy statement
- CONTAINS operator in event policy
CA Compliance Manager 2.0 features ease of use

- Policy statements for multiple components
- SDATE and EDATE relative to TODAY
- Chorus Alerts
CA Compliance Manager 2.0 features
CA Mainframe Chorus integration

Event analysis
CA Mainframe Chorus
New Features in r2.5
Investigator cross-role actions (Storage to Security shown)
Paths and their descriptions are now searchable
Alerts Module
Severity Count summary and Hide-able filter
CA Mainframe Chorus

Security and Compliance Role Improvements in 2.5
Datacom CIA, Data mart(s), and Warehouse
Export from Security Command Manager
Import Into Security Command Manager
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 account 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Field Value Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithm</td>
<td>Signing algorithm</td>
</tr>
<tr>
<td>Trusted</td>
<td>Trust status (Yes or No)</td>
</tr>
<tr>
<td>Cert Length</td>
<td>Certificate length</td>
</tr>
<tr>
<td>Extensions</td>
<td>Contents of certificate extensions (Hex dump, if not common)</td>
</tr>
</tbody>
</table>

• New Totals displayed in Utility output

<table>
<thead>
<tr>
<th>Totals Field</th>
<th>Totals Field Value Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Certificates</td>
<td>Total number of trusted certificates</td>
</tr>
<tr>
<td>High Trust Certificates</td>
<td>Total number of high trusted certificates</td>
</tr>
</tbody>
</table>
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

- 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
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 (SEQ,PDS,etc)

SYS1 / OPTS  LAST CHANGED BY ADMIN ON 02/16/07-12:28
ACCESS BLPLGLOG 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
- **ACFRPRTRX** (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
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.


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

Problem Determination: N/A

Source: ACF2

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

facf2,rebuild(aut),c(r)
ACF8A037 DIRECTORY RAUT ADDED TO RESIDENT CHAIN
```
CA ACF2 sample – compare

<table>
<thead>
<tr>
<th>ACF</th>
<th>Compare JPETERS USING(JSMITH)</th>
</tr>
</thead>
</table>

**LID SECTION**

<table>
<thead>
<tr>
<th>LID</th>
<th>NAME</th>
<th>TSO SECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>JPETERS</td>
<td>JAMES PETERS</td>
</tr>
<tr>
<td></td>
<td>JSMITH</td>
<td>JOHN SMITH</td>
</tr>
</tbody>
</table>

**TSOPROC**

<table>
<thead>
<tr>
<th>DFT-PFX</th>
<th>CATSO</th>
<th>XXTSO</th>
</tr>
</thead>
<tbody>
<tr>
<td>PETERS</td>
<td>SMITH</td>
<td></td>
</tr>
</tbody>
</table>

**RESTRICTIONS SECTION**

<table>
<thead>
<tr>
<th>PREFIX</th>
<th>GROUP</th>
<th>ROLES SECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>PETERS</td>
<td>DEFGRPA</td>
<td>DEFAULTG</td>
</tr>
</tbody>
</table>

**CICS PROFILES**

<table>
<thead>
<tr>
<th>OPCLASS</th>
<th>OPPRTY</th>
<th>TIMEOUT VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>255</td>
<td>15</td>
</tr>
</tbody>
</table>
CA ACF2 sample – archive

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

SET LID
INSERT NEWUSER -
  PASSWORD(NEWUSER) -
  ACCOUNT -
  ACCTPRIV -
  ALLCMD -
  TSOFSCRN -
  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,TYP(ROL)
END
### CA ACF2 sample - role based security

<table>
<thead>
<tr>
<th>RESOURCE(XROL)</th>
<th>GROUP</th>
<th>SYSID(LONG)</th>
<th>RECID - USERGRP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

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

tss per(DCA01) casecaut(tsscmd.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
```
• 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

Example (for demonstration):

```
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))
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