CA Security Update and Hidden Gems

Carla A Flores

Carla.Flores@ca.com

March 11, 2014
Session Number 15225
I changed all my passwords to "incorrect".

So whenever I forget, it will tell me "Your password is incorrect."
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
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

<table>
<thead>
<tr>
<th>Certificate Key display changes</th>
<th>CHKCERT command now displays Public/Private key size and type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Utility (SAFCRRPT) displays key size and type in header</td>
<td>Certificate commands allow for ECC key to be stored and retrieved from ICSF</td>
</tr>
<tr>
<td><strong>ECC (Elliptic Curve Cryptography) Keys and ICSF</strong></td>
<td>New CHKADDRES field in GSO REALM record</td>
</tr>
<tr>
<td>Kerberos address checking</td>
<td>Allows ticket address checking in Kerberos server</td>
</tr>
<tr>
<td><strong>User mount and unmount</strong></td>
<td>Privilege checking accomplished by resource checks</td>
</tr>
<tr>
<td><strong>New R_ usormap function to return Userid from DN or Realm name</strong></td>
<td>No need for all users to have superuser privilege</td>
</tr>
</tbody>
</table>

### z/OS 1.13 compatibility and new functionality
CA ACF2 r15 interim enhancements since GA

IDMAP Cleanup Utility
- 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

CTS 4.2 compatibility and new functionality
- 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

- 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

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

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ACFVSAM Reserve Enqueue Name</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Logonid exclusion from Password / Passphrase Violations</strong></td>
<td>Password violation counters will not be incremented for defined userids. Prevents application outages due to violations. Controlled through new resource class and resource rules.</td>
</tr>
<tr>
<td><strong>Unique UID and GID values</strong></td>
<td>Helps make sure each user is accountable using a unique UID or GID value.</td>
</tr>
</tbody>
</table>
CA ACF2 Incremental Enhancements

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
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
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

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

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
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.
CA Top Secret incremental enhancements

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 as you upgrade to V2R1?
Replays available

December 5 Replay: CA ACF2 Preparation for OMVS Defaults Removal
12/5/13 2:25 PM

Thank you to those of you who joined us today for our "CA ACF2 Preparation for OMVS Defaults Removal" webcast.

The replay is now available:

CA ACF2 Preparation for OMVS Defaults Removal
Thursday, December 5, 2013 1:06 pm New York Time
51 Minutes
+ Watch now

I'm also attaching a PDF of the presentation for your convenience.

Attachments:  CA ACF2 OMVS default_UG_120513.pdf (831.4k)

December 5 Replay: CA Top Secret preparation for OMVS defaults removal
12/5/13 2:25 PM

Thank you to those of you who joined us today for our "CA Top Secret Preparation for OMVS Defaults Removal" webcast.

The replay is now available:

CA Top Secret Preparation for OMVS Defaults Removal
Thursday, December 5, 2013 11:06 am New York Time
51 Minutes
+ Watch it now

I'm also attaching a PDF of the presentation for your convenience.

Attachments:  CA Top Secret OMVS default_UG_120513.pdf (688.1k)

Complete your session evaluations online at www.SHARE.org/Anaheim-Eval
Technical documents available on support.ca.com

CA ACF2 for z/OS:

Knowledge Base Article

Title: I am preparing to implement z/OS 2.1 with ACF2 R15. IBM announced that BPX.DEFAULT.USER was being removed at this release. What do I need to do to setup my system so that I can remove the default UID and GID from the ACF2 GSO

CA Top Secret for z/OS:

Knowledge Base Article

Title: Preparation for removal of Default OMVSUSR and OMVSGRP
ACF2 changes to TEC599992 z/OS 2.1 bpx.default.user

trace usage zos 2.1 acf2 r15 bpx.default.user
2/7/14 12:07 PM

Have you recently followed the instructions in TEC599992 to help with the removal of BPX.DEFAULT.USER for z/OS 2.1?

The details of the trace process that was introduced by RO55702 to identify users of BPX.DEFAULT.USER has now been changed by RO65357.

The new mechanism for tracing users of BPX.DEFAULT.USER in an ACF2 r15 system is to set the TRACEDFT bit in the C(GSO) UNIXOPTS record.

The default for this field is NOTRACEDFT.

The output from the trace will still be reported in ACFRPTOM for any INITUSP requests that use the omvs defaults.

TEC599992 has been updated to provide the details of RO65357.
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 *DATAACL$ 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)
Q&A

Thank you!