Security Update – Hear what's new

Carla A. Flores
CA Technologies

Monday ~ August 8, 2011
Session Number: **9938**

legal notice

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 ACF2 & CA Top Secret r14 Review
- CA ACF2 & CA Top Secret r15 Overview
- CA Mainframe Security Future Direction
- Open Discussion/Questions

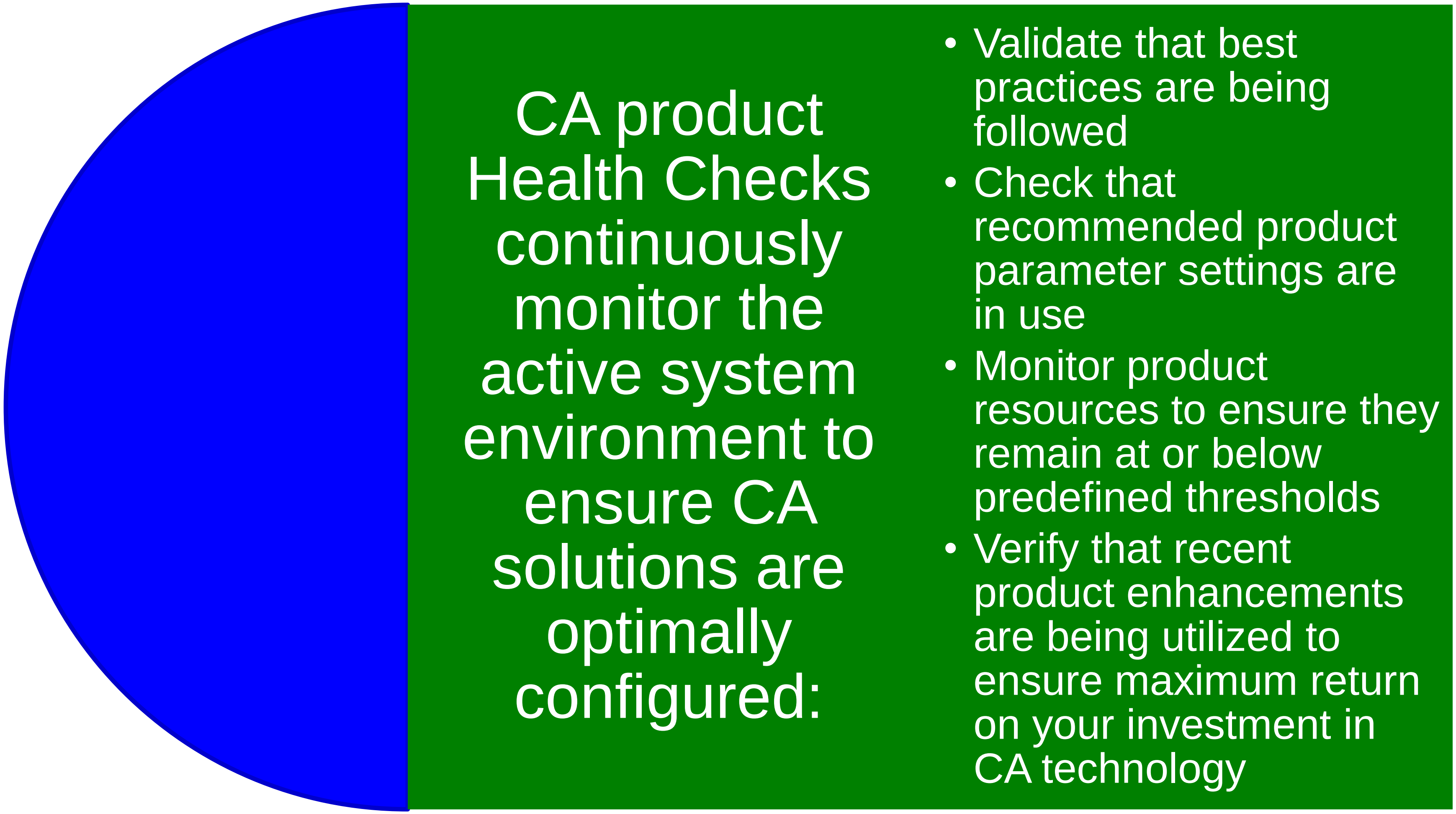
Note: Specific examples of some features are in an Appendix section at the end of this presentation

Release status

- CA ACF2 & CA Top Secret r15 – eta 10/2010
- CA ACF2 & CA Top Secret r14 sp1 – 2/2010
- CA ACF2 / CA Top Secret r12 – End of Service 3/1/2011
- CA ACF2 & CA Top Secret r1.3 for DB2 – 6/2010
- CA Web Administrator r15 – 2/2010
- CA Cleanup r12.1 – 6/2010
- CA Auditor r12.1 – 6/2010
- CA Compliance Manager r1 – 5/2009
- EAL4+ Certification (CA ACF2, CA Top Secret, CA Compliance Manager) – Complete

- http://www.ca.com/us/Support/mainframe-compatibilites/z196-Compatibility-Matrix.aspx

An overview of CA Security Health Checks



CA product Health Checks continuously monitor the active system environment to ensure CA solutions are optimally configured:

- Validate that best practices are being followed
- Check that recommended product parameter settings are in use
- Monitor product resources to ensure they remain at or below predefined thresholds
- Verify that recent product enhancements are being utilized to ensure maximum return on your investment in CA technology

CA ACF2 Health Checks

ACF2 Health Checks

- ✓ Determine use of SAFDEFs with NOAPFCHK
- ✓ Determine if the CA ACF2 AUTO Start feature is in use (CAISEC00)
- ✓ Determine if volume contention exits with ACF2 Databases
- ✓ Exits

Leveraging the power of the z/OS Health Checker for your Security implementation

CA ACF2 Health Checks

ACF2 Health Checks

- ✓ Determine use of SAFDEFs with NOAPFCHK
- ✓ Determine if the CA ACF2 AUTO Start feature is in use (CAISEC00)
- ✓ Determine if volume contention exits with ACF2 Databases
- ✓ Exits

Leveraging the power of the z/OS

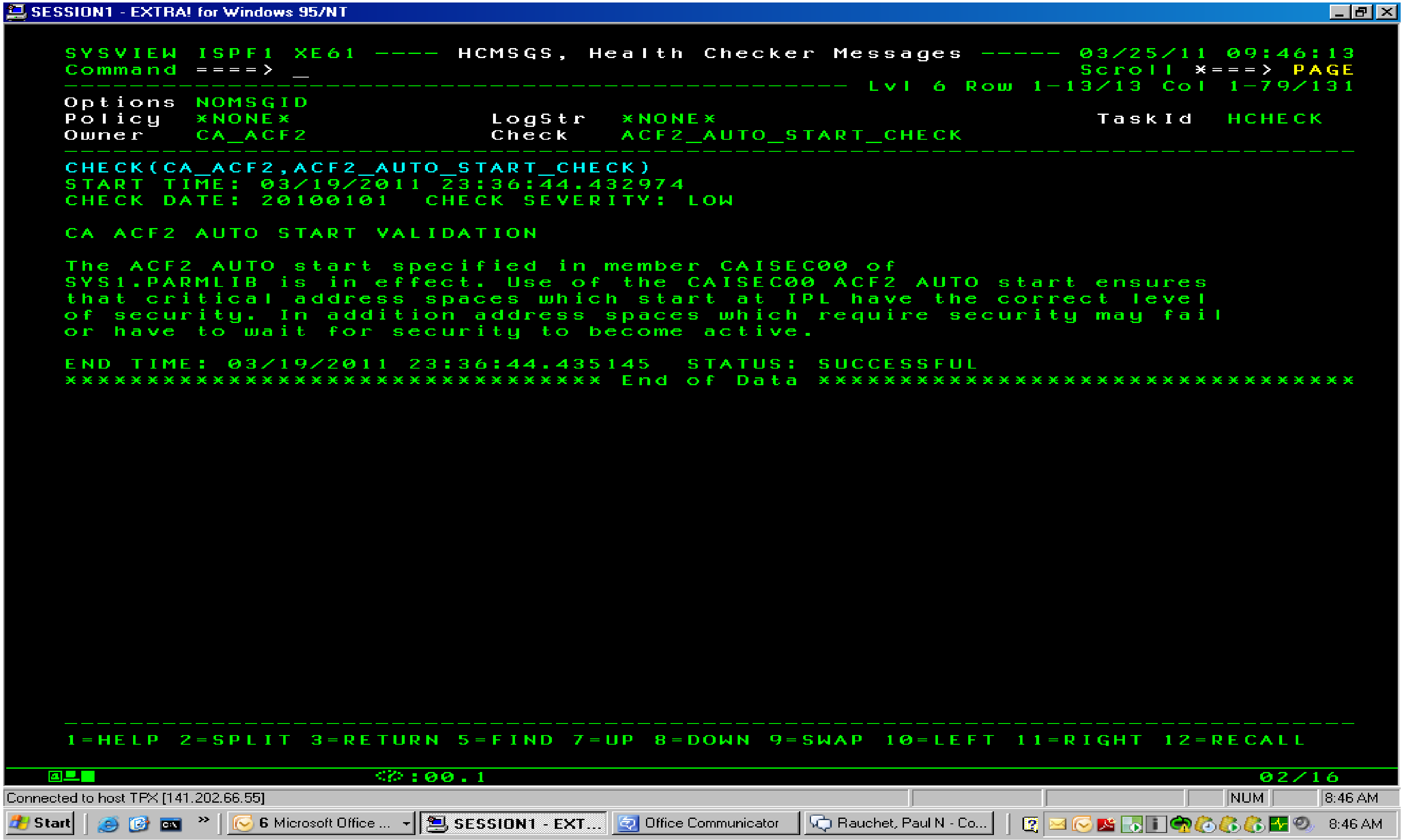
Health Checker for your

Security implementation

Benefit

- ✓ Reduces risk of user bypassing APF checking on RACROUTE calls
- ✓ Enables CA ACF2 to start early and ensures other Address Spaces that start during IPL will have correct level of security

CA ACF2 Health Check Sample



```
SYSVIEW ISPF1 XE61 ---- HCMSGS, Health Checker Messages ------ 03/25/11 09:46:13
Command ====> _                                                 Scroll *===> PAGE
------------------------------------------------ Lvl 6 Row 1-13/13 Col 1-79/131
Options  NOMSGID
Policy   *NONE*              LogStr  *NONE*                     TaskId   HCHECK
Owner    CA_ACF2             Check   ACF2_AUTO_START_CHECK
--------------------------------------------------------------------------------
CHECK(CA_ACF2,ACF2_AUTO_START_CHECK)
START TIME: 03/19/2011 23:36:44.432974
CHECK DATE: 20100101  CHECK SEVERITY: LOW

CA ACF2 AUTO START VALIDATION

The ACF2 AUTO start specified in member CAISEC00 of
SYS1.PARMLIB is in effect. Use of the CAISEC00 ACF2 AUTO start ensures
that critical address spaces which start at IPL have the correct level
of security. In addition address spaces which require security may fail
or have to wait for security to become active.

END TIME: 03/19/2011 23:36:44.435145  STATUS: SUCCESSFUL
********************************* End of Data *********************************













--------------------------------------------------------------------------------
1=HELP 2=SPLIT 3=RETURN 5=FIND 7=UP 8=DOWN 9=SWAP 10=LEFT 11=RIGHT 12=RECALL

                          :00.1                                           02/16
Connected to host TPX [141.202.66.55]
```

Top Secret Health Checks

Top Secret Health Checks

- ✓ Determine if CA Top Secret Audit Tracking file is allocated on same volume as the TSS Security File
- ✓ Determine if CA Top Secret CACHE and SECCACHE features are enabled

Leveraging the power of the

z/OS Health Checker for your

Security implementation

Top Secret Health Checks

Top Secret Health Checks

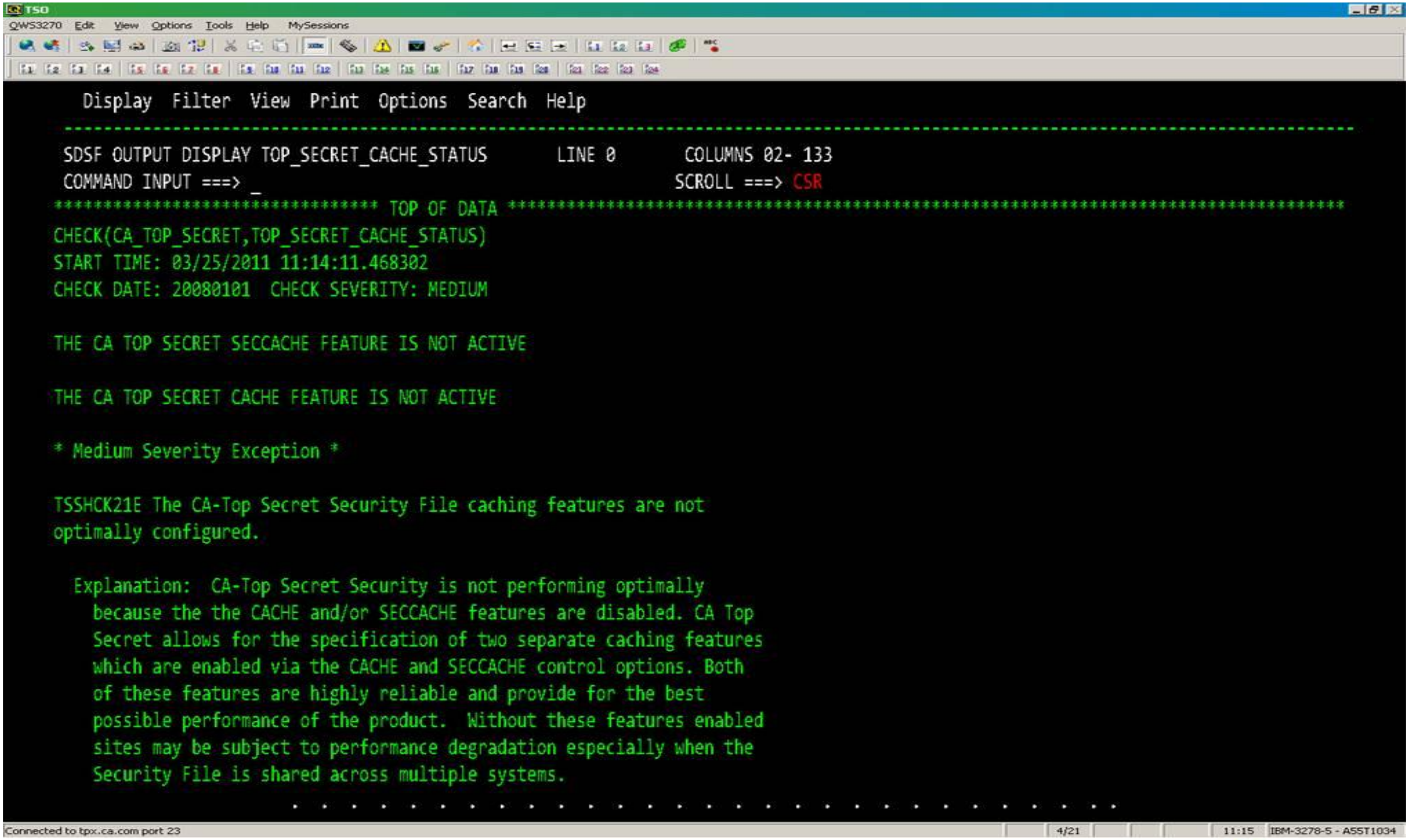
- ✓ Determine if CA Top Secret Audit Tracking file is allocated on same volume as the TSS Security File
- ✓ Determine if CA Top Secret CACHE and SECCACHE features are enabled

Leveraging the power of the z/OS Health Checker for your Security implementation

Benefit

- ✓ Reduces the number of support issues resulting from performance degradation when these two files share a DASD volume
- ✓ Helps prevent performance degradation by not using all of the product-supplied cache features

Top Secret Health Check Sample


TSO
QWS3270 Edit View Options Tools Help MySessions
Connected to tpx.ca.com port 23
4/21
11:15
IBM-3278-5 - A55T1034

```
    Display  Filter  View  Print  Options  Search  Help
  -------------------------------------------------------------------------------------------------------------------
  SDSF OUTPUT DISPLAY TOP_SECRET_CACHE_STATUS      LINE 0       COLUMNS 02- 133
  COMMAND INPUT ===> _                                         SCROLL ===> CSR
 ********************************* TOP OF DATA ******************************************************************
 CHECK(CA_TOP_SECRET,TOP_SECRET_CACHE_STATUS)
 START TIME: 03/25/2011 11:14:11.468302
 CHECK DATE: 20080101  CHECK SEVERITY: MEDIUM

 THE CA TOP SECRET SECCACHE FEATURE IS NOT ACTIVE

 THE CA TOP SECRET CACHE FEATURE IS NOT ACTIVE

 * Medium Severity Exception *

 TSSHCK21E The CA-Top Secret Security File caching features are not
 optimally configured.

   Explanation:  CA-Top Secret Security is not performing optimally
     because the the CACHE and/or SECCACHE features are disabled. CA Top
     Secret allows for the specification of two separate caching features
     which are enabled via the CACHE and SECCACHE control options. Both
     of these features are highly reliable and provide for the best
     possible performance of the product.  Without these features enabled
     sites may be subject to performance degradation especially when the
     Security File is shared across multiple systems.
                              . . . . . . . . . . . . . . . . . . . . . . . . . . . .
```

CA ACF2 & CA TOP SECRET R14 RECAP

CA ACF2 release 14 recap

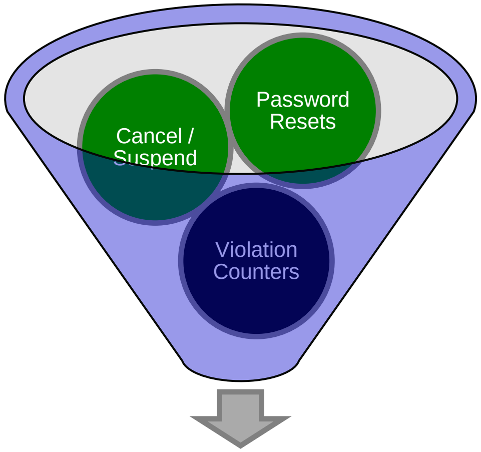
- Role-based Security
  - New X(ROL) records to define ‘roles’ and attach users to the role
  - Dataset and Resource rules:
- Data Classification / Ownership
  - New DCO records to define a classification (SOX, HIPPA) and associate a resource and ownership
  - Reporting modified to use Data Classification
- New Password Encryption Option
  - Support for AES128 using ICSF
- Certificate Processing Improvements
  - In-core storage usage moved to 64-bit memory objects
  - New search algorithm to speed look-up calls
- Sysplex Enhanced
  - Provides the ability to share one CA ACF2 database in the Sysplex Coupling Facility

CA Top Secret release 14 recap

- Data Classification / Ownership
- New Password Encryption Option: AES128 using ICSF
- Certificate processing improvements
  - In-core storage usage moved to 64-bit memory objects
  - New search algorithm to speed look-up calls
- Catalog SMS dataset delete option (CATADELPROT)
- Extract replace changes
  - Data fields now sent through CPF and LDS
- Inactive control option change
- Suspending global table refresh

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)

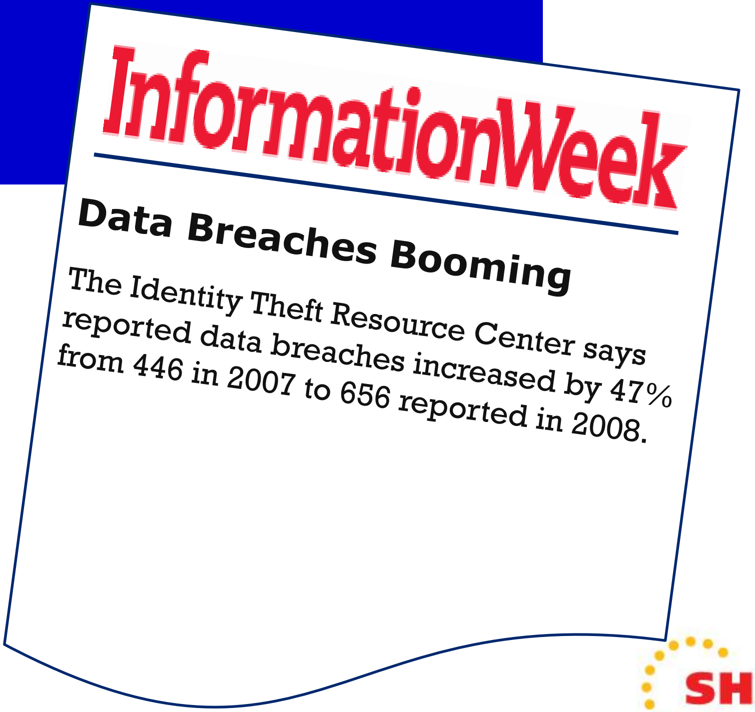
- Description
  - Archival allows user's permissions and resources to be archived into form of TSS commands
  - Generated TSS commands can be stored in PDS dataset and used to restore a user
  - First record in output is a comment, which contains:
    - Command
    - User acid being modeled
    - Date 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



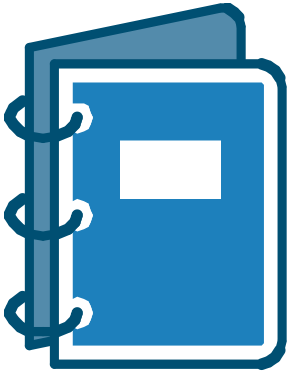
InformationWeek

Data Breaches Booming

The Identity Theft Resource Center says reported data breaches increased by 47% from 446 in 2007 to 656 reported in 2008.

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

CA ACF2™ 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

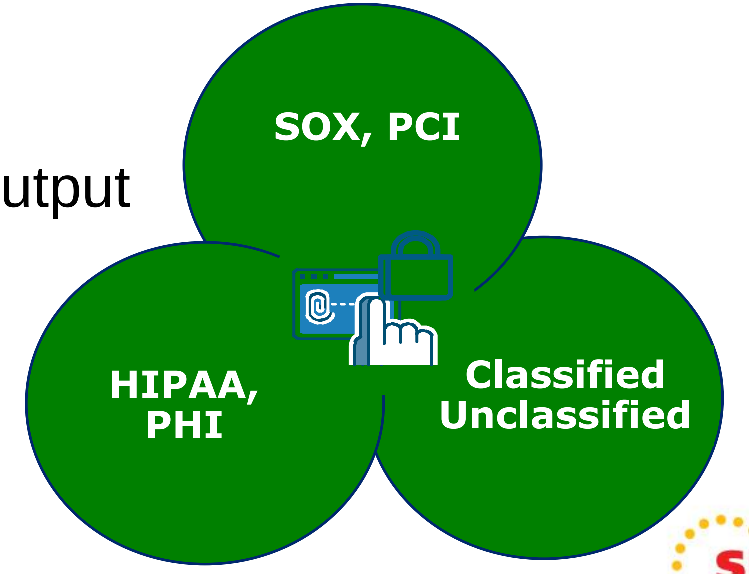
- Erase-on-Scratch (EOS) support
- “Existing” method (ACF2 intercepts-based)
  - Erase processing done out of ACF2 ERASE intercepts
  - If using existing EOS method, ACF2 does the manual scratching
- “New” method (SAF-based)
  - Controlled by GSO AUTOERAS record – new PROCESS(SAF|ACF2)
  - Better control 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

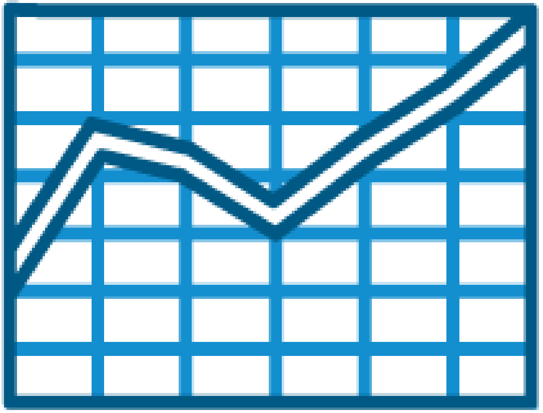
- DSERV Exit Support
  - PDSE support for PDS Member Level Protection and Program Pathing
- Data Classification
  - Data Classification and Ownerships to added to Compliance Manager Event Records
- SHOW RSRCTYPE
  - Incorporated in Show All output



CA TOP SECRET® ONLY

virtual storage constraint relief (VSCR)

- Use of 64-bit storage above the bar
- Kerberos - restructuring of in-core tables
  - Hash Table Based
  - Support update in place
  - Support multiple record key fields for fast lookups
  - Support Variable length fields
  - No length limit

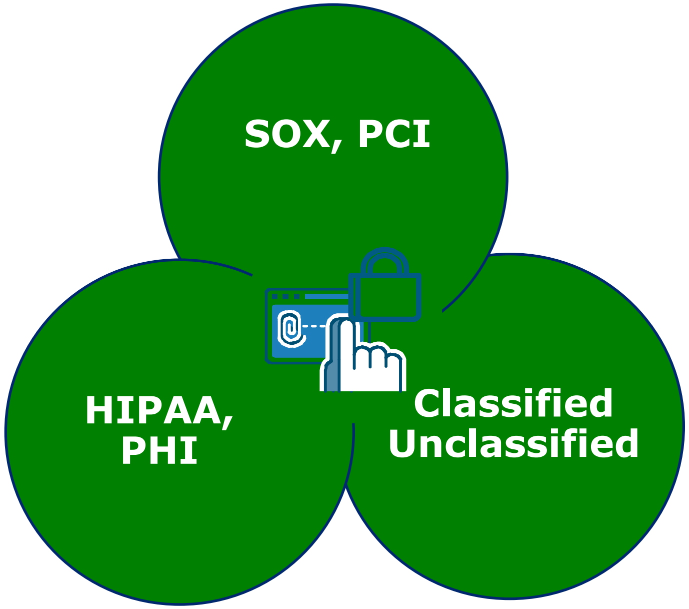


auto start

- Description
  - 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

data classification enhancement

- Data Classification Enhancement
  - Add Data Classification and Ownerships to CA Compliance Manager Event Records



CA MAINFRAME CHORUS ~ SECURITY ROLE

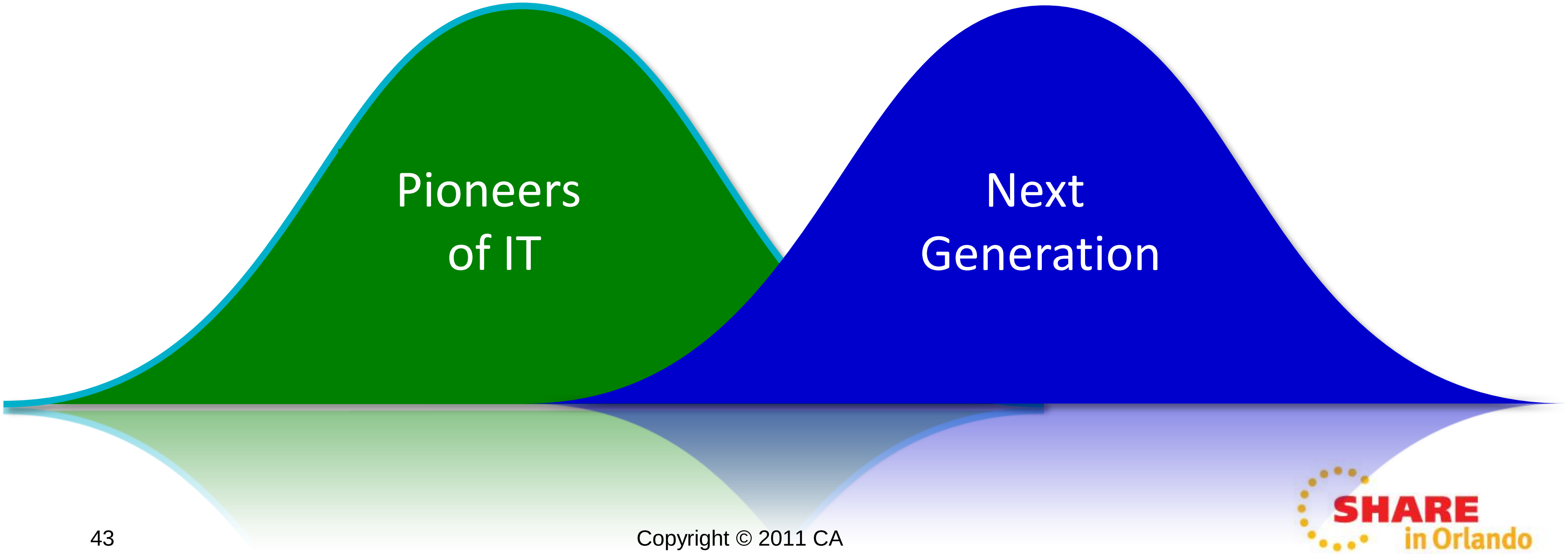
the challenge…

Sustain critical skills and enable next generation mainframer

On-ramp to mainframe mastery is long & steep

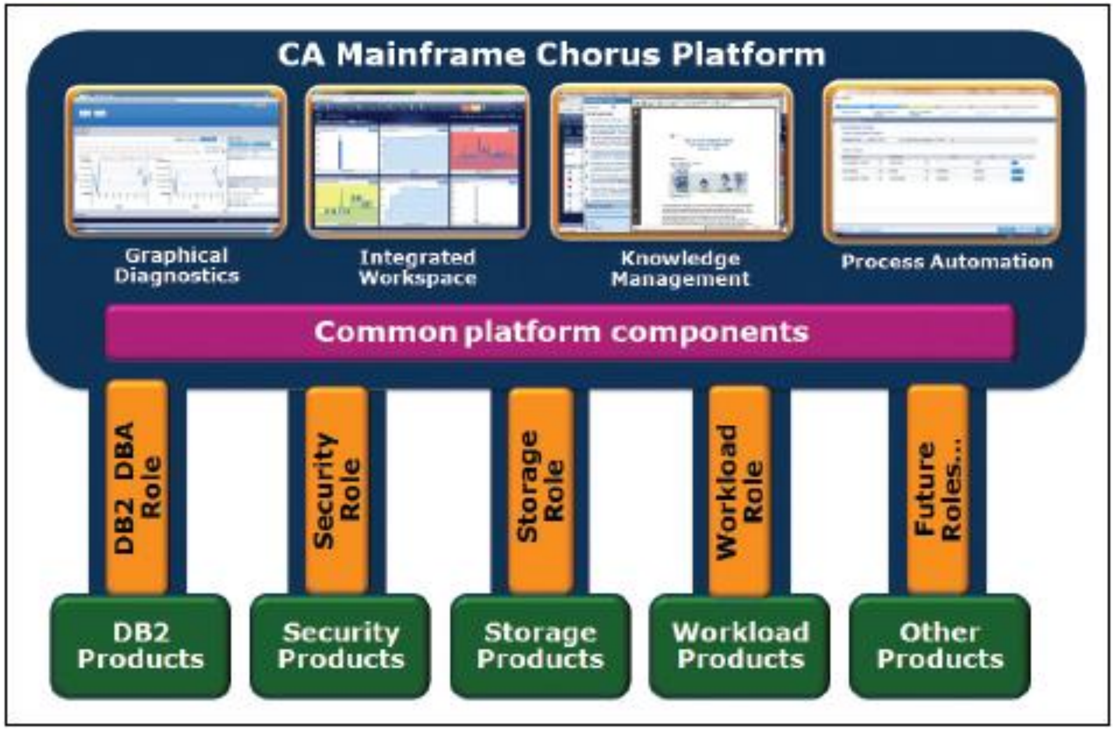
“Net Generation” thinks and works differently

Demands a new approach



CA Mainframe Chorus - approach

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



CA Compliance Manager for z/OS meeting the needs of compliance & auditing

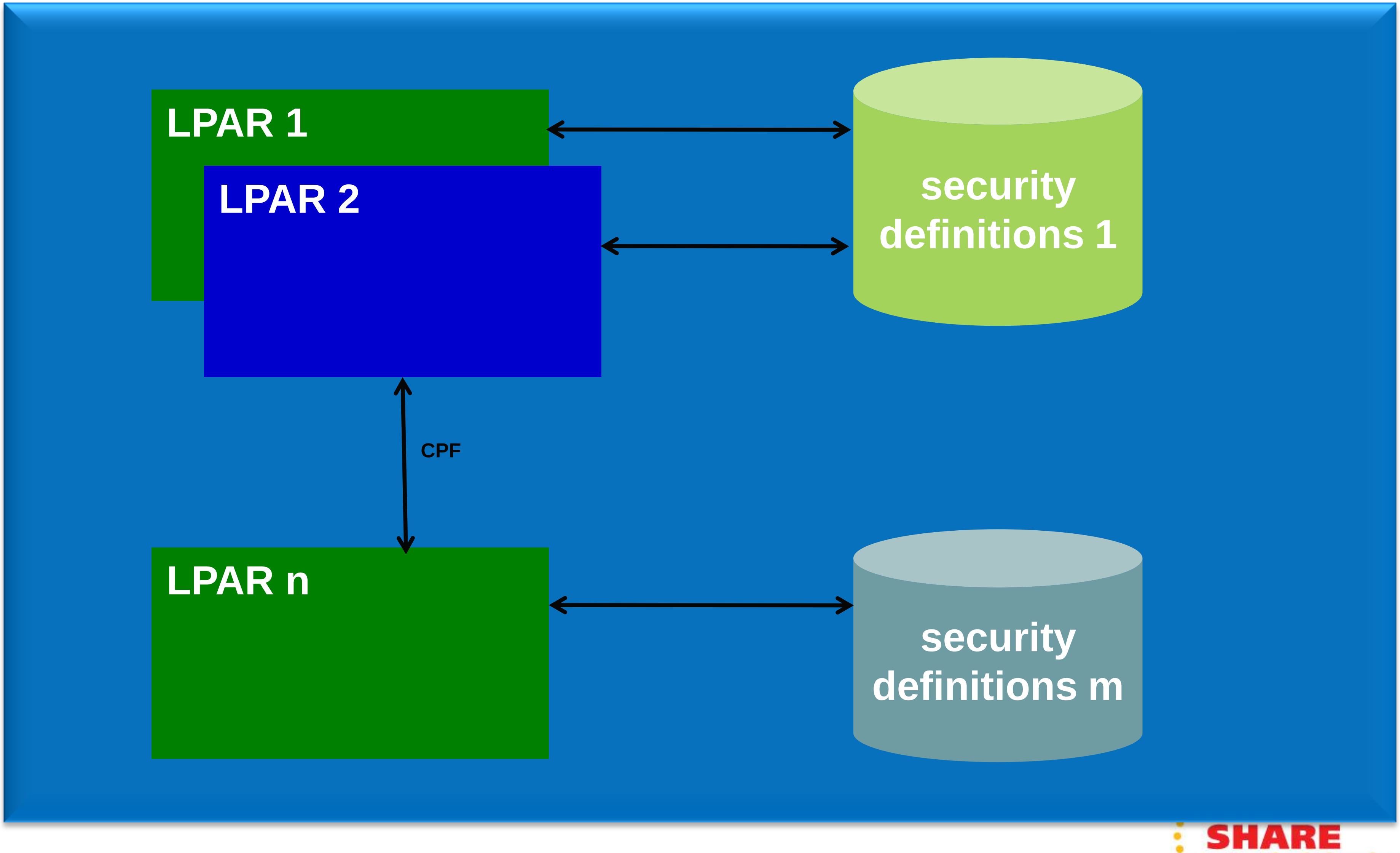
WHAT CAN IT DO?

- Real-time detection and notification of
  - changes to ESM, OS and PDS/PDSE data sets
  - ESM authentications and authorizations
- Complements existing security infrastructure

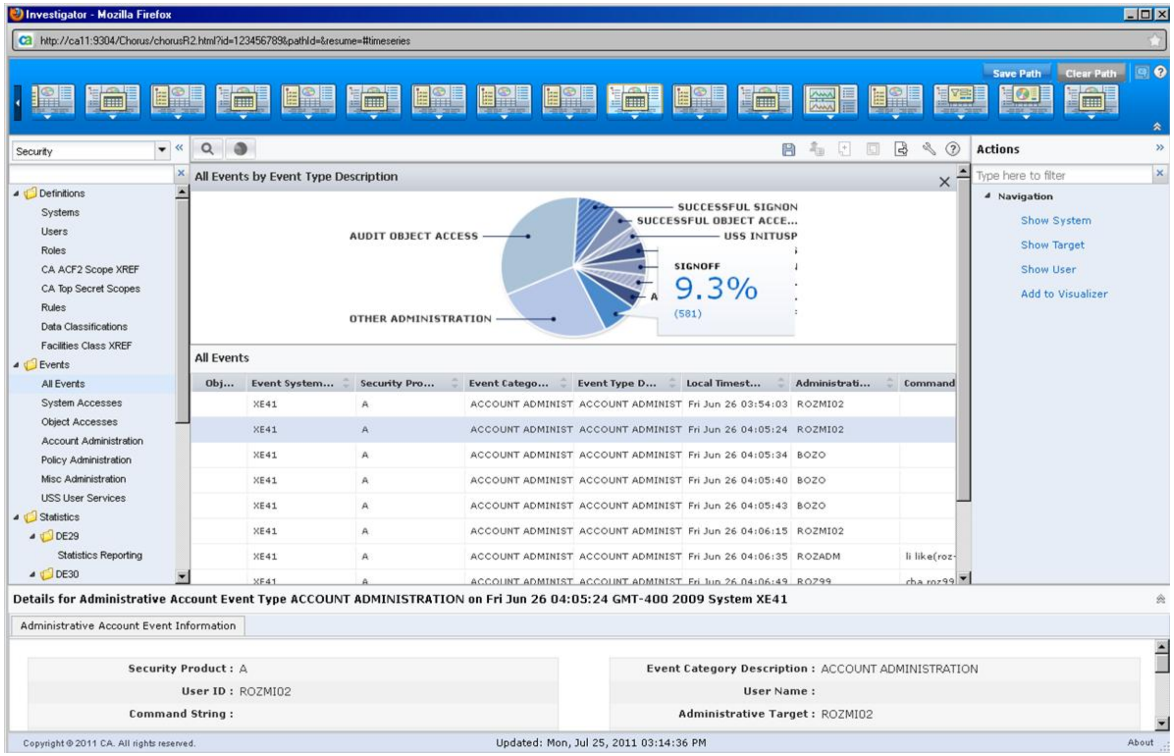
BENEFITS

- Move from a passive compliance stance to an automated, proactive and cost-effective approach
- Reduce unauthorized access risk
- Streamlined compliance
  - Complete compliance activities and reports in

typical security environments and Chorus connections



Investigator



Obj...	Event System...	Security Pro...	Event Catego...	Event Type D...	Local Timest...	Administrati...	Command
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 03:54:03	ROZMI02	
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:05:24	ROZMI02	
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:05:34	BOZO	
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:05:40	BOZO	
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:05:43	BOZO	
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:06:15	ROZMI02	
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:06:35	ROZADM	li like(roz-
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:06:49	ROZ99	cha roz99

Details for Administrative Account Event Type ACCOUNT ADMINISTRATION on Fri Jun 26 04:05:24 GMT-400 2009 System XE41

Administrative Account Event Information

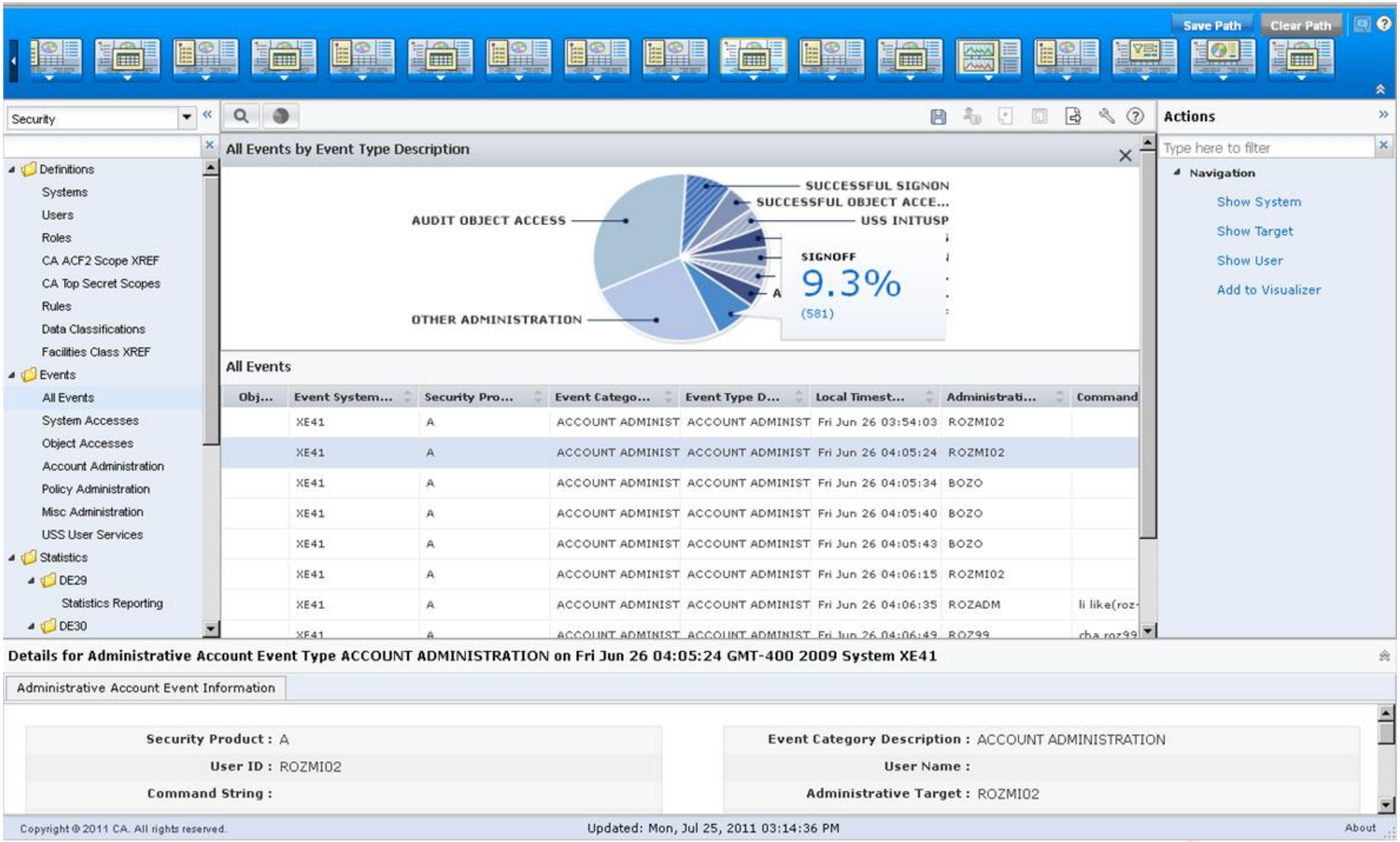
Security Product :	A	Event Category Description :	ACCOUNT ADMINISTRATION
User ID :	ROZMI02	User Name :	
Command String :		Administrative Target :	ROZMI02

Copyright © 2011 CA. All rights reserved.

Updated: Mon, Jul 25, 2011 03:14:36 PM

Changing The Way The Mainframe Is Managed Forever
ca Mainframe 2.0
Next-Generation Mainframe Management
CA Mainframe Chorus

Investigator



All Events

Obj...	Event System...	Security Pro...	Event Catego...	Event Type D...	Local Timest...	Administrati...	Command
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 03:54:03	ROZMI02	
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:05:24	ROZMI02	
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:05:34	BOZO	
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:05:40	BOZO	
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:05:43	BOZO	
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:06:15	ROZMI02	
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:06:35	ROZADM	li like(roz-
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:06:49	ROZ99	cha roz99

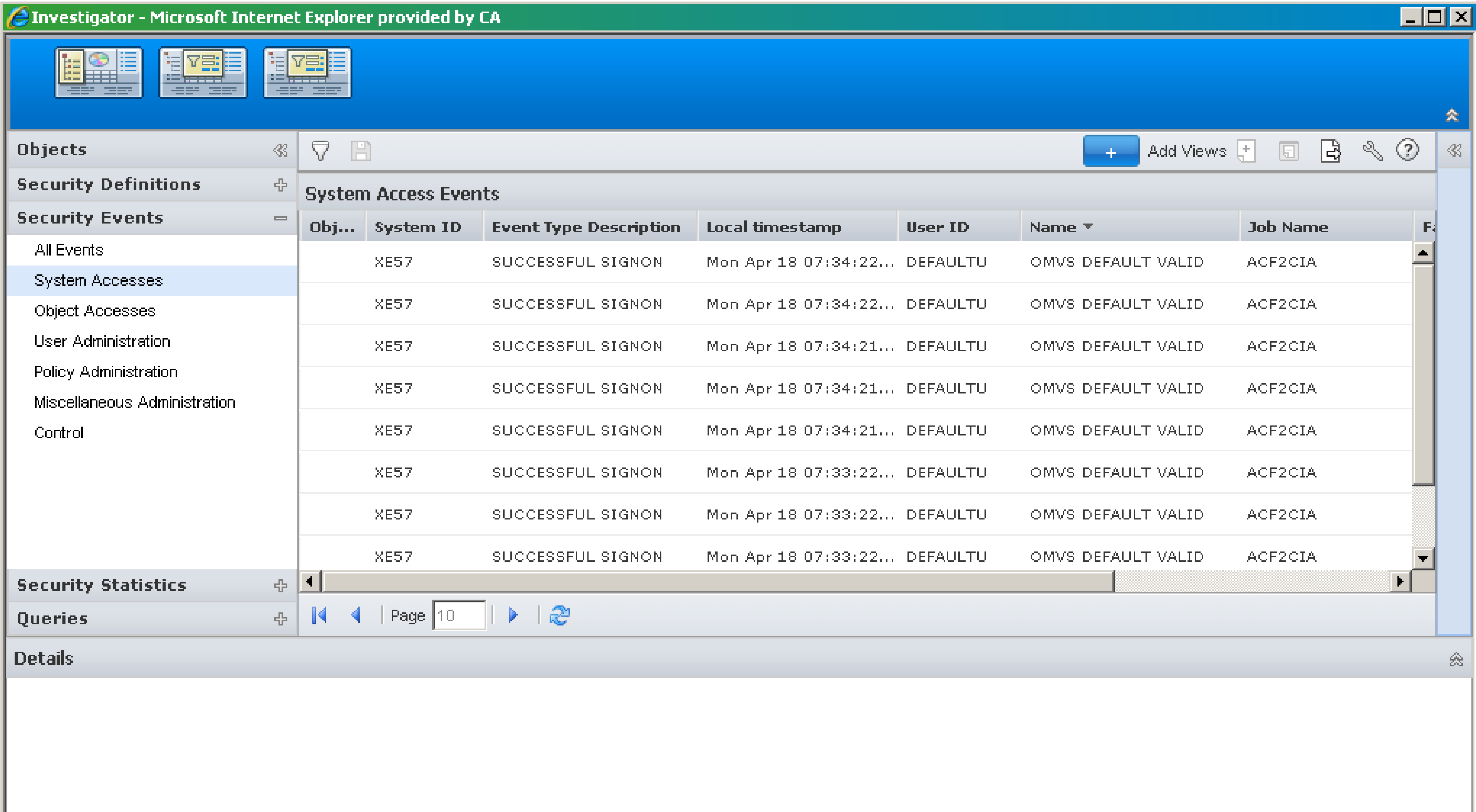
Details for Administrative Account Event Type ACCOUNT ADMINISTRATION on Fri Jun 26 04:05:24 GMT-400 2009 System XE41

Administrative Account Event Information

Security Product :	A	Event Category Description :	ACCOUNT ADMINISTRATION
User ID :	ROZMI02	User Name :	
Command String :		Administrative Target :	ROZMI02

Updated: Mon, Jul 25, 2011 03:14:36 PM

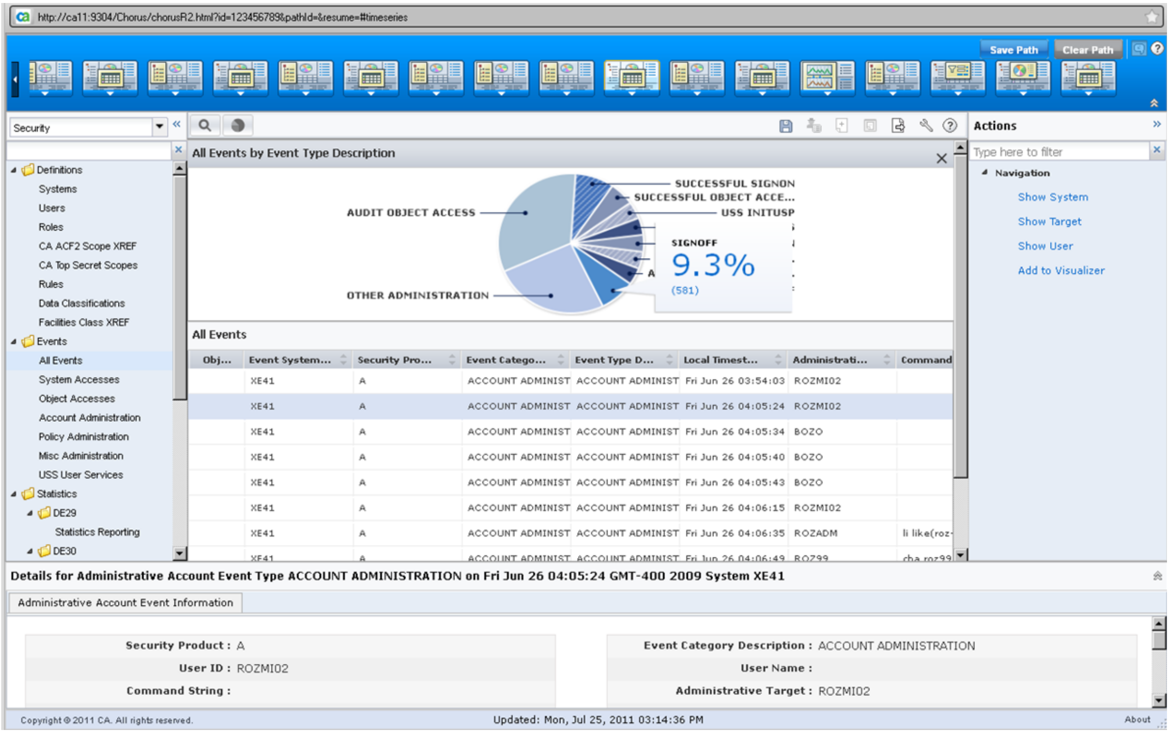
Investigator - reporting on compliance events with join to CIA information



System Access Events

Obj...	System ID	Event Type Description	Local timestamp	User ID	Name	Job Name	F
	XE57	SUCCESSFUL SIGNON	Mon Apr 18 07:34:22...	DEFAULTU	OMVS DEFAULT VALID	ACF2CIA	
	XE57	SUCCESSFUL SIGNON	Mon Apr 18 07:34:22...	DEFAULTU	OMVS DEFAULT VALID	ACF2CIA	
	XE57	SUCCESSFUL SIGNON	Mon Apr 18 07:34:21...	DEFAULTU	OMVS DEFAULT VALID	ACF2CIA	
	XE57	SUCCESSFUL SIGNON	Mon Apr 18 07:34:21...	DEFAULTU	OMVS DEFAULT VALID	ACF2CIA	
	XE57	SUCCESSFUL SIGNON	Mon Apr 18 07:34:21...	DEFAULTU	OMVS DEFAULT VALID	ACF2CIA	
	XE57	SUCCESSFUL SIGNON	Mon Apr 18 07:33:22...	DEFAULTU	OMVS DEFAULT VALID	ACF2CIA	
	XE57	SUCCESSFUL SIGNON	Mon Apr 18 07:33:22...	DEFAULTU	OMVS DEFAULT VALID	ACF2CIA	
	XE57	SUCCESSFUL SIGNON	Mon Apr 18 07:33:22...	DEFAULTU	OMVS DEFAULT VALID	ACF2CIA	

Investigator - summary



All Events

Obj...	Event System...	Security Pro...	Event Catego...	Event Type D...	Local Timest...	Administrati...	Command
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 03:54:03	ROZMI02	
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:05:24	ROZMI02	
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:05:34	BOZO	
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:05:40	BOZO	
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:05:43	BOZO	
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:06:15	ROZMI02	
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:06:35	ROZADM	li like(roz-
	XE41	A	ACCOUNT ADMINIST	ACCOUNT ADMINIST	Fri Jun 26 04:06:49	ROZ99	cha roz99

Details for Administrative Account Event Type ACCOUNT ADMINISTRATION on Fri Jun 26 04:05:24 GMT-400 2009 System XE41

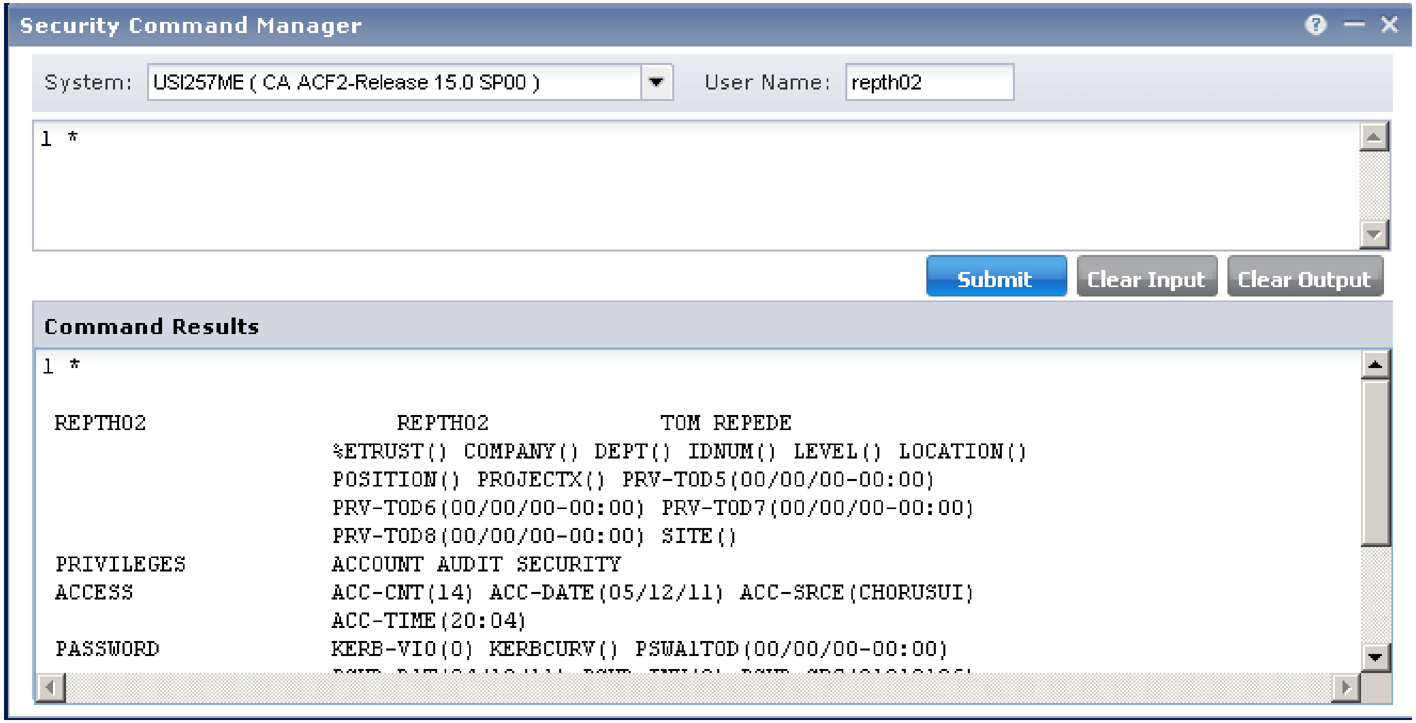
Administrative Account Event Information

Security Product :	A	Event Category Description :	ACCOUNT ADMINISTRATION
User ID :	ROZMI02	User Name :	
Command String :		Administrative Target :	ROZMI02

Copyright © 2011 CA. All rights reserved. Updated: Mon, Jul 25, 2011 03:14:36 PM About

- real-time CIA update
- pie charts to summarize data
- configurable columns and row filters
- easy joins across CA and customer tables and data sources
- Breadcrumbs for history and navigation
- save queries for reuse. Export result to CSV
- save as JCL to run in batch

Security Command Manager



System: USI257ME (CA ACF2-Release 15.0 SP00)

User Name: repth02

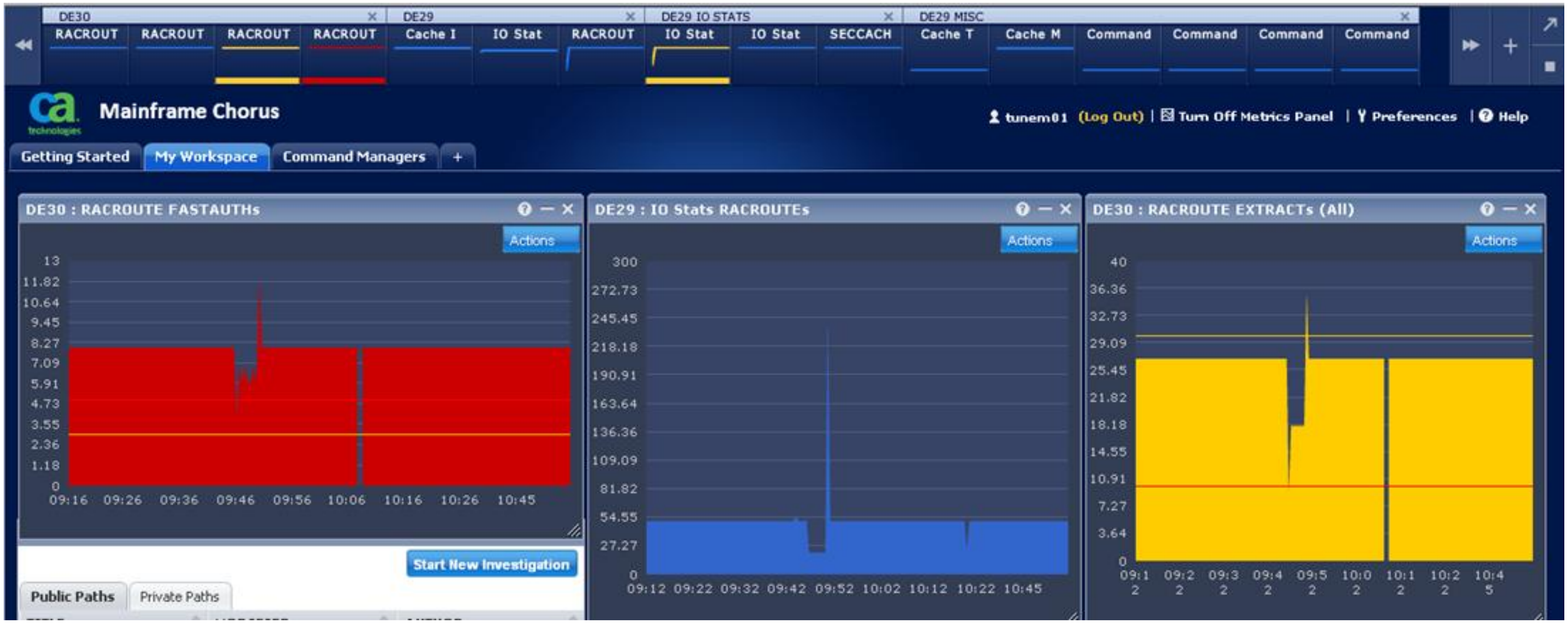
```
1 *
```

```
1 *

 REPTH02                      REPTH02              TOM REPEDE
                         %ETRUST() COMPANY() DEPT() IDNUM() LEVEL() LOCATION()
                         POSITION() PROJECTX() PRV-TOD5(00/00/00-00:00)
                         PRV-TOD6(00/00/00-00:00) PRV-TOD7(00/00/00-00:00)
                         PRV-TOD8(00/00/00-00:00) SITE()
 PRIVILEGES              ACCOUNT AUDIT SECURITY
 ACCESS                  ACC-CNT(14) ACC-DATE(05/12/11) ACC-SRCE(CHORUSUI)
                         ACC-TIME(20:04)
 PASSWORD                KERB-VIO(0) KERBCURV() PSWA1TOD(00/00/00-00:00)
```

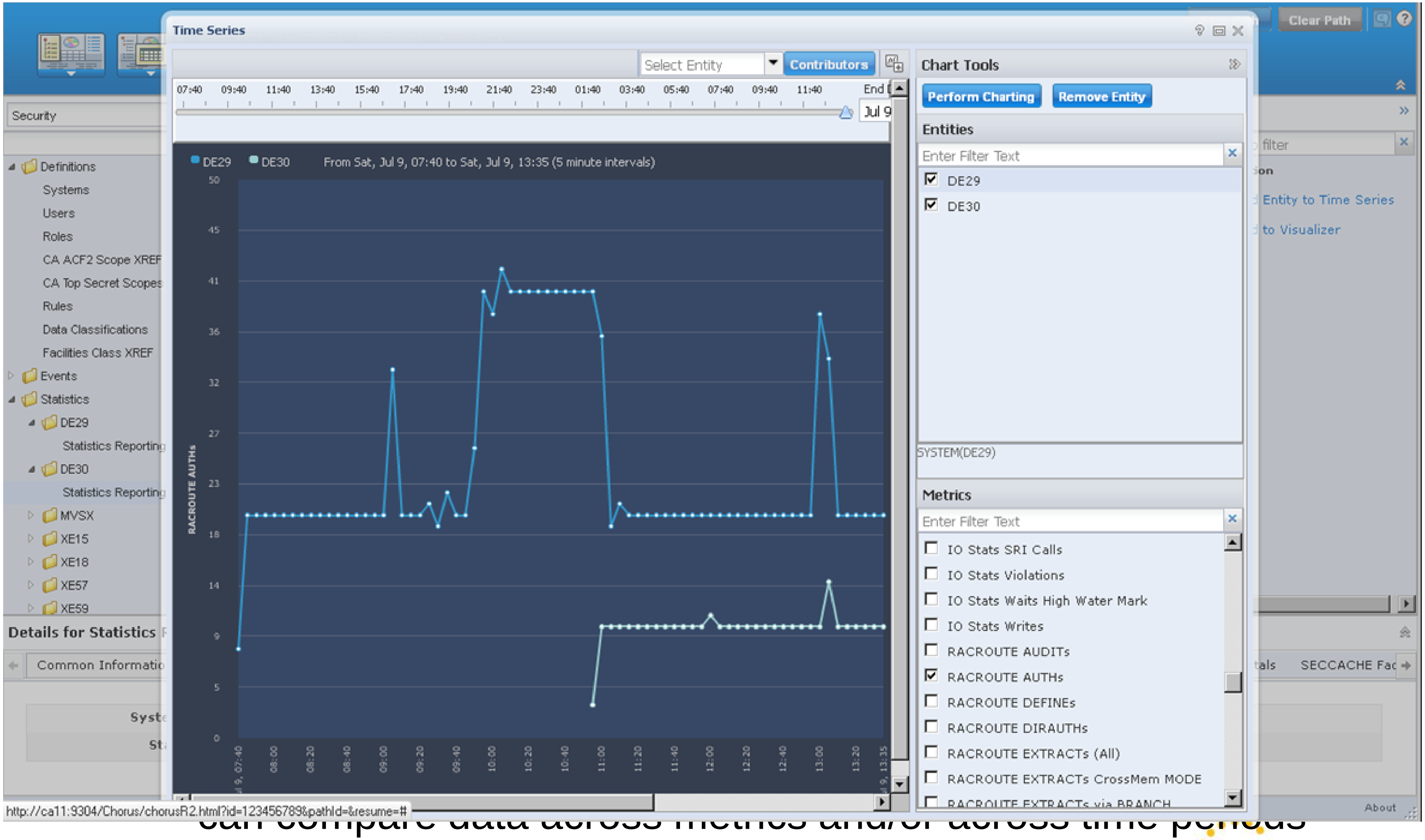
- lets users direct “native” commands to security system(s) without leaving Chorus
- provides scrollable and copyable output
- supports identity inheritance or override
- integrates with Knowledge Center

Metrics Panel and Workspace charts



- visually, continuously monitors security system(s) performance in real-time
- provides configurable content
- provides configurable thresholds
- charts can be added to Workspace for larger display and more data points

Time Series Facility



Time Series

■ DE29 ■ DE30 From Sat, Jul 9, 07:40 to Sat, Jul 9, 13:35 (5 minute intervals)

Entities

- ☑ DE29
- ☑ DE30

SYSTEM(DE29)

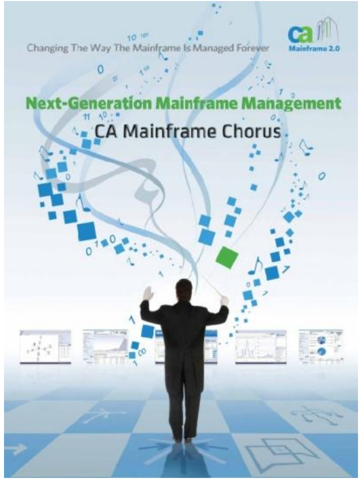
Metrics

- ☐ IO Stats SRI Calls
- ☐ IO Stats Violations
- ☐ IO Stats Waits High Water Mark
- ☐ IO Stats Writes
- ☐ RACROUTE AUDITs
- ☑ RACROUTE AUTHs
- ☐ RACROUTE DEFINEs
- ☐ RACROUTE DIRAUTHs
- ☐ RACROUTE EXTRACTs (All)
- ☐ RACROUTE EXTRACTs CrossMem MODE
- ☐ RACROUTE EXTRACTs via BRANCH

can compare data across metrics and/or across time periods

Feature and benefit recap

- Real-time access to state and event data
- Advanced reporting capabilities
- Security data model extension
- Collaboration and knowledge management
- New and improved event handling for z/OS


Changing The Way The Mainframe Is Managed Forever
ca
Mainframe 2.0
Next-Generation Mainframe Management
CA Mainframe Chorus

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

* Includes support for RACF

Review

- Mainframe Security Directives
  - Electronic Delivery of Software – ESD
  - Health Checker Initiatives
  - SMP/E Standardization across all CA Products
  - Deployment / Serviceability
- CA ACF2 & CA Top Secret Enhancements
  - Compliancy Considerations
  - Administration Capabilities
  - Performance Enhancements
  - Incorporated DARs
- CA Mainframe Chorus ~ Security Role
- **z/VM update: Session 10048 – Tuesday 9:30am – Oceanic 8**

OPEN DISCUSSION – Q&A

APPENDIX

EXAMPLES

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
-------------------------------------------------------------------
          GROUPE                 GROUPA
          GROUPH                 GROUPC
                    CICS PROFILES
-------------------------------------------------------------------
 OPCLASS                          Y
 OPPRTY                   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  -
 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,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(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
```

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
```