#SHAREorg

SHARE

#12264

All Security All The Time: System z Security Update for CA ACF2, IBM RACF, CA Top Secret

February 4, 2013 ~ 3:00pm

Mark Hahn

IBM

Carla A. Flores

ca technologies

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

SHARE in San Francisco 2013

Session Evaluations

- QR codes

- Online for up to 72 hours after the session
  - www.SHARE.org/SFEval

Agenda

- IBM RACF Update
- CA ACF2™ for z/OS Update
- CA Top Secret® for z/OS Update
- Open Discussion/Questions

IBM RACF update

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

Trademarks

- •CICS®
- •DB2®
- •Language Environment®
- •OS/390®

The following are trademarks or registered trademarks of other companies.

* Registered trademarks of IBM Corporation

* All other products may be trademarks or registered trademarks of their respective companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon

considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput

improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance

characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business

contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-

IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

RACF 1.13

- Current RACF 1.13
- z/OS on 2-year cycle
- Are you making use of the valuable features?

RACF 1.13
RRSF via TCP/IP

With z/OS V1.13, you can link RRSF nodes using TCP/IP instead of APPC! This means that you can now:

- Manage your RRSF network using the same skills as the rest of your TCP/IP network.
- Ensure that the same network security policy (IDS, IPS, etc.) is in place for your RRSF network as in place for the rest of your z/OS TCP/IP network.
- Utilize the encryption and peer-node authentication of AT-TLS
- Keep up with improvements in z/OS Communications Server Security.
- Convert a node from using APPC to TCP/IP without stopping communication

RACF 1.13
Identity Propagation

Propagate userid between applications

- **Now you can achieve end-to-end security identity consistency and auditing for key system environments such as:**
  - CICS
  - DB2
  - WebSphere
  - DataPower
- **This provides *consistent end-to-end* auditing of z/OS transactions that originate from the internet by maintaining the user's distributed identity information, without impacting the performance characteristics of transaction providers.**

RACF 1.13
Digital Certificates

RACF support for hardware-generated Elliptic Curve Cryptography (ECC) secure keys,

- Provides the ability to issue and use certificates with hardware protection
- ECC keys added
- RACDCERT support enhanced for greater usability

RACF 1.13
PKI Services

Support of DB2 for PKI Services Databases

- Both PKI Services databases can be stored in DB2
- Object store – holds records to track active certificate requests and posting objects for certificates and CRLs
- Issued Certificate List – permanent record for each certificate issued

RACF 1.13
Certificate Revocation Lists

Larger Certificate Revocation Lists (CRLs)

- When LDAP posting is enabled, 32K limit is removed by storing the CRLs in the HFS or zFS instead of in VSAM

Enhanced support for Web Browsers

- Previously, PKI Services only supported IE to use a smart card for the Windows Logon certificate generation
- Now Mozilla-based browsers on both the Windows and Linux platforms can use a smart card to generate certificates

RACF 1.13
BPX.UNIQUE.USER

What are You Doing About BPX.UNIQUE.USER?

- Many of us use a FACILITY class rule named **BPX.DEFAULT.USER** which provides a default USS identity (UID and GID) for RACF userids that don't have an OMVS segment. This makes it easier for us when we suddenly have to let hundreds of users who don't have OMVS segments access FTP for example.
- IBM plans to stop supporting **BPX.DEFAULT.USER** after RACF Release 1.13.

RACF 1.13 Summary

What was new with z/OS V1.13 RACF?

- RACF Remote Sharing (RRSF) over TCP/IP
- Identity Propagation extensions
- RACF Support for Elliptic Curve Cryptography (ECC)

What was new with z/OS V1.13 PKI Services?

- Support of DB2 for PKI Services Databases
- Larger Certificate Revocation Lists (CRLs)
- Enhanced support for Web Browsers

Remember: BPX.DEFAULT.USER

RACF 2.1
Heads Up

General RACF 2.1

No specifics as yet – watch for pre-announce at SHARE this week

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

Disclaimer

Certain information in this presentation (slides 17-24) may outline CA's general product direction. This presentation shall not serve to (i) affect the rights and/or obligations of CA or its licensees under any existing or future license agreement or services agreement relating to any CA software product; or (ii) amend any product documentation or specifications for any CA software product. This presentation is based on current information and resource allocations as of February 4, 2013 and **is subject to change or withdrawal by CA at any time without notice**. **The development, release and timing of any features or functionality described in this presentation remain at CA's sole discretion**.

Notwithstanding anything in this presentation to the contrary, upon the general availability of any future CA product release referenced in this presentation, CA may make such release available to new licensees in the form of a regularly scheduled major product release. Such release may be made available to licensees of the product who are active subscribers to CA maintenance and support, on a when and if-available basis. The information in this presentation is not deemed to be incorporated into any contract.

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

THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY. CA assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. **In n**o event will CA be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if CA is expressly advised in advance of the possibility of such damages.

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

- **Role Based Security**
  - Enhanced Model/Archive/Compare commands to include users defined roles
  - Clean-up Role records when a user account is deleted
  - Incorporate Roles in ACF ACCESS command
  - Prevention of changing Role record type
- **Cross-Reference record expansion**
  - X(ROL), X(RGP) and X(SGP) from 4K to 16k
- **Digital Certificates**
  - Movement of internal certificate table to 64-bit storage
  - Unsupported Signature Algorithm checking
  - EDAYS(nn) parameter in Certificate Utility reports

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

- **Symbolic substitution in Dataset Rules**
  - Reduces rule administration by allowing &LID as substitution string
  - The &LID is used on the rule line within the dataset rule set
- **GSO LINKLIST enhancements**
  - System Symbolic substitution allowed as defined in SYS1.PARMLIB (IEASYM)
  - Masking capabilities now permitted for Datasets
- **GSO INFODIR expanded**
  - Limitation of 256 entries doubled to 512
- **Optional use of Cancelled LID for RACROUTE EXTRACTS**
  - Equivalent support for all ESM's
  - Prevents Processes from not working

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

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

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

- **IMS Enhancements**
  - Security for the IMS DBCTL Environment
    - Secures IMS TM (transaction/terminal management) environments
    - Used when data in IMS DB databases access is needed
    - Allows sharing of IMS DB data ensuring data integrity
  - Implementation of '/ACF' command
    - Allows execution of '/ACF' command in IMS OM environment
  - Removal of ACF2 IMS Dependence of IMS Security Macro
    - IBM is eliminating the SECURITY macro

#SHAREorg

SHARE
Technology · Connections · Results

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

SHARE in San Francisco 2013

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

- **Reduce Storage Obtains required**
- **Increase MAX ACID size to 1024K**
  - Allows for larger ownership records, which in turn allows for more permissions to be issued for any given resource.
- **TSSUTIL updates support specific resources and dates**
  - Enable TSSUTIL to report on a specific resource via RESOURCE('resourceName') selection criteria option.
  - Enable continuation characters to allow multi-line report commands, keywords and their parameter lists (i.e. FACILITY)

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

- **ENHANCE TO RPW OPTION (** SSPARAM, TSSNPW, TSSRPW)
  - New control option to allow whether or not to restrict passwords by a prefix or a string in any position in the password
- **Expand COMPARE Command**
- **WHOHAS command output corrections**

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

- **Control MODIFY with CASECAUT**
  - This feature will allow more granular authority checking for the TSS MODIFY command
- **Tracking FACILITY and IBMGROUP usage**
  - CA Cleanup: track the use of both FACILITY and IBMGROUP
- **Digital Certificates**
  - Movement of internal certificate table to 64-bit storage
  - Unsupported Signature Algorithm checking
  - EDAYS(nn) parameter in Certificate Utility reports

#SHAREorg

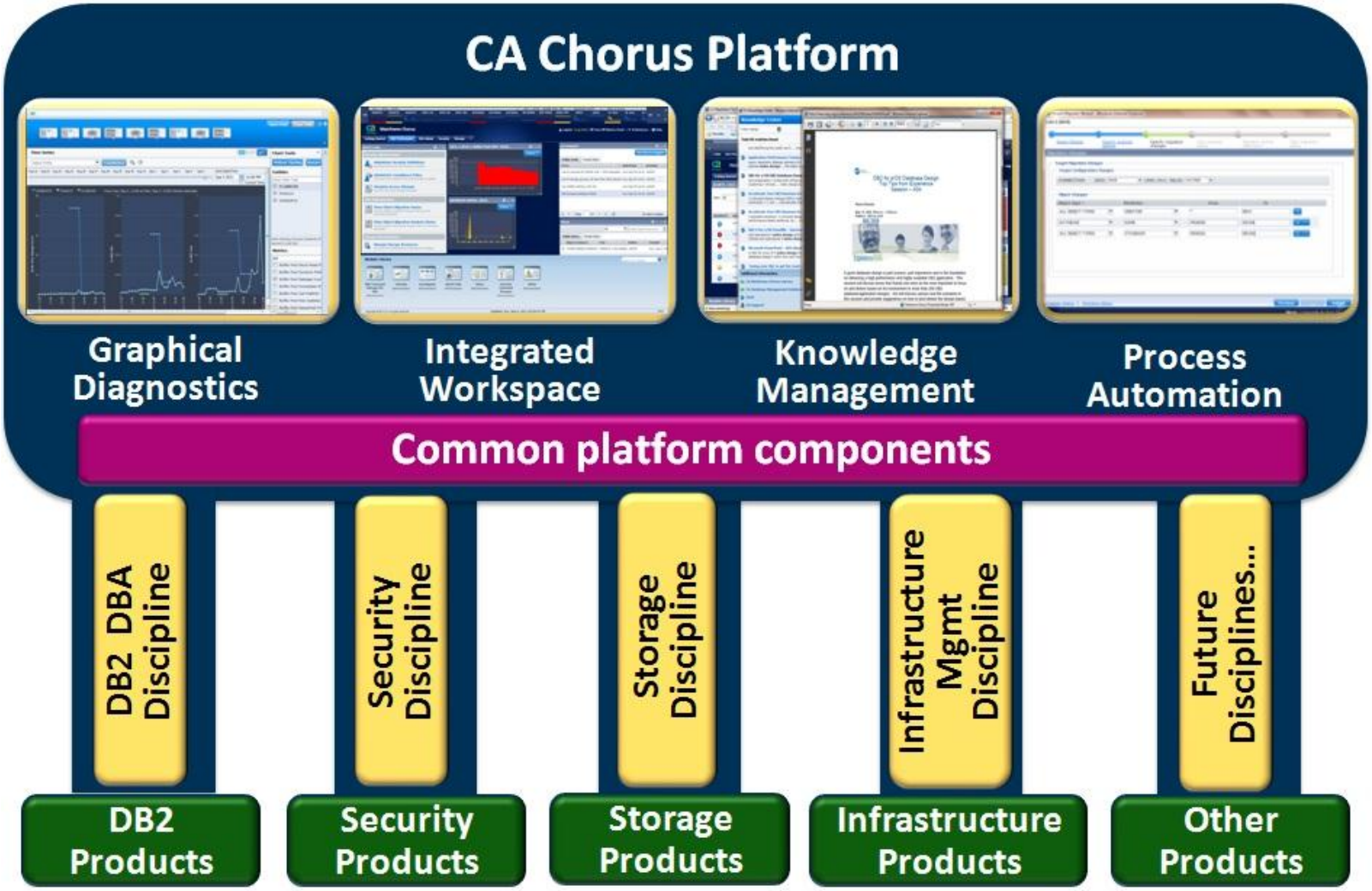
SHARE
Technology · Connections · Results

CA Mainframe Chorus

Security and Compliance Role Improvements in 2.5

SHARE in San Francisco 2013

CA Mainframe Chorus Architecture

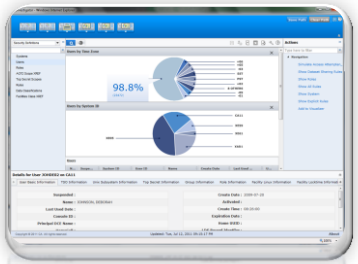


CA Mainframe Chorus
an overview…

SHARE
Technology · Connections · Results

Integrated Workspace

- Singular interaction model
- Fast Learning Curve



Role-Based Navigation

- Matches Job Functions
- Leverage resources across platforms

Graphical Diagnostics

- Data in human readable formats
- Solve problems faster

Knowledge Management

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

Process Automation

- Wizard-like process tools
- Reduces possibility of errors

Improve staff efficiency
CA Chorus vision

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

6 Core Disciplines

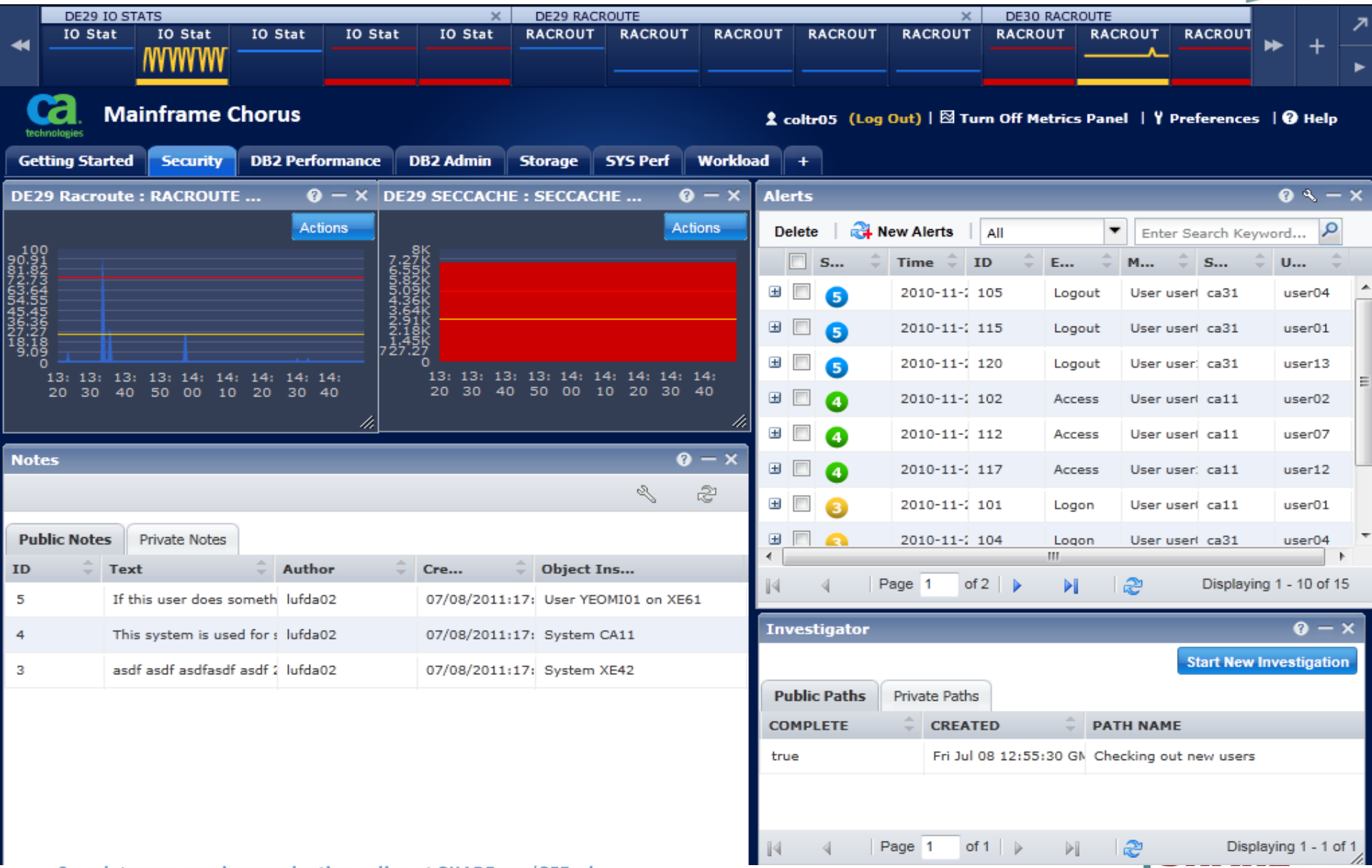
Mainframe Technology Stack

Functional Components	DB2 Database Management
	Security Management
	Storage Management
	Infrastructure Management
	Workload Management
	Systems Management
	Datacom Database Management
	IDMS Database Management
	IMS Database Management
	Operations Management
CCS	Base Common Services Mainframe WS Common Services
	Partner Ecosystem

CA Chorus

- Disciplines
- Collaboration
- Rich Visualization
- Knowledge Management
- Process Automation

CA Mainframe Chorus ~ Security Workspace



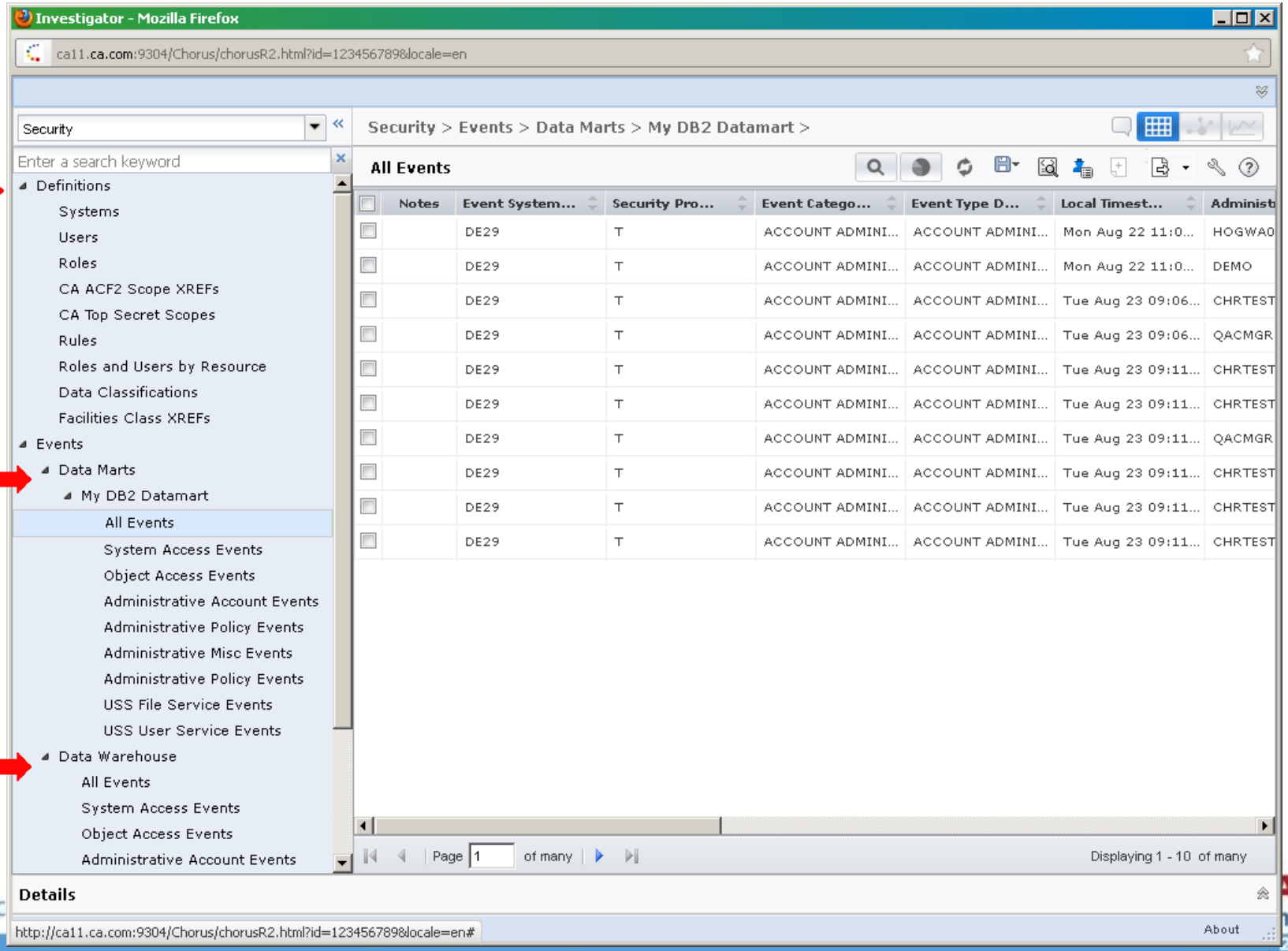
Design goals and architecture

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

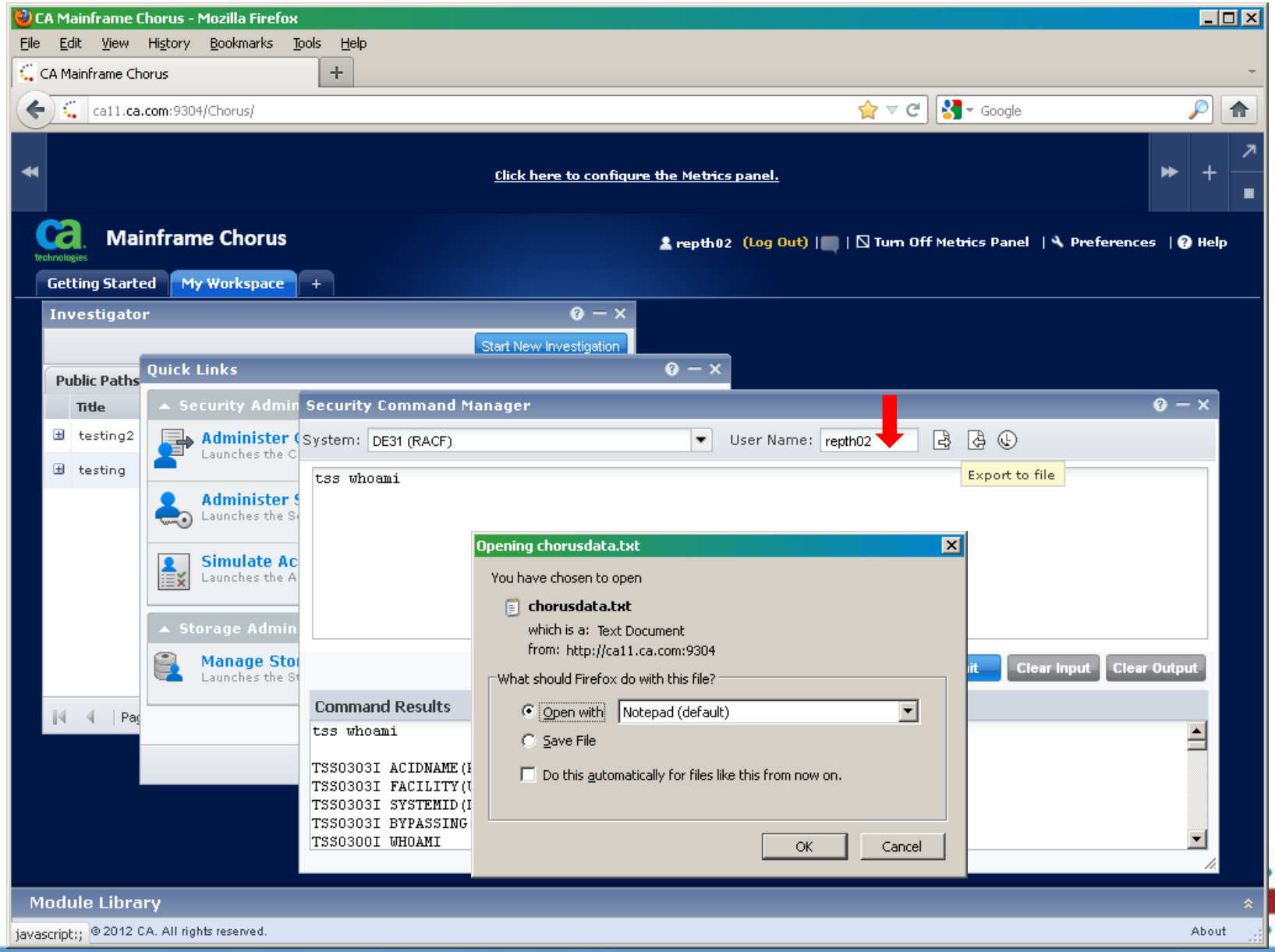
	Knowledge Center	Investigator	Metrics Panel	Security Command Manager	Quick Links	Notes	Security Alerts
ACF2 and Top Secret							
CIA database	x	x				x	
Admin	x				x		
Security command line*	x			x			
ACFTEST/TSSSIM	x				x		
Statg	x	x	x				
Compliance Manager							
Policy*	x				x		
Events*	x	x				x	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

* Includes support for RACF

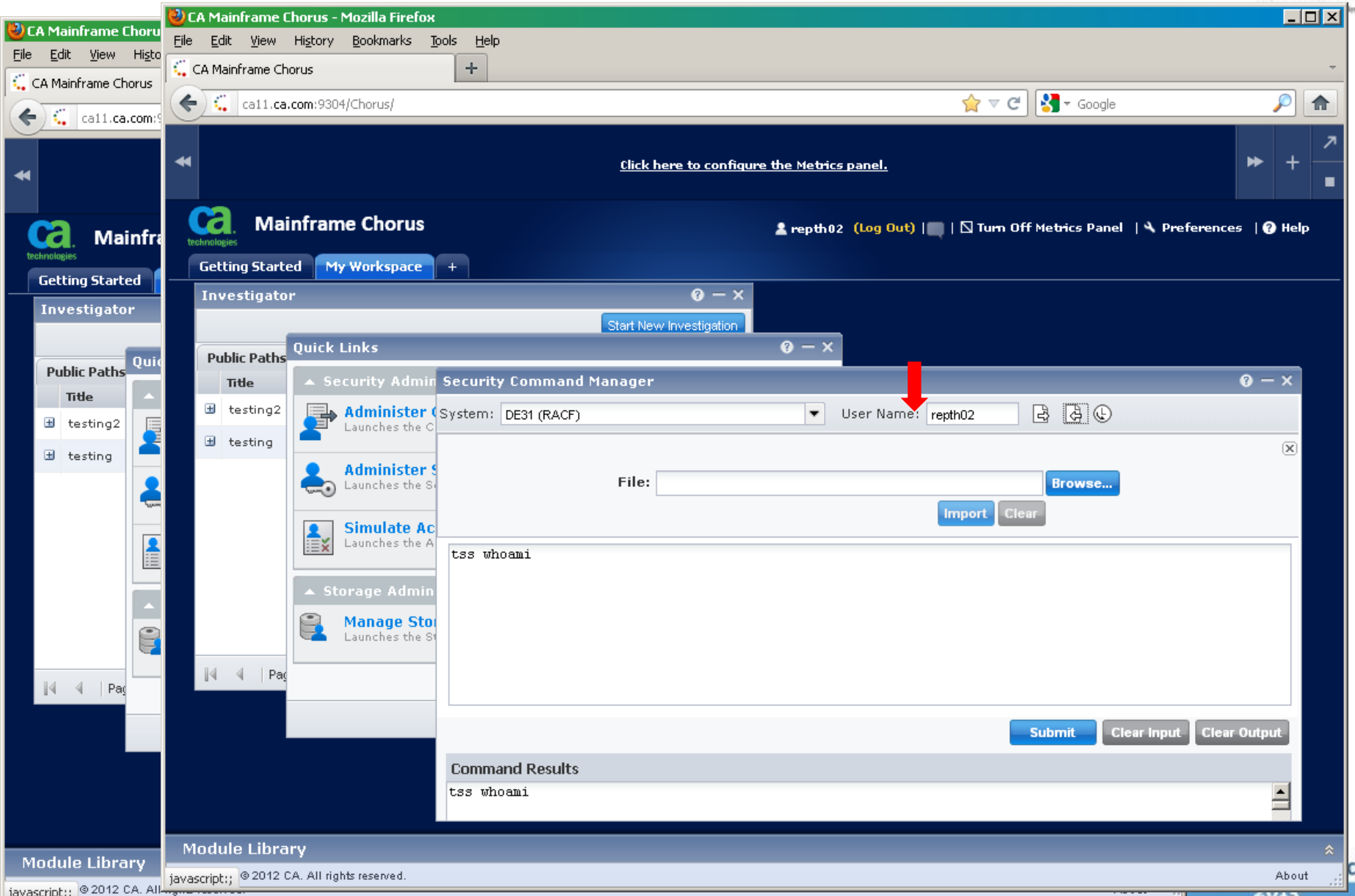
Datacom CIA, Data mart(s), and Warehouse



Export from Security Command Manager



Import Into Security Command Manager



#SHAREorg

SHARE

Open Discussion – Q&A

Thank you!

Session #12264

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

SHARE in San Francisco 2013