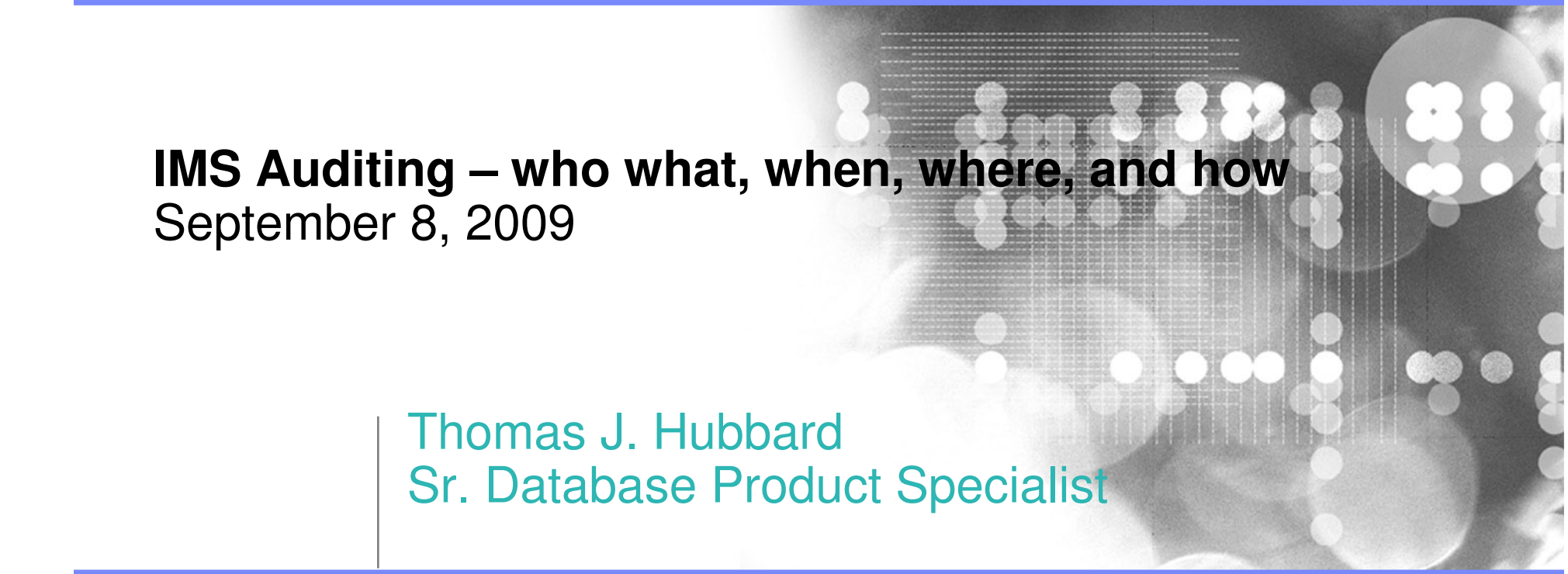
IBM IMS Audit Management Expert for z/OS V1.2



IMS Auditing – who what, when, where, and how

September 8, 2009

Thomas J. Hubbard
Sr. Database Product Specialist

© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

OVERVIEW

- **IMS Audit Management Expert for z/OS**
  - Provides a comprehensive auditing solution that reduces the cost of compliance through automation, centralization, and segregation of duties
  - Simplifies the collection of audit data through automation
    - Reduces manual efforts and increases productivity
  - Provides centralization of the audit data by collecting and correlating data access information from a variety of IMS and SMF resources
    - Removes the difficulty of gathering data from multiple data sources by centralizing audit data
    - Auditors can easily get audit information while requiring fewer resources
    - Data from different sources is presented in a consistent way

© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

OVERVIEW

- **IMS Audit Management Expert for z/OS**
  - Allows for segregation of duties between auditors and DBA's
    - Increases the integrity of the audited data
    - Removes the opportunity for data tampering because reports are no longer provided by the personnel companies need to audit
  - Saves time and effort by eliminating manual auditing processes
  - Facilitates common auditing tasks
    - determining who updated a particular object
    - time frame
    - monitoring access to specific objects
  - Allows auditors to obtain information
    - without being defined as IMS users
    - work without extensive interaction with Data Base and System Administrators
    - Auditors will not be able to directly manipulate IMS resources

© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IMS Audit Management Expert for z/OS

- **Data collection**
  - Collection and reporting of READ (GETS), INSERT, UPDATE and DELETE accesses to databases
  - Ability to audit and report on READ, INSERT, UPDATE, and DELETE calls on specific database segments
    - READ and DELETE calls retain the concatenated key of the audited segment
    - UPDATE and INSERT calls retain the segment concatenated key as well as the segment data, as found in the DLI call I/O area

© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IMS Audit Management Expert for z/OS

- **Data collection**
  - IMS Audit Management Expert Agent
    - Responsible for administrating the collection of data to be audited
    - The agent may collect data from
      - a single IMS system
      - multiple IMS systems that share a set of RECON datasets
      - multiple IMS systems using diverse RECON datasets
    - Populates the DB2 repository with audited data collected
    - Provides audit collection definition to the activity monitors and collectors
      - which databases / segments should be audited
      - the level of auditing that should be done
    - Agent communicates with the Activity Monitors and Data Collectors by using subtasks that execute in their own address spaces as started tasks

© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IMS Audit Management Expert for z/OS

- **Data collection**
  - IMS Online and Batch Activity Monitors
    - Interface with the IMS DL/I language call analyzer module (DFSDLA0) and the IMS/VS/FP Inter-region Communications Controller (DBFIRC10)
    - In an online IMS environment
      - the activity monitor is activated when an INIT call is made to the IMS logger Exit (DFSFLGX0)
      - remain active until a DFSFLGX0 TERM call is made
    - In an IMS batch (DLI/DBB) environment
      - the activity monitor is activated when the IMS Batch exit (DFSISVI0) is called
      - remain active until the batch job terminates
    - The IMS Online and Batch Activity Monitors communicate with the agent via an IMS Online and Batch data collector
      - Transports data to the agent using z/OS System log streams
      - Audited data from the batch and online monitors use individual and separate System log-streams to send data to the agent

© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IMS Audit Management Expert for z/OS

- **Data collection**
  - z/OS System Logger
    - Used to collect audit data from IMS online and DLI/DBB batch jobs
    - Must define structures and log streams for IMS Audit Management Expert to write audit data z/OS System Logger
      - Add CFRM structures
        - > DEFINE STRUCTURE NAME(AUE_BATCH_JRN)
        - > DEFINE STRUCTURE NAME(AUE_ONLINE_JRN)
      - Add log streams to the CFRM environment
        - > DEFINE LOGSTREAM NAME(AUE.BATCH.JRN)
        - > DEFINE LOGSTREAM NAME(AUE.ONLINE.JRN)
    - Update Policy in CFRM (COUPLING FACILITY RESOURCE MANAGER)
    - ACTIVATE THE POLICY
      - SETXCF START,POLICY,TYPE=CFRM,POLNAME=CFRMPOL1

© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IMS Audit Management Expert for z/OS

- **Data collection**
  - IMS Online and Batch Data Collectors
    - Reads audited data from the log-streams, and present it to the agent ready for insertion into the DB2 repository
  - IMS Archive Log Dataset Collectors
    - determines the IMS Archived Log datasets (SLDS) needed to be read in order to collect
      - IMS subsystem starts and stops
      - users signing on to an IMS subsystem
      - PSB and DBD status changes
      - DLI Get, Insert, Delete and Update activity at the database level
  - SMF DUMP Data Collectors
    - reads a subset of SMF records from SMF DUMP datasets to determine if datasets associated with audited IMS databases were read, written, deleted or renamed outside the control of IMS
    - associated dataset type include database datasets, Image copy datasets IMS log datasets and RECON datasets
  - Common Storage Management Utility
    - Not a collector
    - Provides the agent with a method of updating ECSA storage on all LPARS of a Sysplex from a single z/OS image
    - The ESCA storage contains audit criteria used by the IMS Online and Batch Activity Monitors and Data Collectors to determine which IMS systems are to be audited

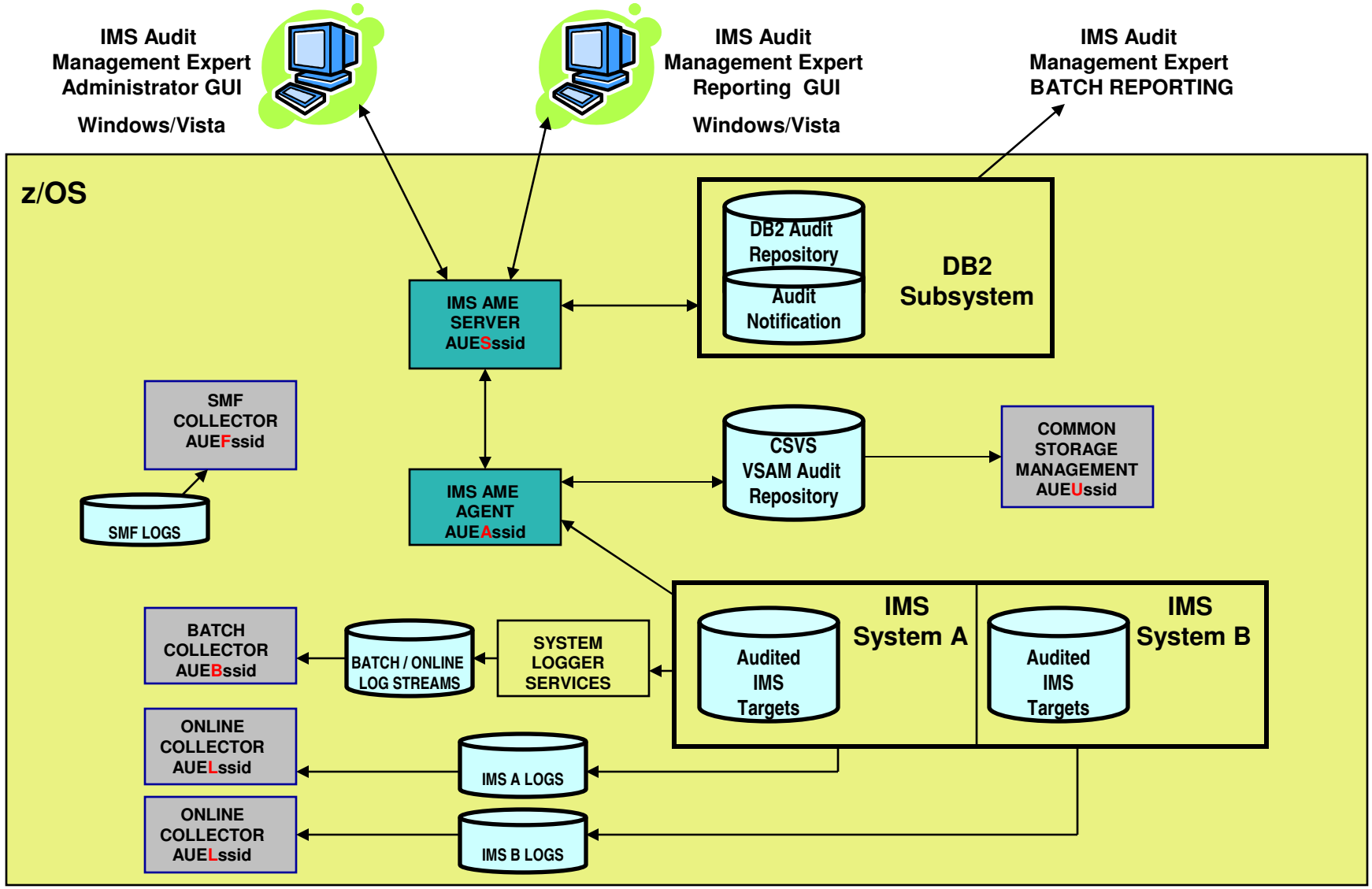
© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IMS Audit Management Expert for z/OS

- **The IMS Audit Management Expert Audit Repository**
  - DB2 Database
  - Stores IMS configuration data
    - Added/updated via Admin GUI
  - Stores audit data collected by the agent
    - Report GUI and Batch Reports display audit data from Repository
- **The IMS Audit Management Expert Server**
  - Central control point for IMS Audit Management Expert
  - Provides the connection for the Administration and Reporting GUIs
  - Runs functions to create summary reports of collected audit data
    - Summary Reports created at time interval set by configuration

© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IMS Audit Management Expert Architecture



© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IMS Audit Management Expert for z/OS

- **REPORTING of audit data**
  - GUI Reporting interface
    - Provides auditors with flexible options for examining the data in the audit repository
    - Summary and detail reports
    - Report filtering
    - Graphical and tabular reports
      - Export data grid values directly to Excel
      - Zoom data grid cells, to view data more easily
      - Search capability for data grid cells
  - Batch Reports
    - Generate reports by
      - USERID, DATABASE, SEGMENT, TRANCODE, PSB, JOBNAME
      - Date Range with STARTDATE, ENDDATE
      - Masking and control card omission allows desired report content
    - Provides capability to view segment concatenated key and segment data in it's raw format

© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IMS Audit Management Expert for z/OS

- **Automated audit notification**
  - Exceptions exceeding CRITICAL or WARNING threshold values
    - Thresholds values are set by individual Report users
  - Trigger Action
    - Email notification with message to selected email addresses
    - WTO to selected TSO USERids

© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IMS Audit Management Expert for z/OS

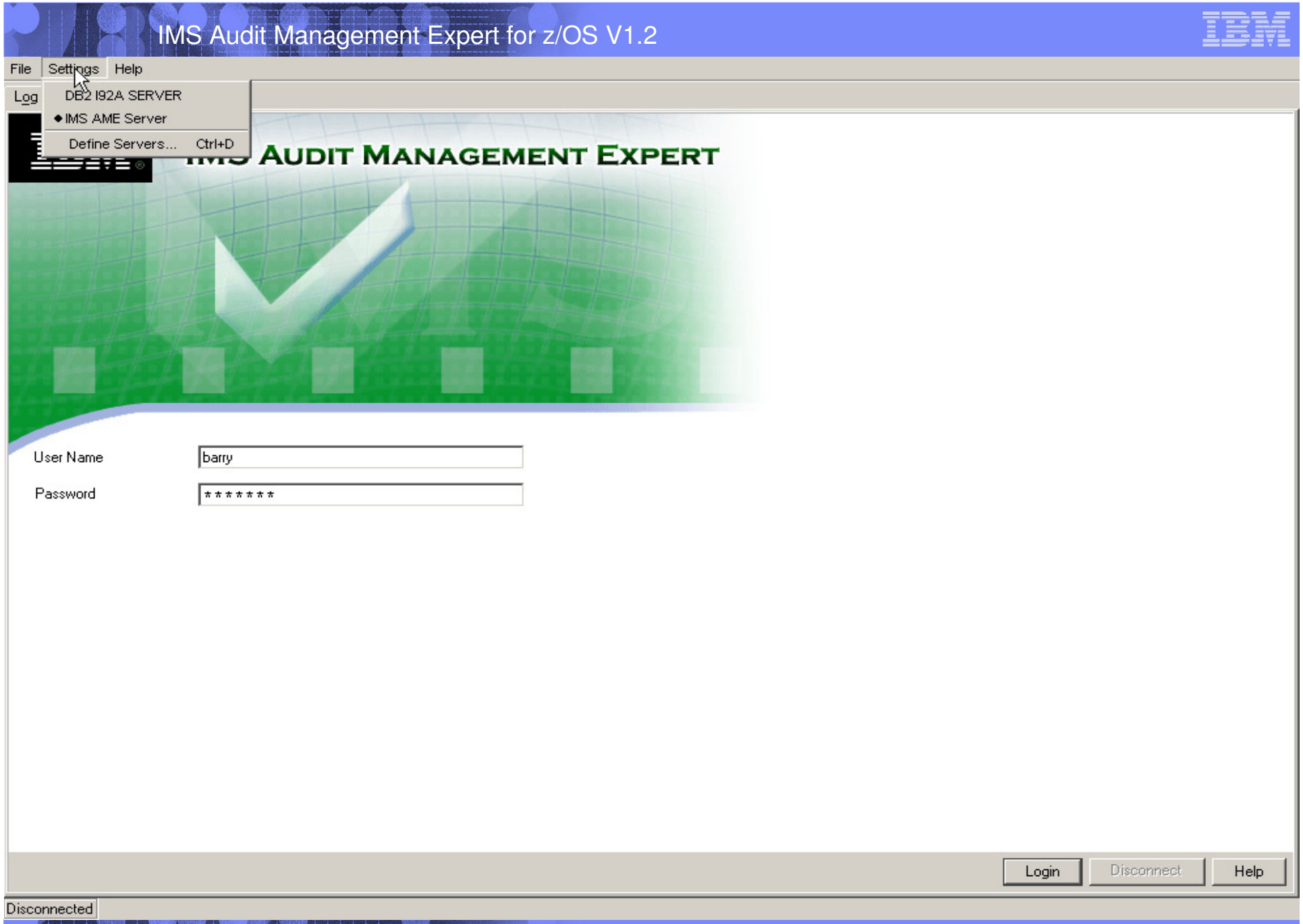
- **Administration User Interface GUI**
  - Provides administrators with flexible control options
    - User management
    - Auditing profile management
      - Ability to define what will be targets of auditing
      - Ability to set auditing rules for different levels of auditing
      - Ability to filter auditing at the database level as well as segment level
      - The inclusion of PSBs within a rule, to audit all databases within the PSB at the database level
    - Reporting authorizations

© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IBM IMS Audit Management Expert for z/OS V1.2

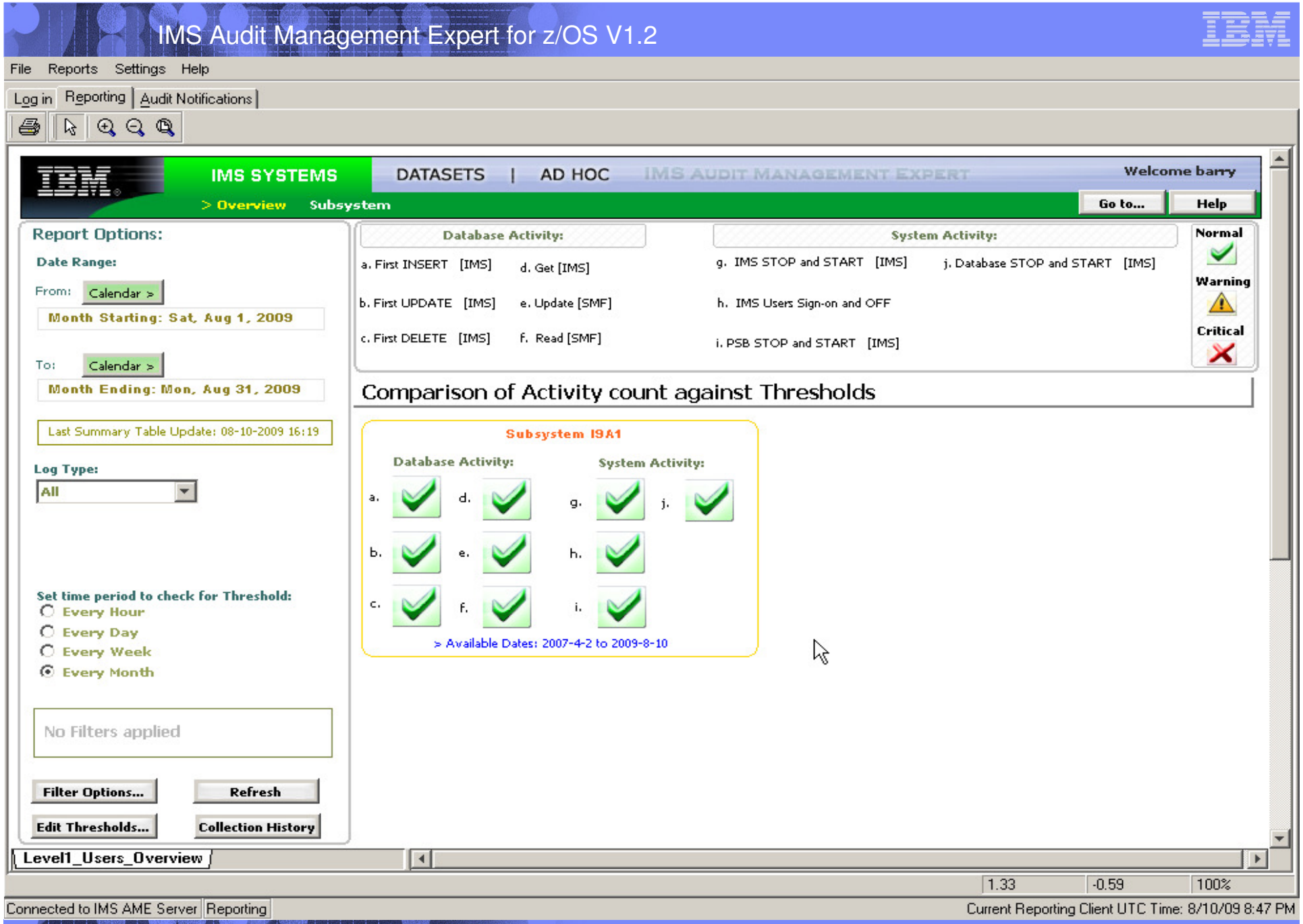
Report GUI sample

© 2009 IBM Corporation
© 2009 Rocket Software, Inc.



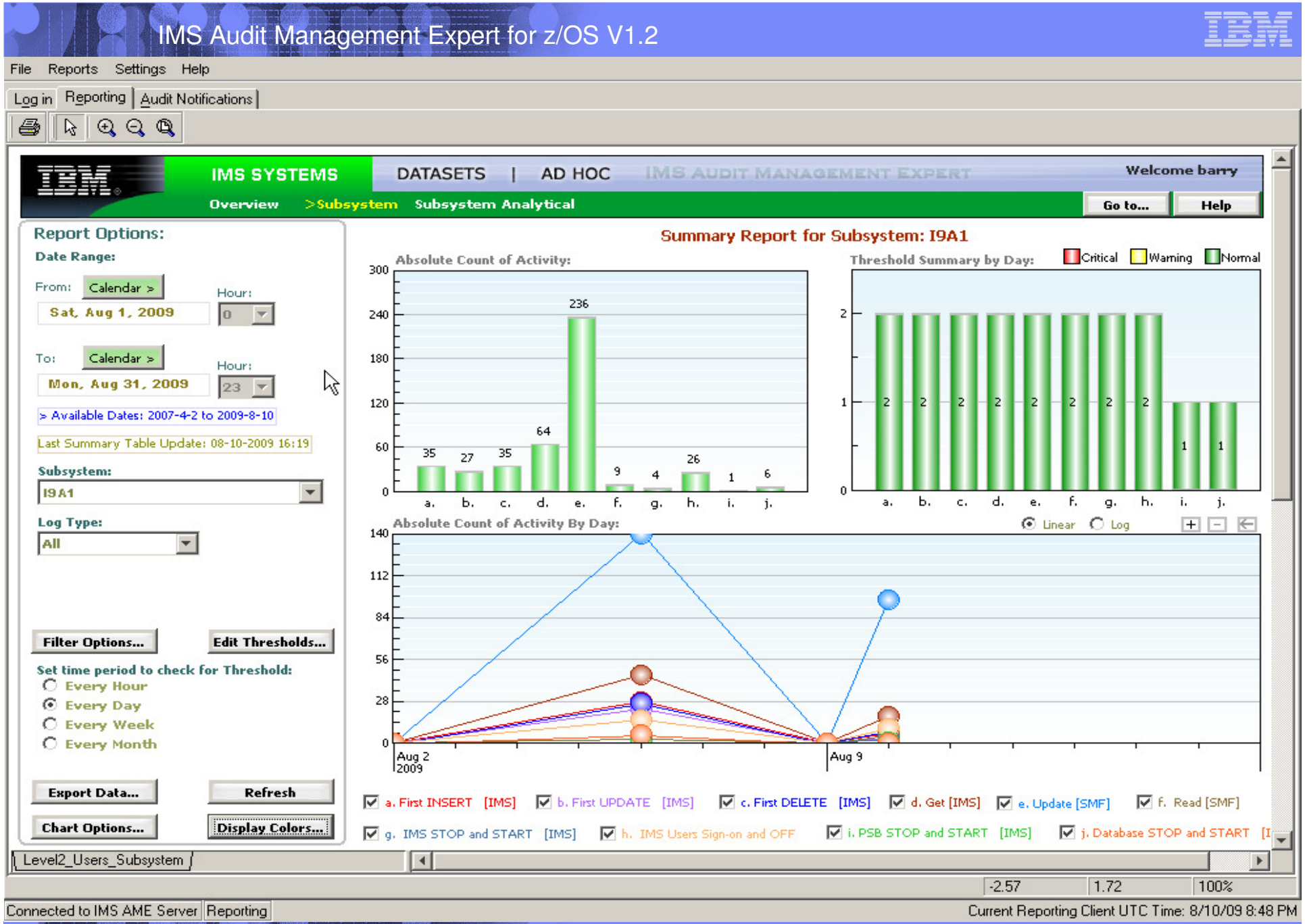
© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IMS Audit Management Expert for z/OS V1.2



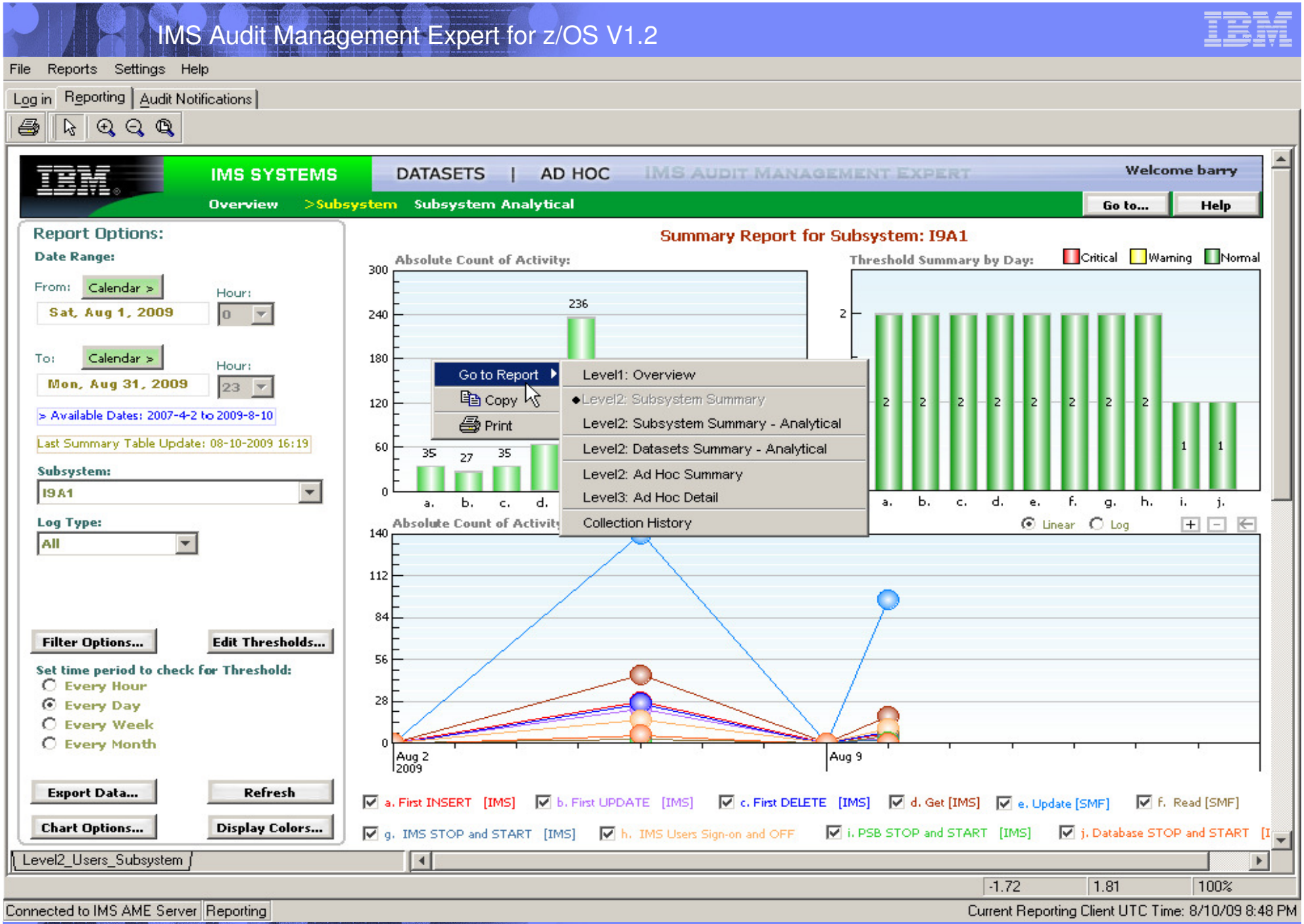
© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IMS Audit Management Expert for z/OS V1.2



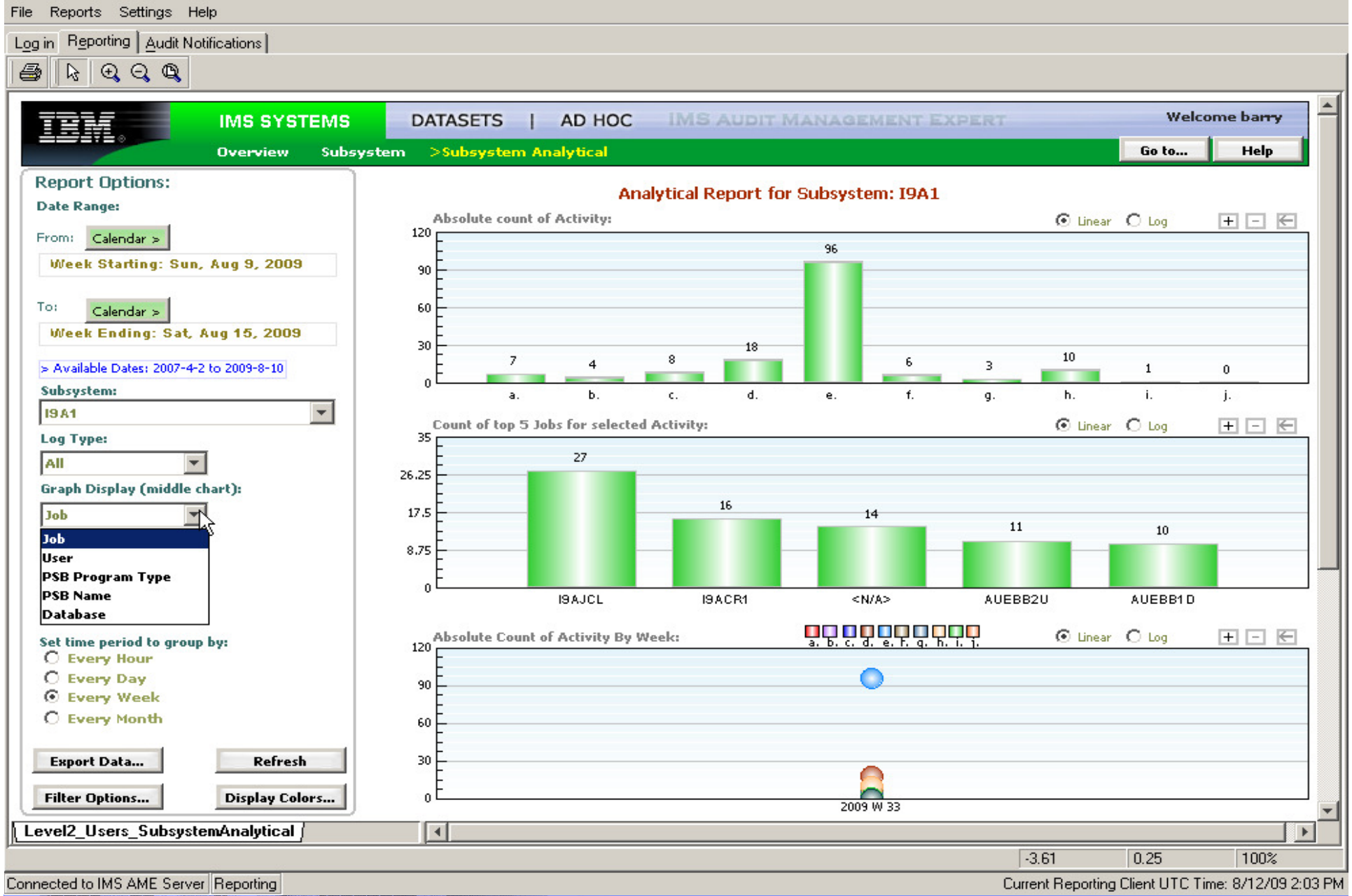
© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IMS Audit Management Expert for z/OS V1.2



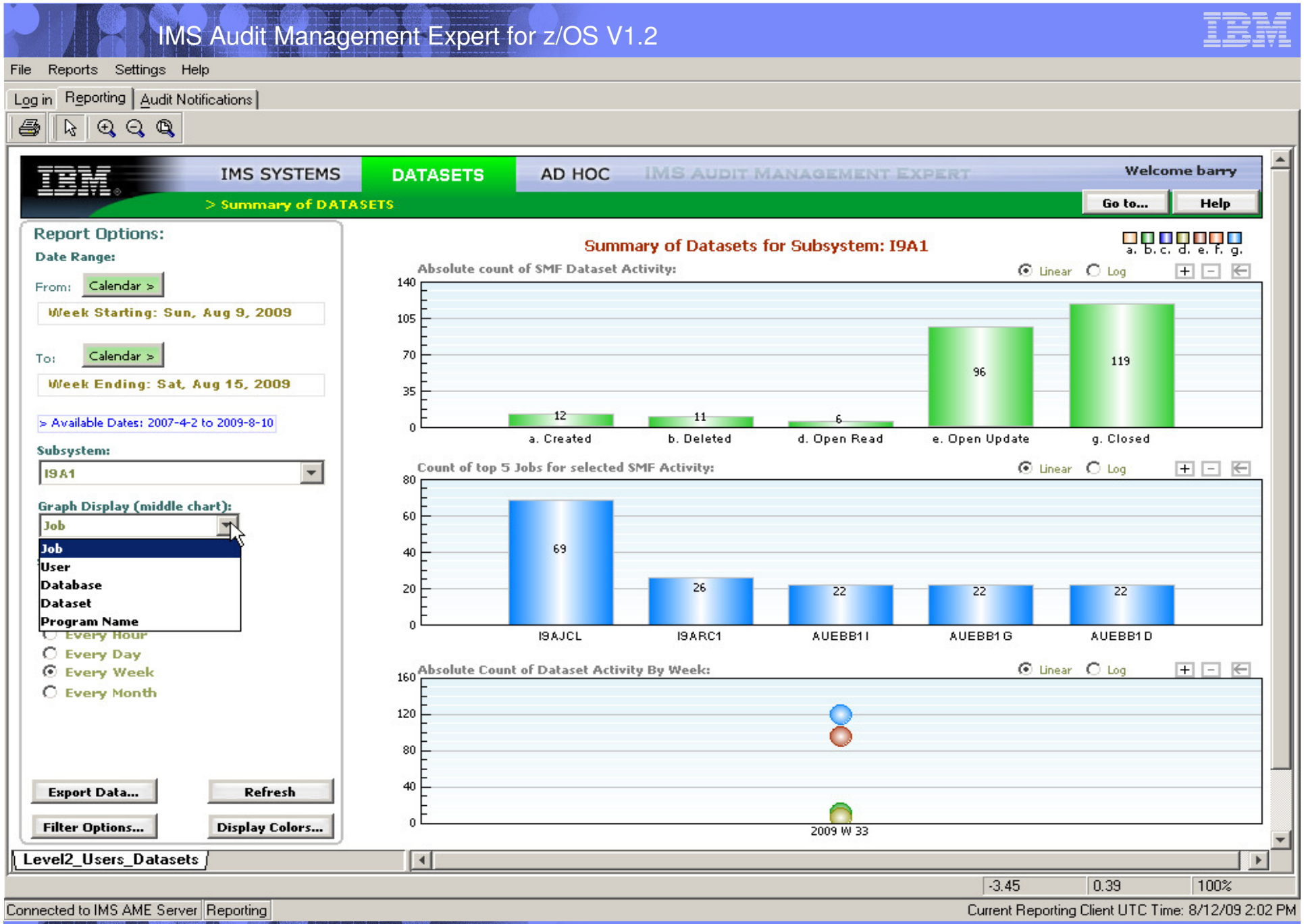
© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IMS Audit Management Expert for z/OS V1.2



© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IMS Audit Management Expert for z/OS V1.2



© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

Option

Record Count: 64

Display all columns

Default SMF Columns

✓ Default IMS Columns

✓ ROW

✓ DESCRIPTION

✓ EVENT_TYPE

✓ START_TIME

✓ END_TIME

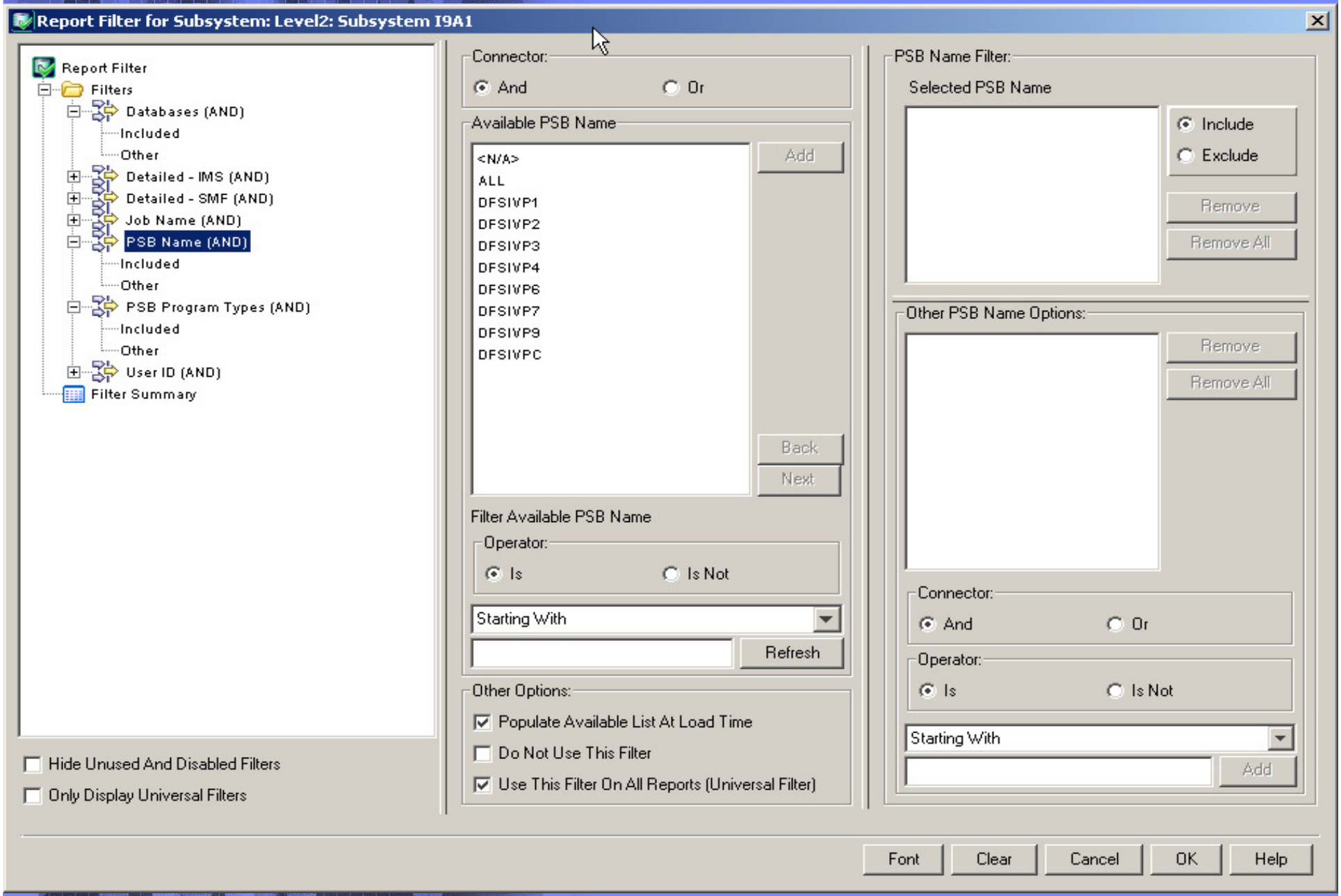
✓ IMS_SUBSYSTEM

✓ SYSTEM_ID

		EVENT_TYPE	START_TIME	END_TIME	IMS_SUBSYSTEM	SYSTEM_ID	JOB_NAME	JOB_NUMBER	S
		IMS050	2009-08-06 21:00:47...	2009-08-06 21:00:5...	I9A1	AUEBB1G	AUEBB1G	JOB09348	G
		IMS050	2009-08-06 21:01:22...	2009-08-06 21:01:2...	I9A1	AUEBB1I	AUEBB1I	JOB09349	G
		IMS050	2009-08-06 21:01:42...	2009-08-06 21:01:4...	I9A1	AUEBB1D	AUEBB1D	JOB09350	G
		IMS050	2009-08-06 21:02:06...	2009-08-06 21:02:1...	I9A1	AUEBB1U	AUEBB1U	JOB09351	G
		IMS050	2009-08-06 21:02:52...	2009-08-06 21:03:2...	I9A1	AUEBB1U	AUEBB1U	JOB09352	G
		IMS050	2009-08-06 21:03:50...	2009-08-06 21:03:5...	I9A1	AUEBB1S	AUEBB1S	JOB09353	G
		IMS050	2009-08-06 21:13:13...	2009-08-06 21:13:1...	I9A1	AUEBB2I	AUEBB2I	JOB09358	G
		IMS050	2009-08-06 21:13:51...	2009-08-06 21:13:5...	I9A1	AUEBB2D	AUEBB2D	JOB09359	G
		IMS050	2009-08-06 21:14:06...	2009-08-06 21:14:1...	I9A1	AUEBB2U	AUEBB2U	JOB09360	G
		IMS050	2009-08-06 21:14:26...	2009-08-06 21:14:3...	I9A1	AUEBB2S	AUEBB2S	JOB09361	G
		IMS050	2009-08-06 21:16:14...	2009-08-06 21:16:4...	I9A1	AUEBB2U	AUEBB2U	JOB09364	G
		IMS050	2009-08-06 21:47:33...	2009-08-06 21:47:3...	I9A1	I9A1	I9AM11		RE
		IMS050	2009-08-06 21:47:57...	2009-08-06 21:47:5...	I9A1	I9A1	I9AM11		RE
		IMS050	2009-08-06 21:48:16...	2009-08-06 21:48:1...	I9A1	I9A1	I9AM11		RE
		IMS050	2009-08-06 21:48:21...	2009-08-06 21:48:2...	I9A1	I9A1	I9AM11		RE
		IMS050	2009-08-06 21:48:35...	2009-08-06 21:48:3...	I9A1	I9A1	I9AM11		RE
		IMS050	2009-08-06 21:48:37...	2009-08-06 21:48:3...	I9A1	I9A1	I9AM11		RE
		IMS050	2009-08-06 21:50:24...	2009-08-06 21:50:2...	I9A1	I9A1	I9AM11		RE
34	SEG GET CALL (IMS050 - 70)	IMS050	2009-08-06 21:50:33...	2009-08-06 21:50:3...	I9A1	I9A1	I9AM11		RE
35	SEG GET CALL (IMS050 - 70)	IMS050	2009-08-06 21:50:43...	2009-08-06 21:50:4...	I9A1	I9A1	I9AM11		RE
36	SEG GET CALL (IMS050 - 70)	IMS050	2009-08-06 21:50:46...	2009-08-06 21:50:4...	I9A1	I9A1	I9AM11		RE
37	SEG GET CALL (IMS050 - 70)	IMS050	2009-08-06 21:51:49...	2009-08-06 21:51:4...	I9A1	I9A1	I9AM11		
38	SEG GET CALL (IMS050 - 70)	IMS050	2009-08-06 21:51:52...	2009-08-06 21:51:5...	I9A1	I9A1	I9AM11		
39	SEG GET CALL (IMS050 - 70)	IMS050	2009-08-06 21:52:36...	2009-08-06 21:52:3...	I9A1	I9A1	I9AM11		RE
40	SEG GET CALL (IMS050 - 70)	IMS050	2009-08-06 21:52:43...	2009-08-06 21:52:4...	I9A1	I9A1	I9AM11		RE
41	SEG GET CALL (IMS050 - 70)	IMS050	2009-08-06 21:52:59...	2009-08-06 21:52:5...	I9A1	I9A1	I9AM11		RE
42	SEG GET CALL (IMS050 - 70)	IMS050	2009-08-06 21:53:02...	2009-08-06 21:53:0...	I9A1	I9A1	I9AM11		RE
43	SEG GET CALL (IMS050 - 70)	IMS050	2009-08-06 21:58:41...	2009-08-06 21:58:4...	I9A1	I9A1	I9AF11	JOB09329	IFF
44	SEG GET CALL (IMS050 - 70)	IMS050	2009-08-06 21:58:47...	2009-08-06 21:58:4...	I9A1	I9A1	I9AF11	JOB09329	IFF
45	SEG GET CALL (IMS050 - 70)	IMS050	2009-08-06 21:58:58...	2009-08-06 21:58:5...	I9A1	I9A1	I9AF11	JOB09329	IFF
46	SEG GET CALL (IMS050 - 70)	IMS050	2009-08-06 21:59:05...	2009-08-06 21:59:0...	I9A1	I9A1	I9AF11	JOB09329	IFF
47	SEG GET CALL (IMS050 - 70)	IMS050	2009-08-10 15:11:51...	2009-08-10 15:11:5...	I9A1	I9A1	I9AM11		RE
48	SEG GET CALL (IMS050 - 70)	IMS050	2009-08-10 15:12:13...	2009-08-10 15:12:1...	I9A1	I9A1	I9AM11		RE

Copy | Export | Zoom | Search | Cancel | Columns | Close | Help

© 2009 IBM Corporation
© 2009 Rocket Software, Inc.



© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IMS Audit Management Expert for z/OS V1.2

File Settings Help

Log in | Reporting | Audit Notifications

Notifications:

Name	Description	Type	Created	Owner	Next Scheduled	Notification Enabled	Subsystem	Time Range From	Time Range To	Run Count	Critical Count	Warnir Count
barry1	first notificatio...	Standard	7/20/09 8:43...	barry	7/20/09 9:00...	☑	All Subsystems	4/1/07 12:00...	8/1/09 12:00...	15	6	7
barry1	test on reads	Standard	7/23/09 9:39...	barry	7/24/09 8:00...	☑	All Subsystems	7/1/09 12:00...	8/1/09 12:00...	1	1	0
barry3	test the good ...	Standard	7/30/09 12:4...	barry	7/31/09 8:00...	☑	All Subsystems	7/26/09 12:0...	8/2/09 12:00...	0	0	0

Quick Filter

Name like [ ] Refresh

- (•) Show All Notifications
- ( ) Show only enabled Notifications
- ( ) Show only disabled Notifications
- ( ) Show only Notifications with warnings

Selected Notification History

Run Date	Result	Duration (Seconds)	Time Range From	Time Range To	Messages
8/10/09 9:49 AM	Critical	2	4/1/07 12:00 AM	7/31/09 11:59 PM	1
8/7/09 7:57 AM	Critical	1	4/1/07 12:00 AM	7/31/09 11:59 PM	1
8/6/09 4:29 PM	Critical	1	4/1/07 12:00 AM	7/31/09 11:59 PM	1
8/6/09 1:48 PM	Critical	2	4/1/07 12:00 AM	7/31/09 11:59 PM	1
7/30/09 10:54 AM	Critical	1	4/1/07 12:00 AM	7/31/09 11:59 PM	1
7/29/09 7:05 PM	Critical	16	4/1/07 12:00 AM	7/31/09 11:59 PM	1
7/27/09 9:26 AM	Warning	1	4/1/07 12:00 AM	7/31/09 11:59 PM	1
7/24/09 7:35 AM	Warning	3	4/1/07 12:00 AM	7/31/09 11:59 PM	1
7/23/09 1:33 PM	Warning	3	4/1/07 12:00 AM	7/31/09 11:59 PM	1
7/23/09 8:50 AM	Warning	1	4/1/07 12:00 AM	7/31/09 11:59 PM	1
7/22/09 5:08 PM	Warning	1	4/1/07 12:00 AM	7/31/09 11:59 PM	1
7/22/09 3:35 PM	Warning	1	4/1/07 12:00 AM	7/31/09 11:59 PM	1
7/21/09 9:58 AM	Warning	1	4/1/07 12:00 AM	7/31/09 11:59 PM	1
7/20/09 5:04 PM	Normal	1	4/1/07 12:00 AM	7/31/09 11:59 PM	1
7/20/09 9:00 AM	Normal	1	4/1/07 12:00 AM	7/31/09 11:59 PM	1

View Graphical Report... | View Messages... | Delete

Create Notification | Clone Notification | Enable Notification | Disable Notification | View Notification | Delete Notification | Run Notification...

Current Notification Server Time: 8/10/09 5:06 PM

Connected to IMS AME Server | Audit Notifications

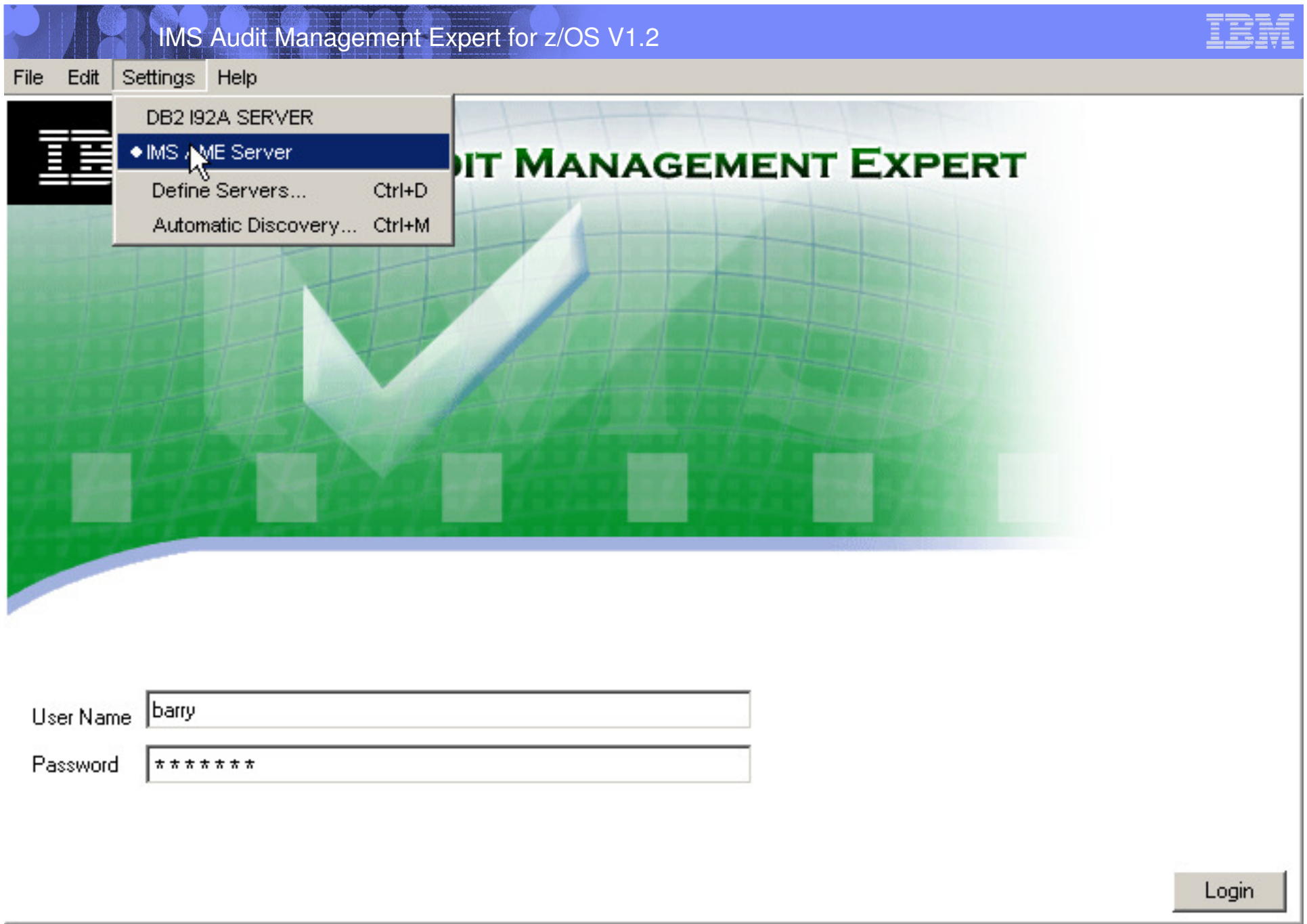
Current Reporting Client UTC Time: 8/10/09 9:06 PM

© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IBM IMS Audit Management Expert for z/OS V1.2

Administration GUI sample
Configuration of IMS, Agent and Collections

© 2009 IBM Corporation
© 2009 Rocket Software, Inc.



© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

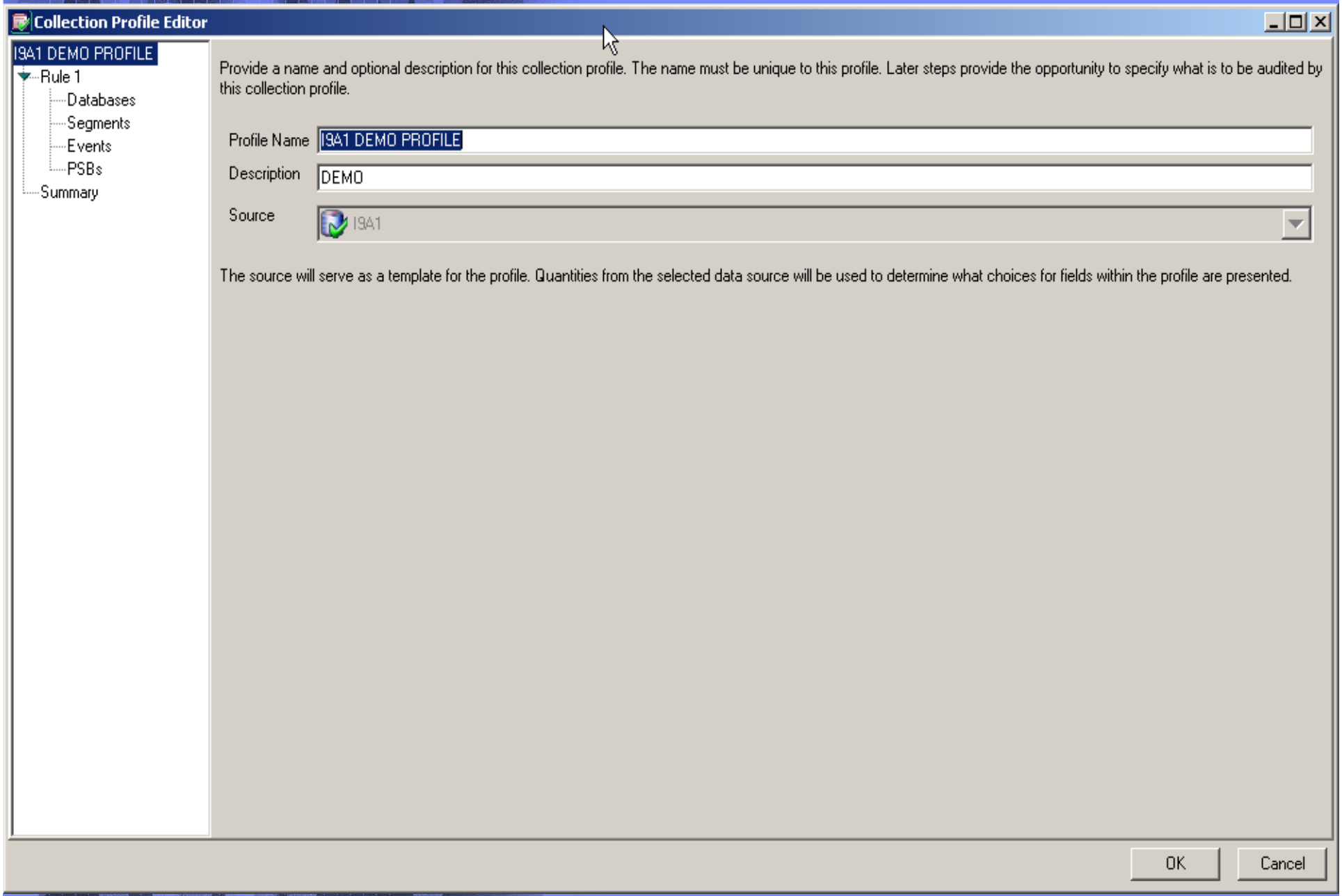
File Edit Settings Help

Users | Groups | IMSs | Agents | Collection Profiles | Collections | Authorizations | Repository

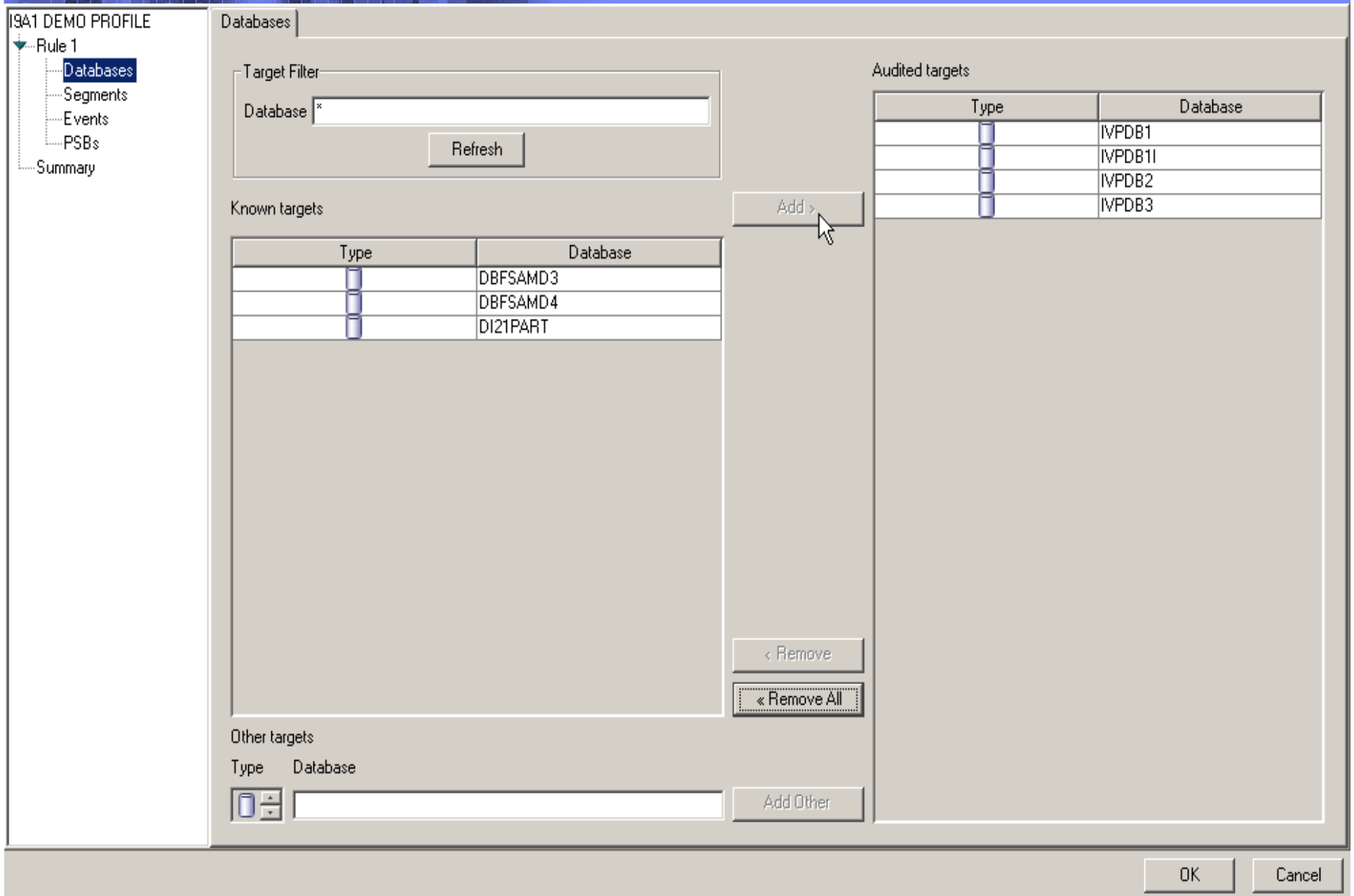
Profile Name	Description	Last Modified	Active Collections
I9A1 DEMO PROFILE	DEMO	2009-07-17 09:09:28	1

Add | Edit | Clone | Delete | Refresh

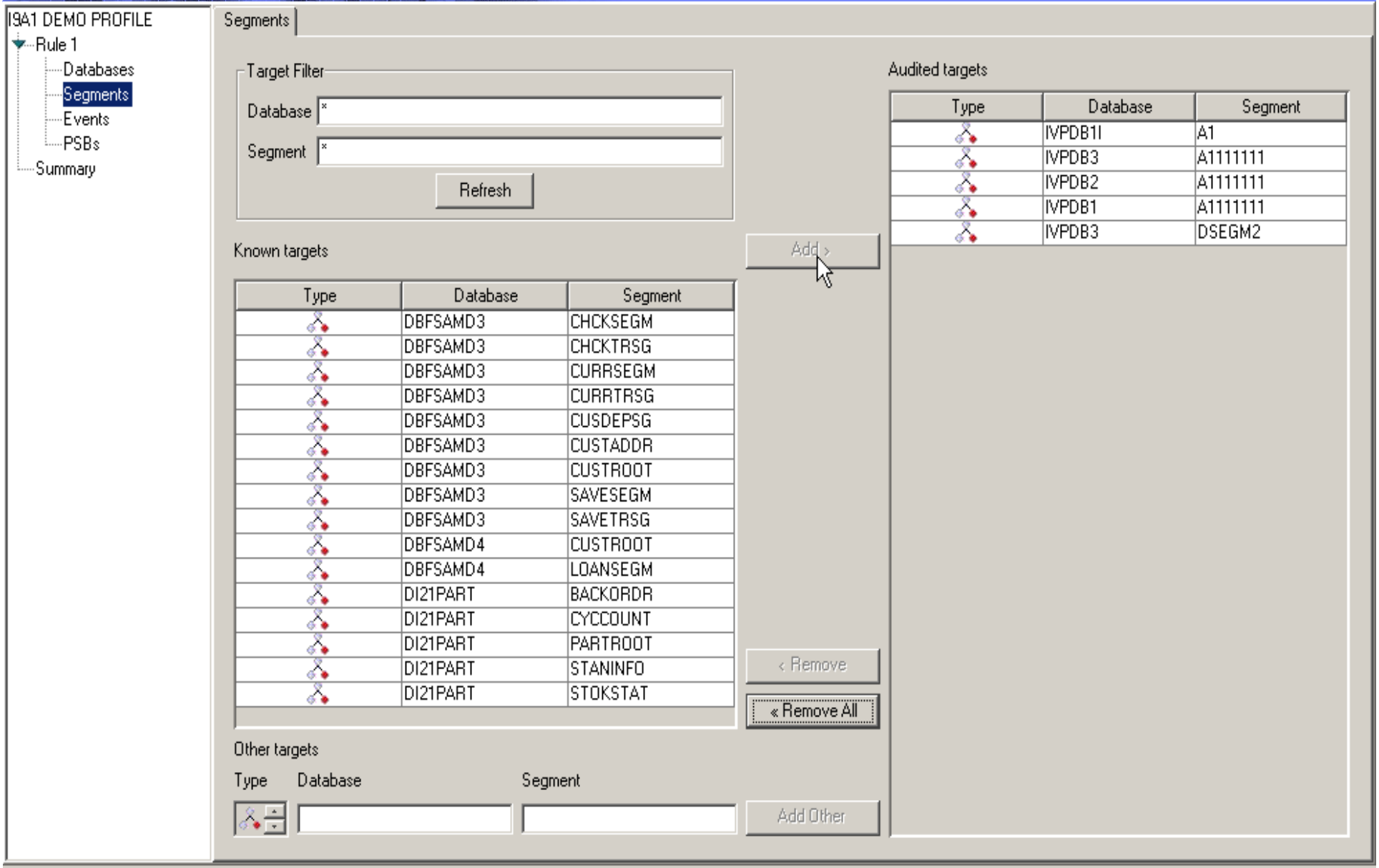
© 2009 IBM Corporation
© 2009 Rocket Software, Inc.



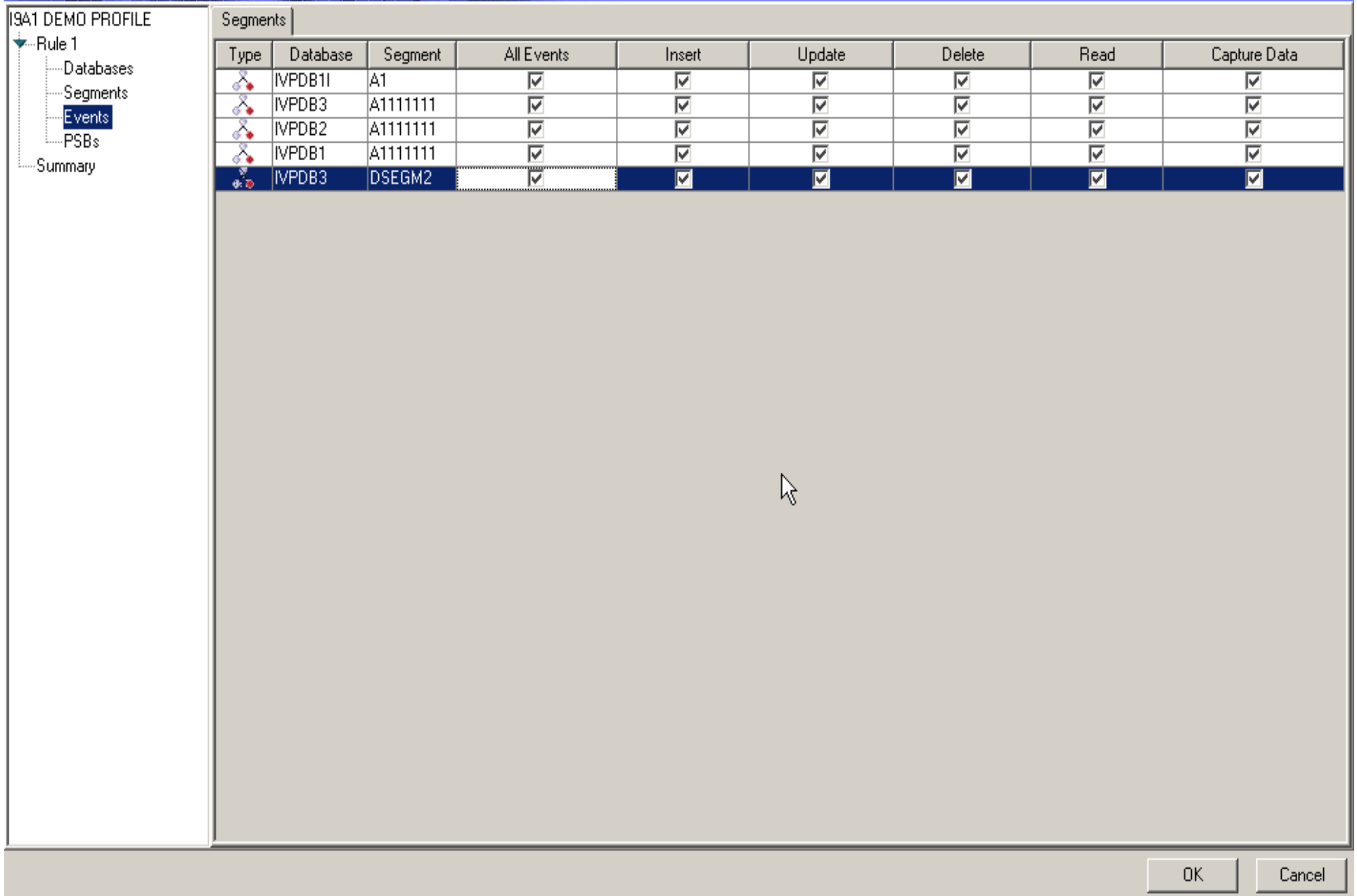
© 2009 IBM Corporation
© 2009 Rocket Software, Inc.



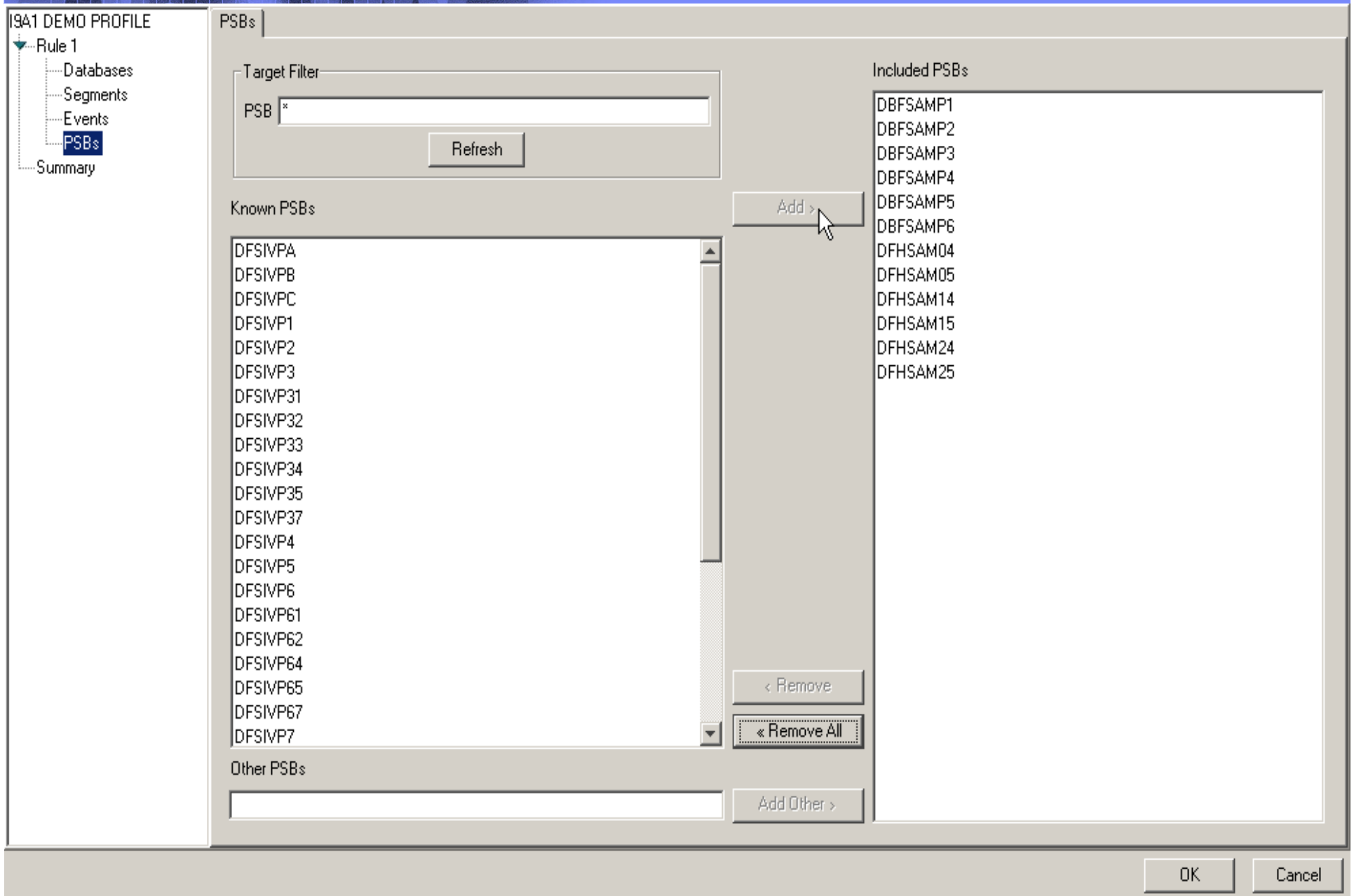
© 2009 IBM Corporation
© 2009 Rocket Software, Inc.



© 2009 IBM Corporation
© 2009 Rocket Software, Inc.



© 2009 IBM Corporation
© 2009 Rocket Software, Inc.



© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

I9A1 DEMO PROFILE
- Rule 1
  - Databases
  - Segments
  - Events
  - PSBs
  - Summary

Profile Summary

I9A1 DEMO PROFILE for IMS on z/OS

DEMO

Rule 1

Audited Databases

- IVPDB1
- IVPDB1I
- IVPDB2
- IVPDB3

Audited Segments

Segment	Database	Audit insert	Audit update	Audit delete	Audit read	Audit capture data
A1	IVPDB1I	true	true	true	true	true
A1111111	IVPDB3	true	true	true	true	true
A1111111	IVPDB2	true	true	true	true	true
A1111111	IVPDB1	true	true	true	true	true
DSEGM2	IVPDB3	true	true	true	true	true

OK Cancel

© 2009 IBM Corporation
© 2009 Rocket Software, Inc.

IBM IMS Audit Management Expert for z/OS V1.2

Questions

© 2009 IBM Corporation
© 2009 Rocket Software, Inc.