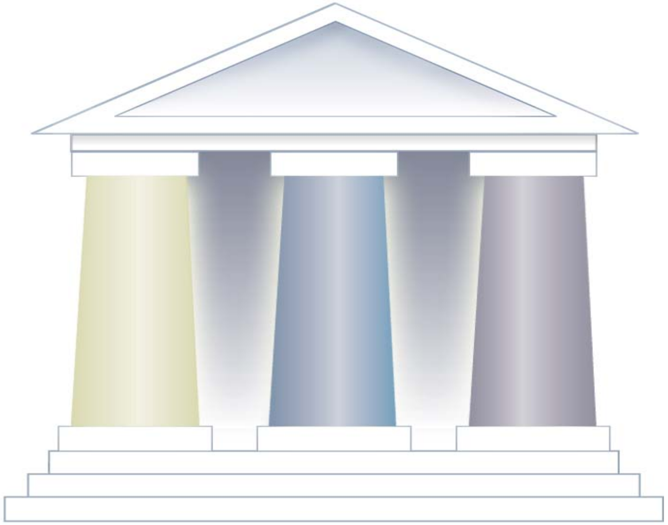
IBM’s Compliance Suite

Regulatory Compliance Not Just for DBA’s

Ernie Mancill and Elaine Morelli
Certified Consulting IT Specialists
DB2 for z/OS Tools

Agenda

- **Customer challenges and regulatory landscape**
- **Encrypting data**
- **Protecting data**
- **Analyzing and auditing data**
- **Archiving data**



Note: Bullet items which have been “grayed out are intended to provide you with additional information and not going to be discussed during our Presentation today

Life is not easy…..

- **Basel II - Improve measurement of total risk and strengthen ability to determine capital needed**
- **Sarbanes-Oxley - Strengthen financial reporting, internal controls by fixing responsibility within companies' management**
- **HIPAA - Secure medical records (lifetime), prove how they have been used & who has used them**
- **Patriot Act - Prevent usage of the financial system to support illegal activities, particularly terrorism**
- **Various anti-money laundering (AML) - Prevent the laundering of money derived from illegal activities**
- **Gramm-Leach-Bliley - Protection of personally identifiable financial information**

…Nor Getting Easier

- Department of Defense - 5015.2
  - requires certified application or technology to manage records (retention)
- SEC Rule 17a-4
  - requires brokers to preserve communications with clients (6 years)
- Corporate Information Security Accountability Act of 2003
  - requires audit of IT security and reporting
  - security infrastructures meet minimum standards
- California Bill 1386
  - a bill that protects data concerning California Residents in all computers across the United States
- European Union
  - various countries are working on proposed bills to protect data concerning EU residents
- **VISA and Mastercard PIC**
  - Requires among other things data encryption of cardholder account number, PIN, etc.
- ... and more to come

The Bottom Line – Improving Internal Control

Regulators have multiple goals. . .

- ✓ Security of the national and international services infrastructure
- ✓ Improved risk management across the enterprise
- ✓ Integrity of financial reporting processes and related business practices
- ✓ Customer information security

. . . which drive investment in several areas

- **People**: Professionals with regulatory experience will be hired to enable firms to meet and anticipate new regulatory requirements
- **Process**: More robust processes and procedures will enable top management to monitor and enhance regulatory compliance
- **Technology**: Significant investment will be made to do the following:
  - Encrypt sensitive data
  - Protect sensitive production data
  - Save data for future audits and to comply with retention rules
  - Auditiability - discover who did what, where and when
    - Real time
    - Historically
  - Engage in real-time monitoring of operations

Visa PCI – A closer look at one compliance example

- **PCI – Payment Card Industry**
  - Initiative enacted by major cardholder companies to ensure that vendor partner
  - Standard is used by other major credit card issuers
  - Compliance is a mandated requirement
  - Severe penalties for non-compliance
  - Synchronicity with other compliance initiatives
  - Compliance viewed by many as competitive advantage

PCI – Specific areas of compliance

- **Requirement 3: Protect Stored Data**
  - Encryption is the ultimate protection mechanism because even if someone breaks through all other protection mechanisms and gains access to encrypted data, they will not be able to read the data without further breaking the encryption
- **Requirement 7: Restrict access to data by business "need to know"**
  - Limit access to computing resources and cardholder information to only those individuals whose job requires such access.
- **Requirement 10: Track and monitor all access to network resources and cardholder data**.
  - Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong.
- **Requirement 10.7 Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulations.**
  - An audit history usually covers a period of at least one year, with a minimum of 3 months available online.

PCI – IBM Compliance Solution

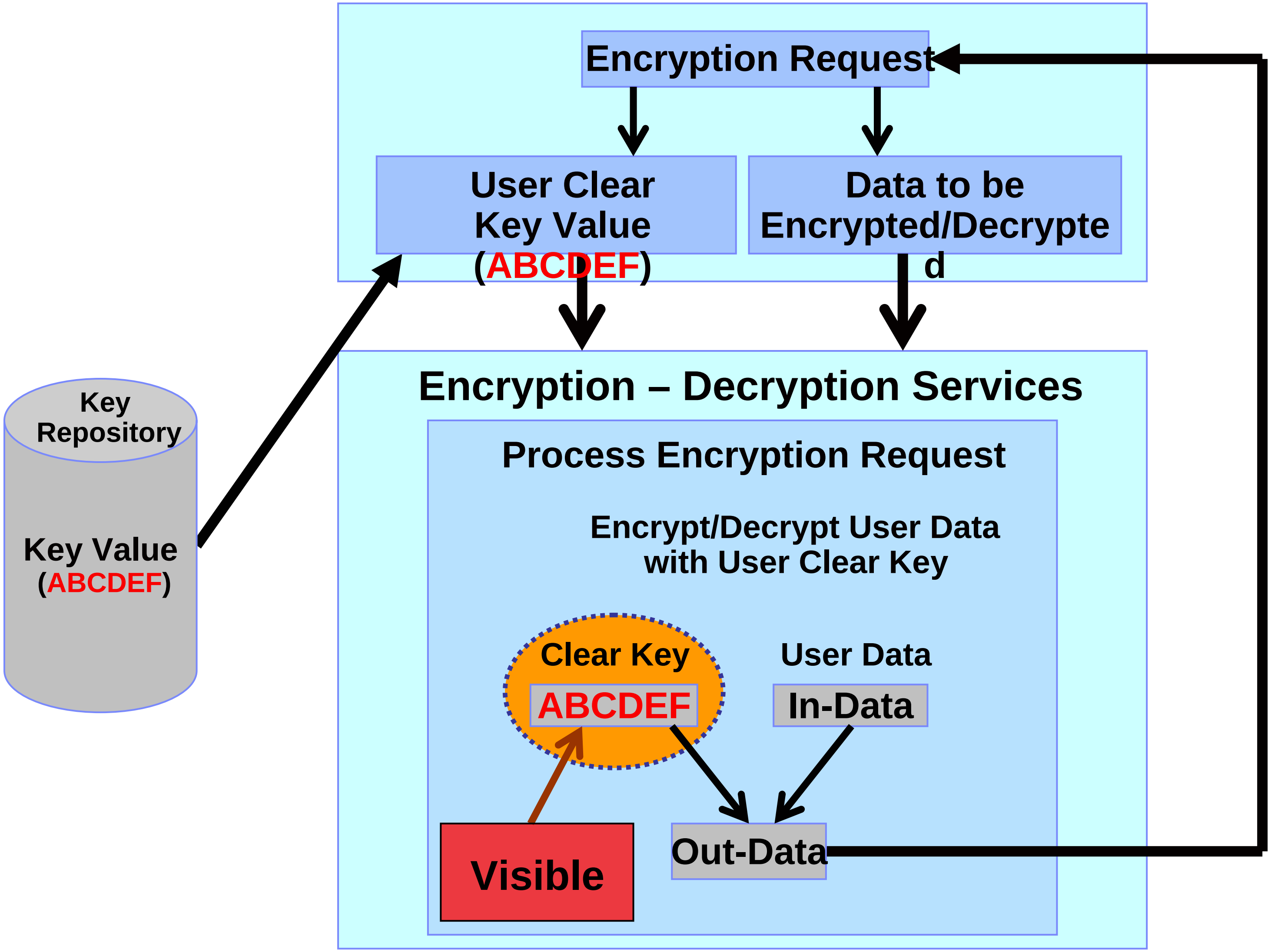
- **Requirement 3: Protect Stored Data**
  - IBM Data Encryption Tool for DB2 and IMS Databases
- **Requirement 7: Restrict access to data by business “need to know”**
  - DB2 for z/OS V8 Multi-Level Security implemented via RACF
- **Requirement 10: Track and monitor all access to network resources and cardholder data**.
  - IBM Tivoli OMEGAMON XE for DB2 Performance Expert on z/OS
  - IBM Audit Management Expert
- **Requirement 10.7 Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulations.**
  - IBM Data Archive Expert

IBM’s Compliance Suite

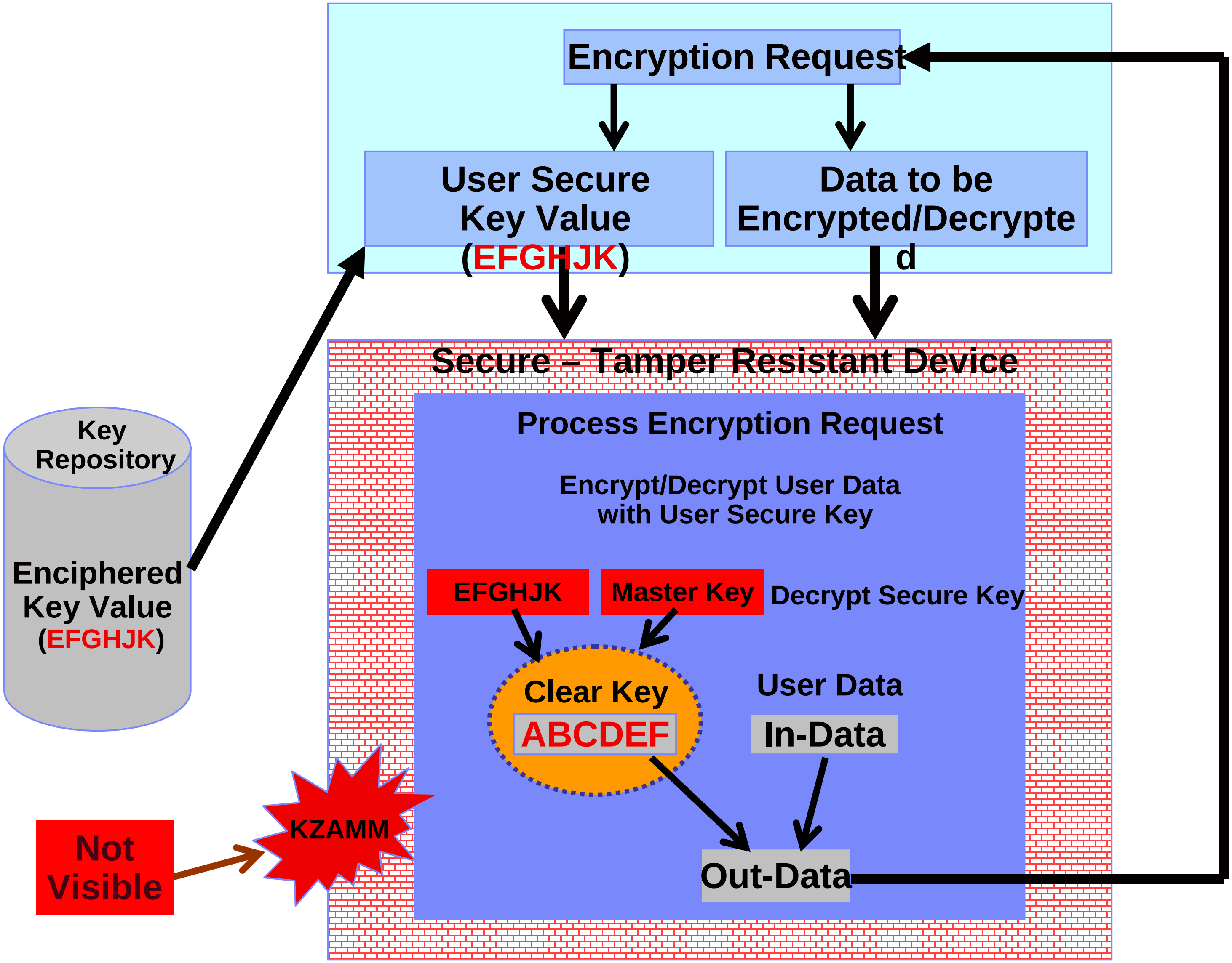
IBM Data Encryption Tool for DB2 and IMS Databases

Step 1 – Encrypt sensitive data

Visual Representation of Clear Key Processing


Encryption Request
User Clear Key Value (ABCDEF)
Data to be Encrypted/Decrypted
Key Repository
Key Value (ABCDEF)
Encryption – Decryption Services
Process Encryption Request
Encrypt/Decrypt User Data with User Clear Key
Clear Key
ABCDEF
User Data
In-Data
Out-Data
Visible

Visual Representation of Secure Key Processing

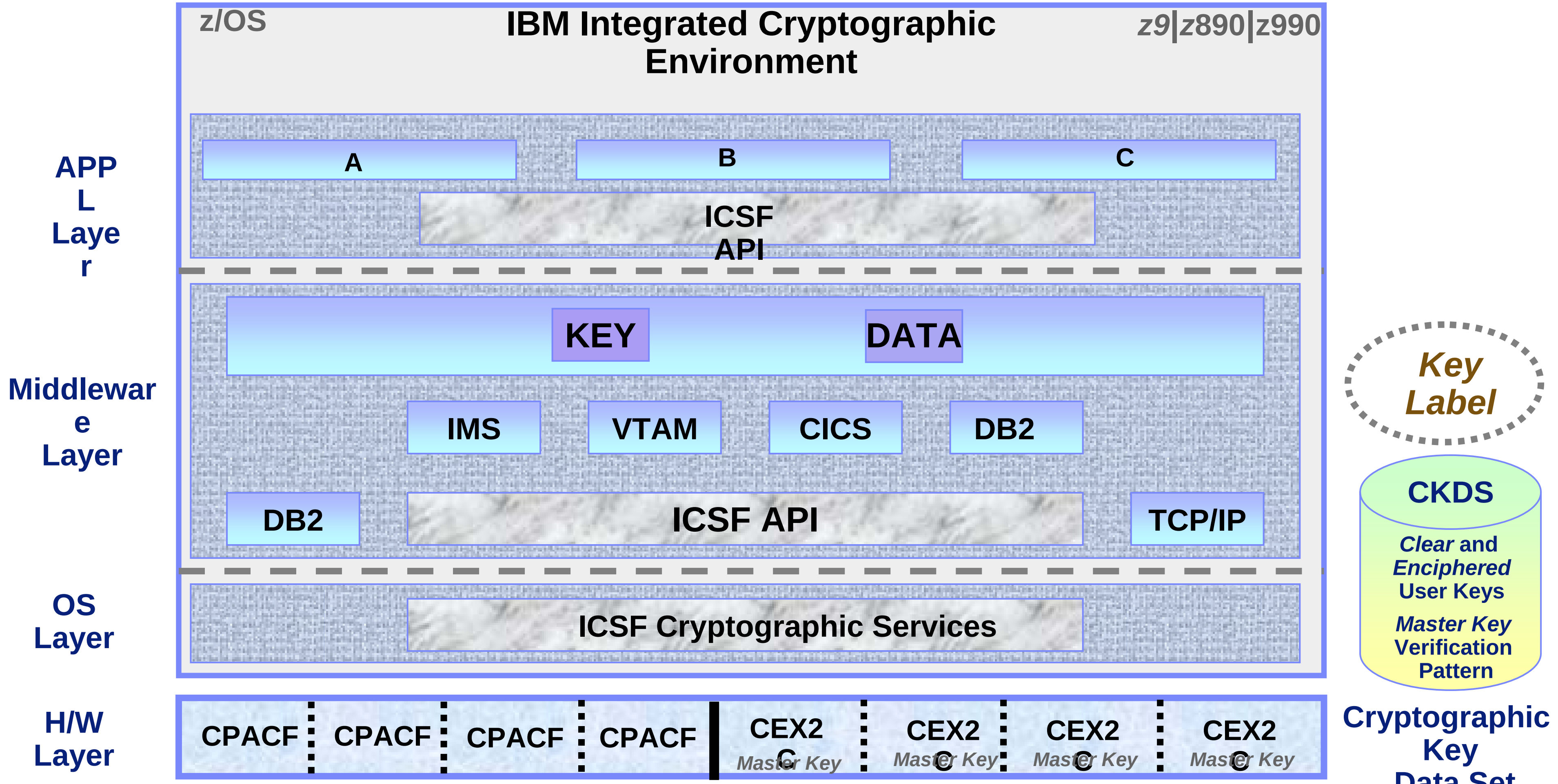

Encryption Request
User Secure Key Value (EFGHJK)
Data to be Encrypted/Decrypted
Secure – Tamper Resistant Device
Process Encryption Request
Encrypt/Decrypt User Data with User Secure Key
EFGHJK
Master Key
Decrypt Secure Key
Clear Key
ABCDEF
User Data
In-Data
Out-Data
Key Repository
Enciphered Key Value (EFGHJK)
KZAMM
Not Visible

Integrated Cryptographic Service Facility (ICSF)

z/OS Integrated Software Support for Data Encryption

- **Enhanced Key Management (Cryptographic Key Data Set (CKDS) Key Repository)**
  - **Key Creation and Distribution**
    - **Public and Private Keys**
    - **Secure and Clear Keys**
    - **Master Keys**
  - **Unique *Key Label* (Key Alias) Indexes each Key stored in the CKDS**
- **Access Control for CKDS via Security Access Facility (SAF)**
  - **Control access to ICSF Callable Services**
  - **Control access to *Key Labels* (Key Alias) stored in the CKDS**
- **ICSF Software Implementation of AES (z9 CPACF)**
- **Operating System S/W API Interface to Cryptographic Hardware**
- **Procedures for creating Installation-Defined Callable Services (UDX)**

IBM Encryption Flow



z/OS

IBM Integrated Cryptographic Environment

z9|z890|z990

APPL Layer

A

B

C

ICSF API

Middleware Layer

KEY

DATA

IMS

VTAM

CICS

DB2

DB2

ICSF API

TCP/IP

OS Layer

ICSF Cryptographic Services

H/W Layer

CPACF

CPACF

CPACF

CPACF

CEX2C *Master Key*

CEX2C *Master Key*

CEX2C *Master Key*

CEX2C *Master Key*

Key Label

CKDS

Clear and *Enciphered* User Keys

Master Key Verification Pattern

Cryptographic Key Data Set

CP Assist for Cryptographic Functions

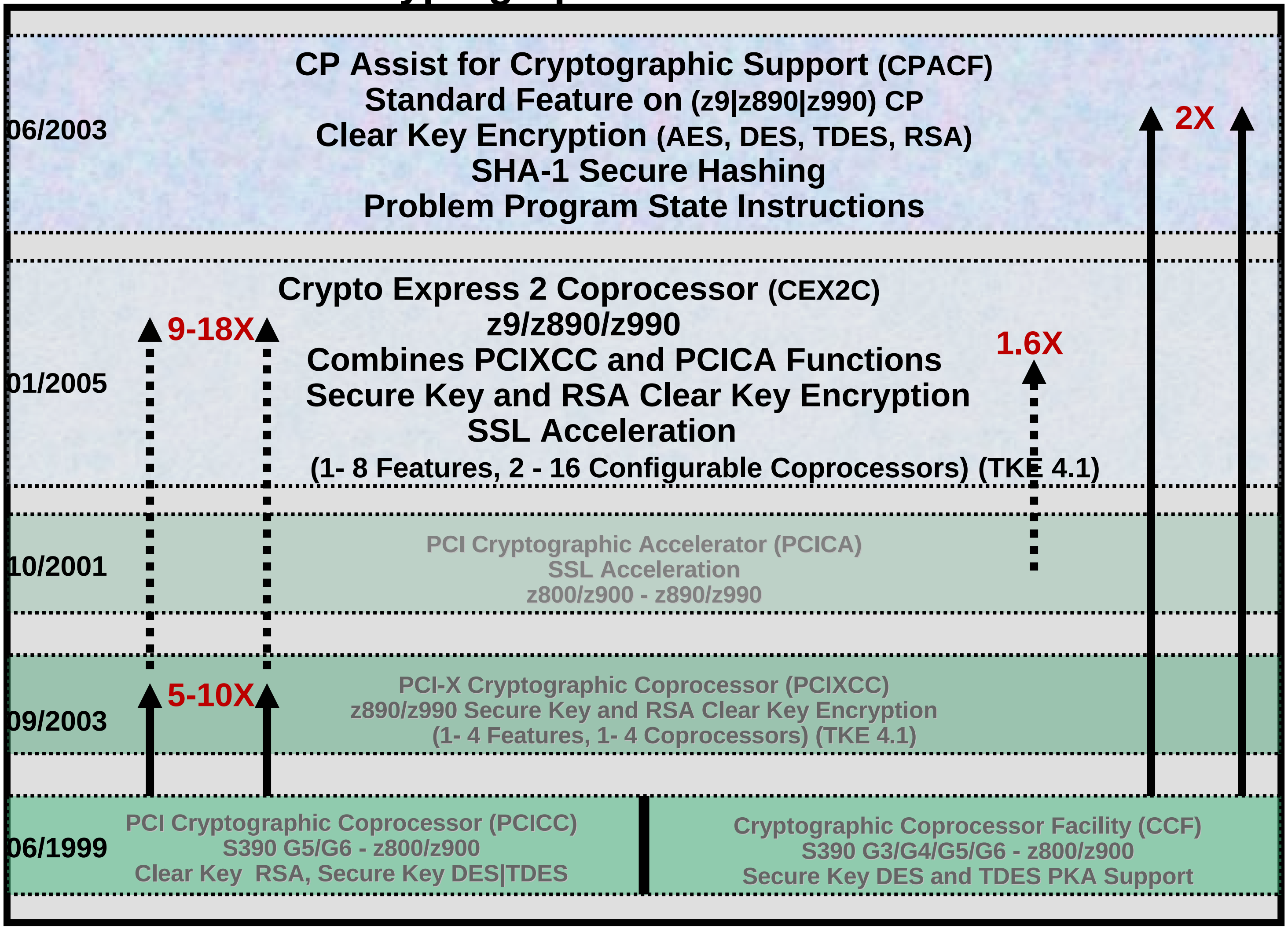
- Problem State Instructions
- Clear Keys Only
- DES/TDES Encryption
- AES (128 Bit)
- SHA-1 (256 on z9)

Crypto Express 2 Coprocessor

- ICSF Access Only (Key 0)
- Master Key Stored Within Boundary of Crypto Express 2 Feature
- Secure Key DES/TDES Encryption
- SSL Accelerator
- Tamper Resistant

zSeries H/W Support for Data Encryption

zSeries Cryptographic Functional Evolution



06/2003

CP Assist for Cryptographic Support (CPACF)
Standard Feature on (z9|z890|z990) CP
Clear Key Encryption (AES, DES, TDES, RSA)
SHA-1 Secure Hashing
Problem Program State Instructions

01/2005

Crypto Express 2 Coprocessor (CEX2C)
z9/z890/z990
Combines PCIXCC and PCICA Functions
Secure Key and RSA Clear Key Encryption
SSL Acceleration
(1- 8 Features, 2 - 16 Configurable Coprocessors) (TKE 4.1)

10/2001

PCI Cryptographic Accelerator (PCICA)
SSL Acceleration
z800/z900 - z890/z990

09/2003

PCI-X Cryptographic Coprocessor (PCIXCC)
z890/z990 Secure Key and RSA Clear Key Encryption
(1- 4 Features, 1- 4 Coprocessors) (TKE 4.1)

06/1999

PCI Cryptographic Coprocessor (PCICC)
S390 G5/G6 - z800/z900
Clear Key RSA, Secure Key DES|TDES

Cryptographic Coprocessor Facility (CCF)
S390 G3/G4/G5/G6 - z800/z900
Secure Key DES and TDES PKA Support

IBM Data Encryption for IMS and DB2 Databases (5799-GWD)

Standard DB2 EDITPROC for Accessing Cryptographic Functions

- All Supported DB2 Versions
- Member of IBM IMS | DB2 Tools Family of Products
- Pre-coded EDITPROC for encryption of DB2® Data
- Encryption/Decryption occurs at the DB2 Row Level
- Unique EDITPROC can be defined for each DB2 Table
- Exploits z/OS Integrated Cryptographic Service Facility (ICSF)
- Exploits zSeries CPACF Cryptographic Hardware Directly
- Requires no changes to your applications
- Fast implementation

Edit Procedures (EDITPROC) are Programs That:

- Transform Data on INSERT | UPDATE | LOAD
- Restore Data to Original Format on SELECT
- Transformations on Entire ROW
- Supported by Utilities
- Implemented via Create Table specification
- Requires unload/load of data

IBM Data Encryption for IMS and DB2 Databases Summary

- Configure the Integrated Cryptographic Service Facility (ICSF)
- Enable CP Assist for Cryptographic Functions (CPACF) (z890/z990)
  (This Feature subject to US Export Restrictions)
- Generate and store in the Cryptographic Key Data Set (CKDS) Key Labels
- Build the IMS User Exit or DB2 EDITPROC
  - For IMS use the Sample JCL Provided or the ISPF Panels
  - For DB2 use the ISPF Panels
  - For IMS Custom Built Exits follow Instructions outlined in:
    - ICSF Application Programmers Guide (SA22-7522)
    - IMS Customization guide (SC18-7817)
    - IMS Utilities Reference System (SC18-7834)
- Back - Up and Unload Databases
- Create Exits for IMS or EDITPROCS for DB2
- Reload the Databases: Data Bases will be Encrypted
- Validate your Output

IBM's Compliance Suite

DB2 V8 on z/OS : Multi-row Security

Step 2 – Access for “need to know” only

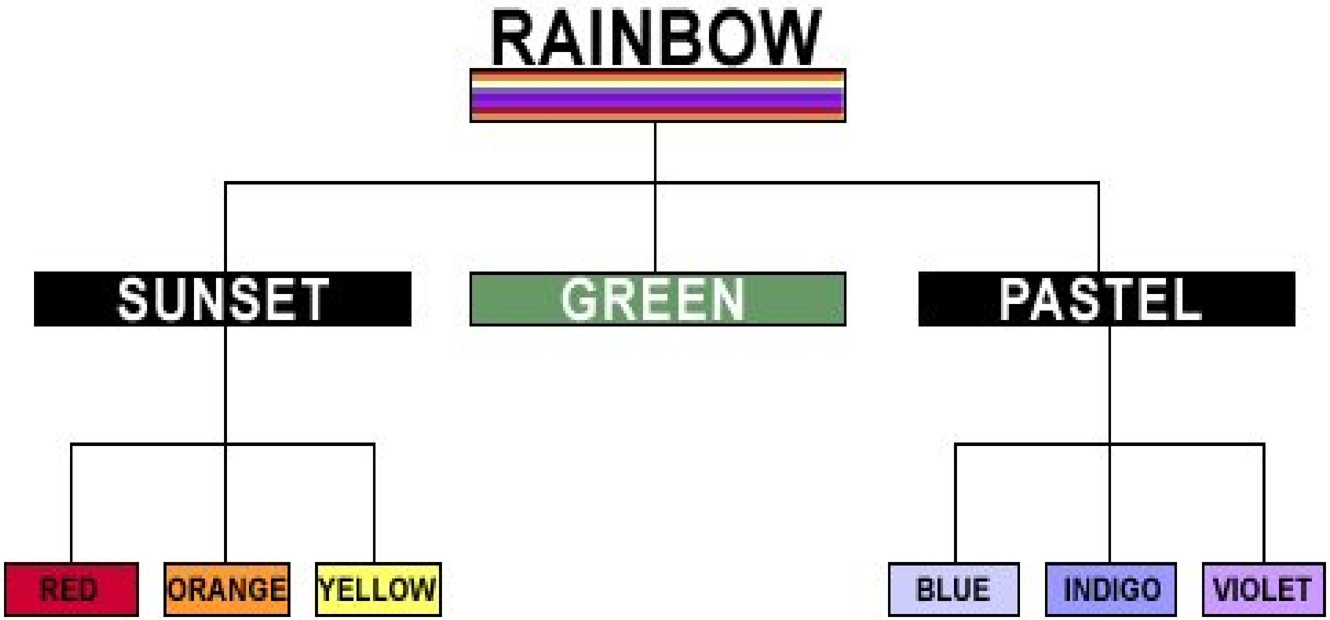
DB2 MLS

- **Rows in a DB2 table have a security label associated with them by means of a special column of the table that contains only the 8-character security label that defines the security classification of each row in that table.**
- **new attribute 'AS SECURITY LABEL'**

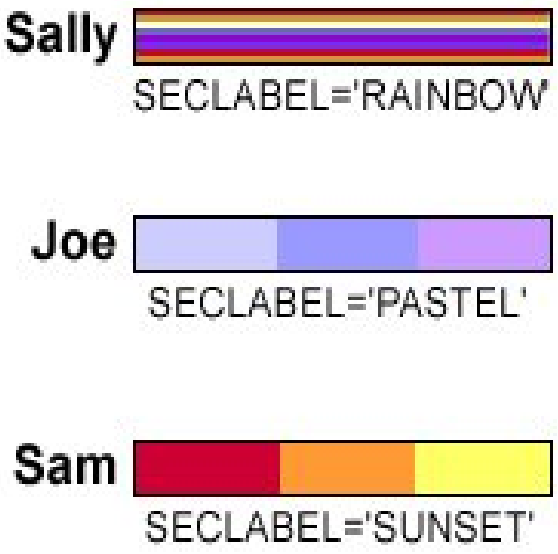
  – The traditional response to these sorts of requirements for DB2 applications has been to use views

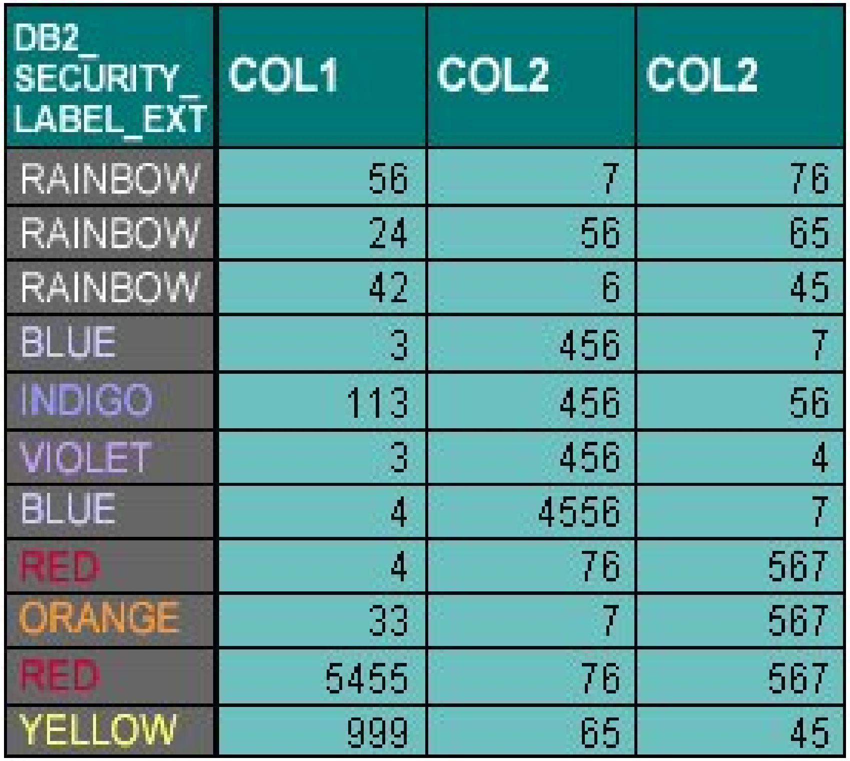
  – some DB2 customers have adopted is to use exits, using fieldprocs or editprocs.

Multilevel Security by Row ...



Multilevel Security by Row





DB2_ SECURITY_ LABEL_EXT	COL1	COL2	COL2
RAINBOW	56	7	76
RAINBOW	24	56	65
RAINBOW	42	6	45
BLUE	3	456	7
INDIGO	113	456	56
VIOLET	3	456	4
BLUE	4	4556	7
RED	4	76	567
ORANGE	33	7	567
RED	5455	76	567
YELLOW	999	65	45

Row Granularity Multilevel Security

- Table has column defined AS SECURITY LABEL
  - Each row value has a specific security label
  - Get security labels from RACF
  - Save in rows for INSERT, UPDATE, LOAD, ...
- Check for each new seclabel value accessed
  - If access is allowed, then normal access
  - If access is not allowed, data not returned
- Runtime user to data checking
- Seclabel values are cached to minimize cpu
- Requires z/OS V1R5 and Security Server (RACF)

Implement Security Labels in DB2

- **In order to implement MLS for DB2, it is first necessary to implement MLS on your MVS system.**

- **identify all of the SECLABELs to be used in the system.**

  - 1. Identify which users and groups require what access to which rows of which tables.
  - 2. Design a set of security labels for users and table rows that reflects the result of step 1.
  - 3. Get the RACF administrators to define that set in RACF, and then activate the RACF SECLABEL class.
  - 4. Add a security label column to each table requiring row-level security. This process assigns an initial default value to every row.
  - 5. Update the security labels of the rows to appropriate values.

Users & Objects

- **relationship between DB2 users and DB2 objects is important**
- **a user is any entity that requires access to system resources. The term user includes not only human users, but can also be stored procedures or batch jobs.**
- **an object is any system resource to which access must be controlled**
  - Data sets
  - Tables
  - Rows
  - Commands

Its not all or nothing

- **You do not have to enable the DB2 RACF exit DSNX@XAC in order to use SECLABELs for row-level security. You may continue to use native DB2 GRANTs and REVOKEs to control all other DB2 access, but you will not have SECLABELs for object-level security.**
- **To run in a DB2 row-level security environment, it is sufficient to have:**
  - the RACF SECLABEL class active
  - SECLABELS for users
  - SECLABELS on DB2 table rows
  - With this setup, *all* DB2 users are equivalent to having write-down authority.

IBM's Compliance Suite

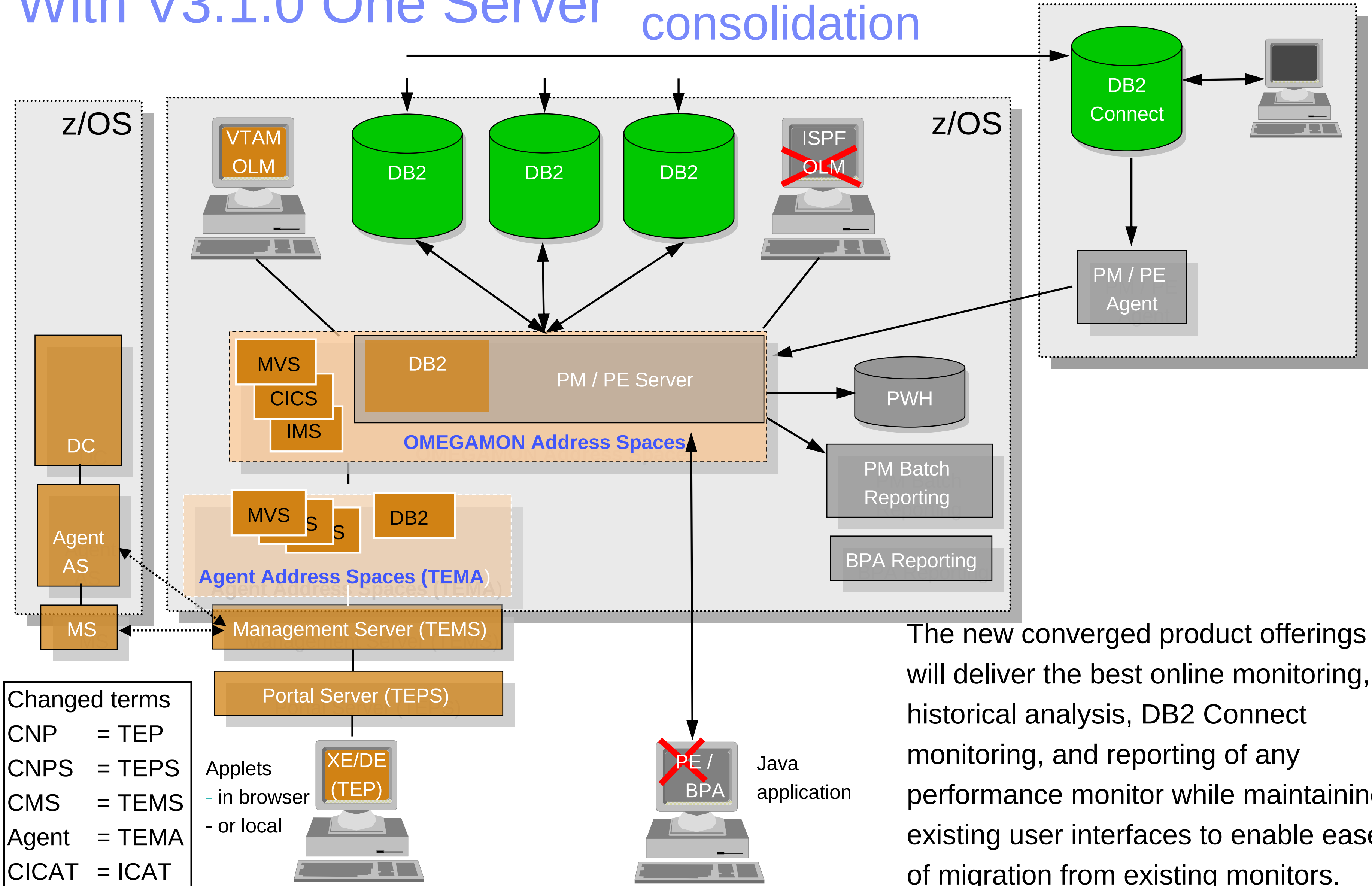
IBM Tivoli OMEGAMON XE for DB2 Performance Expert on z/OS

Step 3 – Track and monitor access to data

OMPE – Audit Trace Management and Reporting

- **While we will show how to use OMPE to perform this task, we'll also see that a much better solution is provided with DB2 Audit Management Expert. The OMPE approach is very much a "labor intensive" implementation.**
- **While the Audit Detail report has activity information, we'll show how to load this information into the Performance Database for long term audit data storage and providing the ability to use SQL for audit reporting requirements.**
- **We need to use the OMPE Performance Database vs. the Performance Warehouse since the PWH only supports Accounting and Statistics data. The PWH process is much more automated and requires significantly less DBA interaction.**
- **Our scenario shows an "ad hoc" collection of trace data, while this is acceptable, many customers start the necessary audit traces at DB2 startup and direct the trace output to SMF.**

With V3.1.0 One Server and later UI consolidation



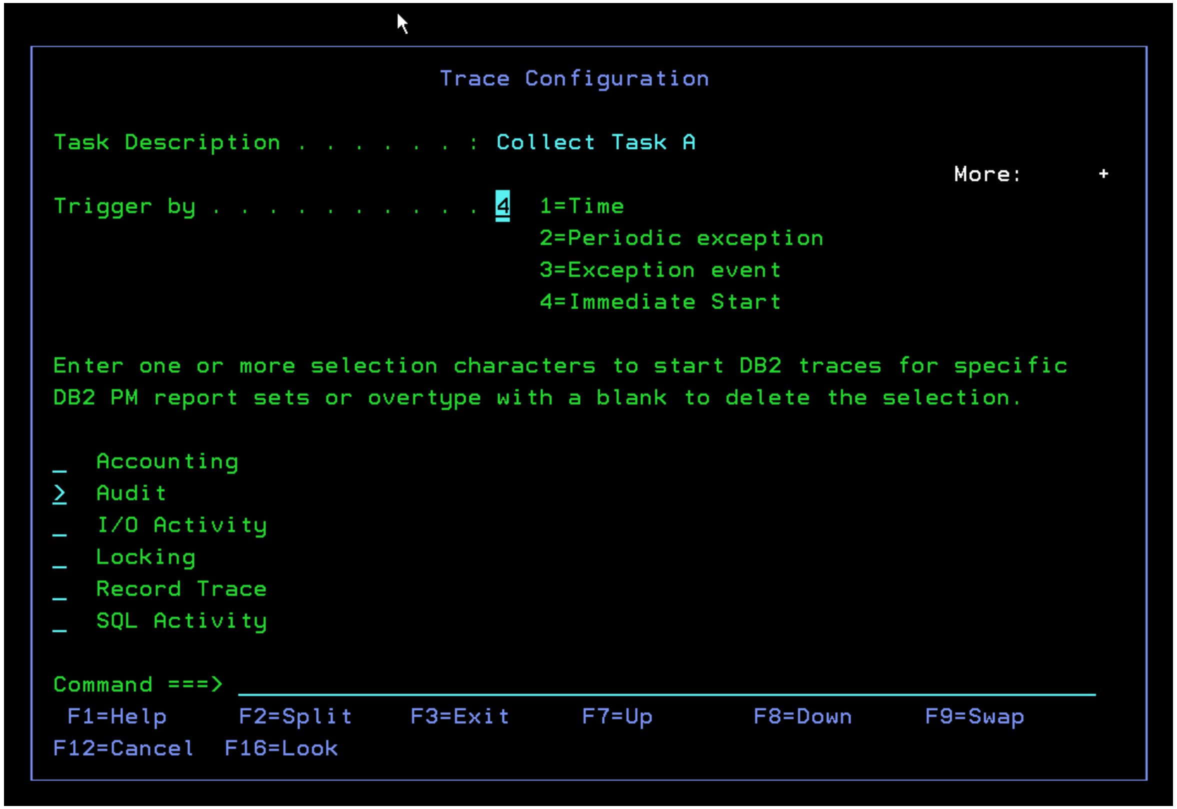
Changed terms	
CNP	= TEP
CNPS	= TEPS
CMS	= TEMS
Agent	= TEMA
CICAT	= ICAT

The new converged product offerings will deliver the best online monitoring, historical analysis, DB2 Connect monitoring, and reporting of any performance monitor while maintaining existing user interfaces to enable ease of migration from existing monitors.

Summary of functions – OMEGAMON XE for DB2 Performance Monitor/Expert for z/OS

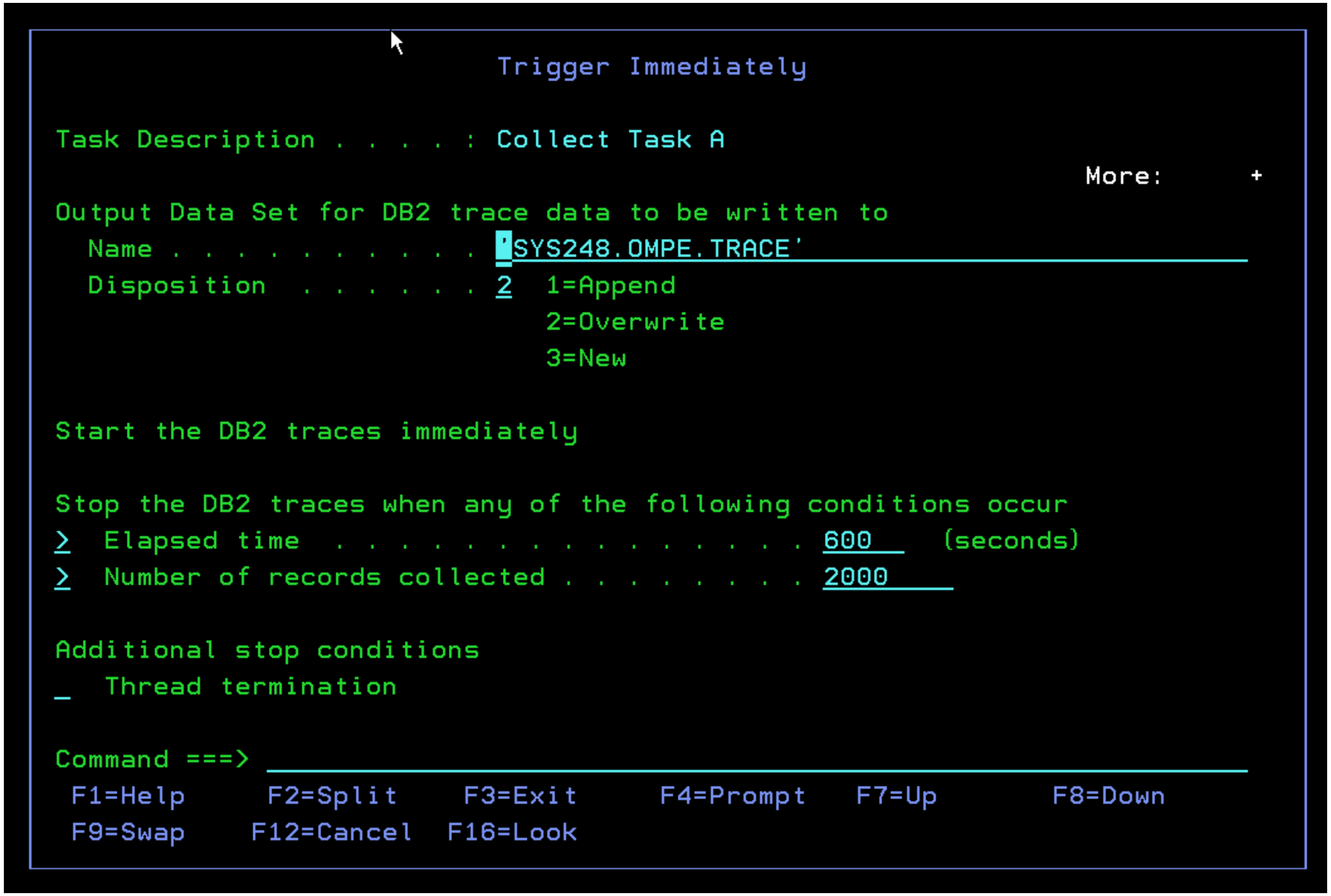
- **Real-time monitoring**
  - Threads and Statistics monitoring
  - DB2 Connect monitoring
  - Object Analysis
  - Data Sharing/Sysplex data (DB2Plex data)
- **Near-term history**
- **Trace collection** (also as part of the PWH process support)
- **Reporting**
  - Accounting, Statistics, SQL Activities, Locking, I/O Activity, Audit, Utilities, Record Trace
  - Executable as separate jobs or via PWH process engine
- **Performance Warehouse with expert analysis support**
- **Buffer Pool Analysis, expert advice, and simulation** (only with the OMEGAMON XE for DB2 Performance Expert)

This shows the Trace Configuration dialog from OMPE. You can also manage the collection of trace data from the OMPE PWH client.



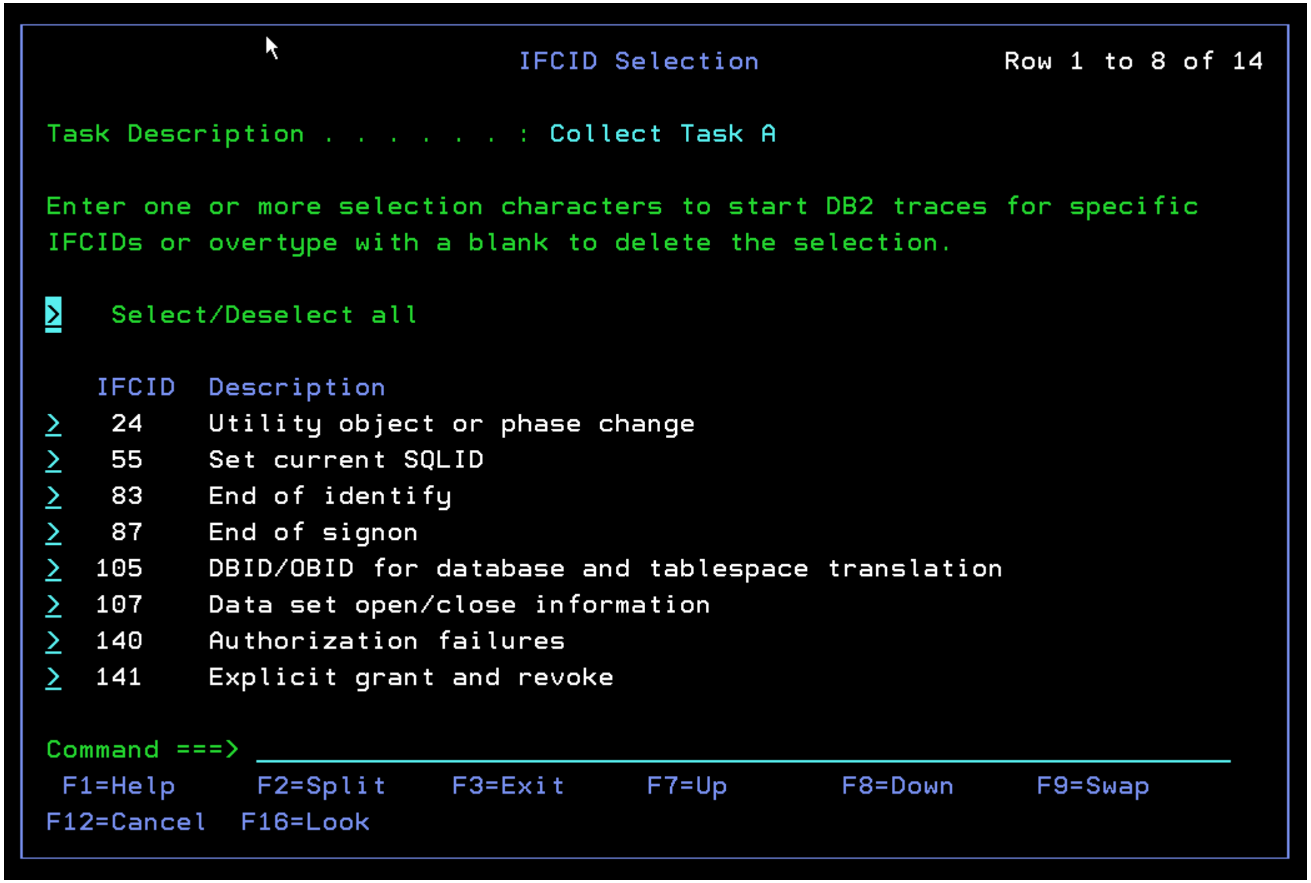
```
                         Trace Configuration

Task Description . . . . . . : Collect Task A
                                                         More:     +
Trigger by . . . . . . . . . . 4  1=Time
                                  2=Periodic exception
                                  3=Exception event
                                  4=Immediate Start

Enter one or more selection characters to start DB2 traces for specific
DB2 PM report sets or overtype with a blank to delete the selection.

_  Accounting
>  Audit
_  I/O Activity
_  Locking
_  Record Trace
_  SQL Activity

Command ===> ____________________________________________________________
 F1=Help     F2=Split     F3=Exit     F7=Up       F8=Down     F9=Swap
F12=Cancel  F16=Look
```

Trace collection can be controlled to only collect data for a set period of time, probably not recommended for audit purposes



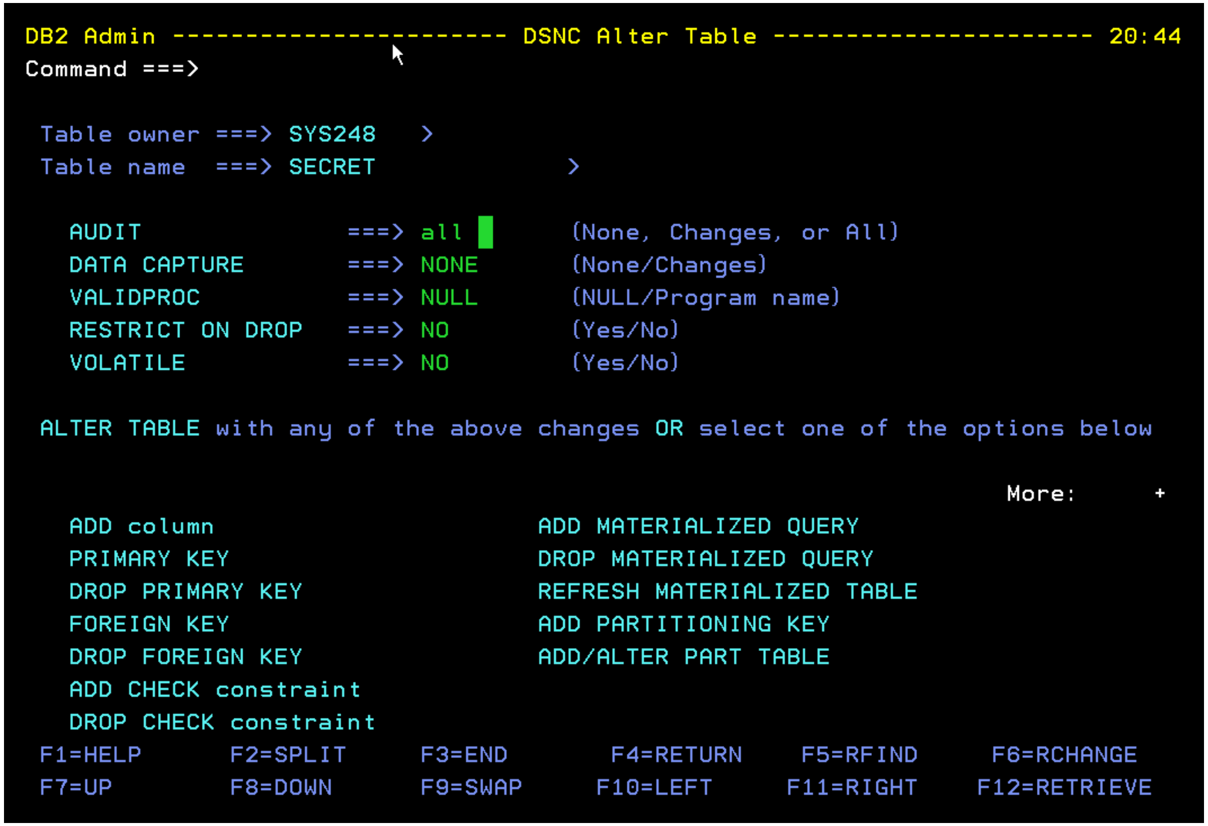
```
                           Trigger Immediately

Task Description . . . . : Collect Task A
                                                               More:      +
Output Data Set for DB2 trace data to be written to
  Name . . . . . . . . . . 'SYS248.OMPE.TRACE'
  Disposition  . . . . . . 2  1=Append
                              2=Overwrite
                              3=New

Start the DB2 traces immediately

Stop the DB2 traces when any of the following conditions occur
>  Elapsed time  . . . . . . . . . . . . . . . 600     (seconds)
>  Number of records collected . . . . . . . . 2000

Additional stop conditions
_  Thread termination

Command ===>
 F1=Help     F2=Split    F3=Exit     F4=Prompt   F7=Up       F8=Down
 F9=Swap    F12=Cancel  F16=Look
```

We can see the different Audit IFCID's started by default. In this example, we'll collect all IFCIDs then filter when we generate the load file later in the process….



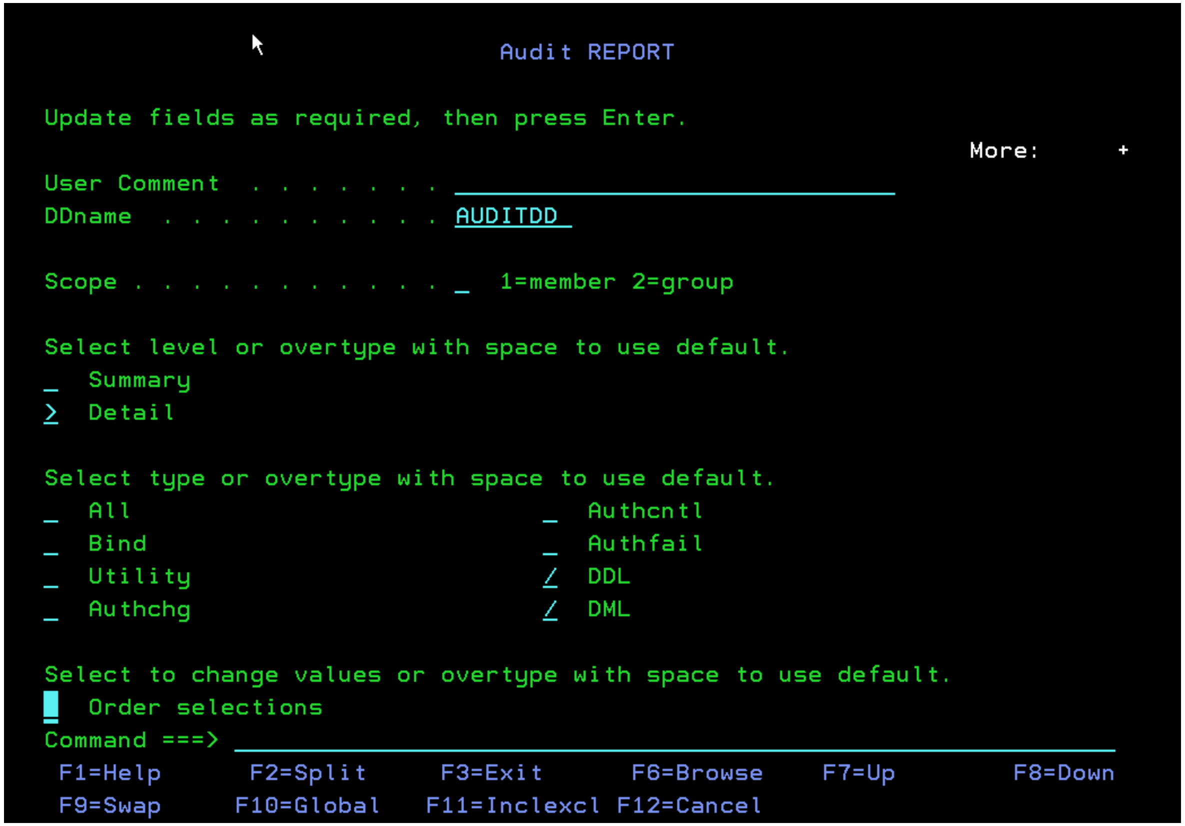
```
                              IFCID Selection                  Row 1 to 8 of 14

Task Description . . . . . . . : Collect Task A

Enter one or more selection characters to start DB2 traces for specific
IFCIDs or overtype with a blank to delete the selection.

>   Select/Deselect all

   IFCID  Description
>   24    Utility object or phase change
>   55    Set current SQLID
>   83    End of identify
>   87    End of signon
>  105    DBID/OBID for database and tablespace translation
>  107    Data set open/close information
>  140    Authorization failures
>  141    Explicit grant and revoke

Command ===> ____________________________________________________________
 F1=Help     F2=Split    F3=Exit     F7=Up       F8=Down     F9=Swap
F12=Cancel  F16=Look
```

One additional step needed to collect access information is that each “audited” object needs to be ALTERED with the AUDIT attribute. This is shown below using the DB2 Administration Tool.



```
DB2 Admin ----------------------- DSNC Alter Table --------------------- 20:44
Command ===>

 Table owner ===> SYS248   >
 Table name  ===> SECRET             >

   AUDIT                  ===> all █      (None, Changes, or All)
   DATA CAPTURE           ===> NONE       (None/Changes)
   VALIDPROC              ===> NULL       (NULL/Program name)
   RESTRICT ON DROP       ===> NO         (Yes/No)
   VOLATILE               ===> NO         (Yes/No)

 ALTER TABLE with any of the above changes OR select one of the options below

                                                                  More:      +
   ADD column                       ADD MATERIALIZED QUERY
   PRIMARY KEY                      DROP MATERIALIZED QUERY
   DROP PRIMARY KEY                 REFRESH MATERIALIZED TABLE
   FOREIGN KEY                      ADD PARTITIONING KEY
   DROP FOREIGN KEY                 ADD/ALTER PART TABLE
   ADD CHECK constraint
   DROP CHECK constraint
 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

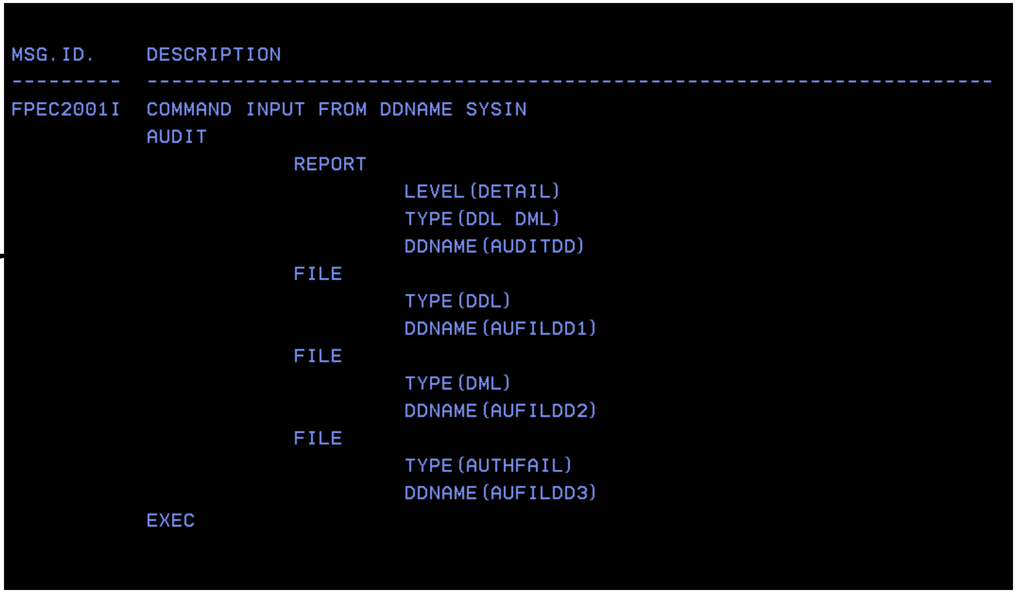
Once the data is collected, we next generate the appropriate Audit report. In this example, we're filtering on DDL and DML access only.



```
                               Audit REPORT

Update fields as required, then press Enter.
                                                               More:     +
User Comment  . . . . . . . ______________________________
DDname  . . . . . . . . . . AUDITDD_

Scope . . . . . . . . . . . _  1=member 2=group

Select level or overtype with space to use default.
_  Summary
>  Detail

Select type or overtype with space to use default.
_  All                               _  Authcntl
_  Bind                              _  Authfail
_  Utility                           /  DDL
_  Authchg                           /  DML

Select to change values or overtype with space to use default.
_  Order selections
Command ===> ____________________________________________________________
 F1=Help      F2=Split     F3=Exit      F6=Browse    F7=Up        F8=Down
 F9=Swap     F10=Global   F11=Inclexcl F12=Cancel
```

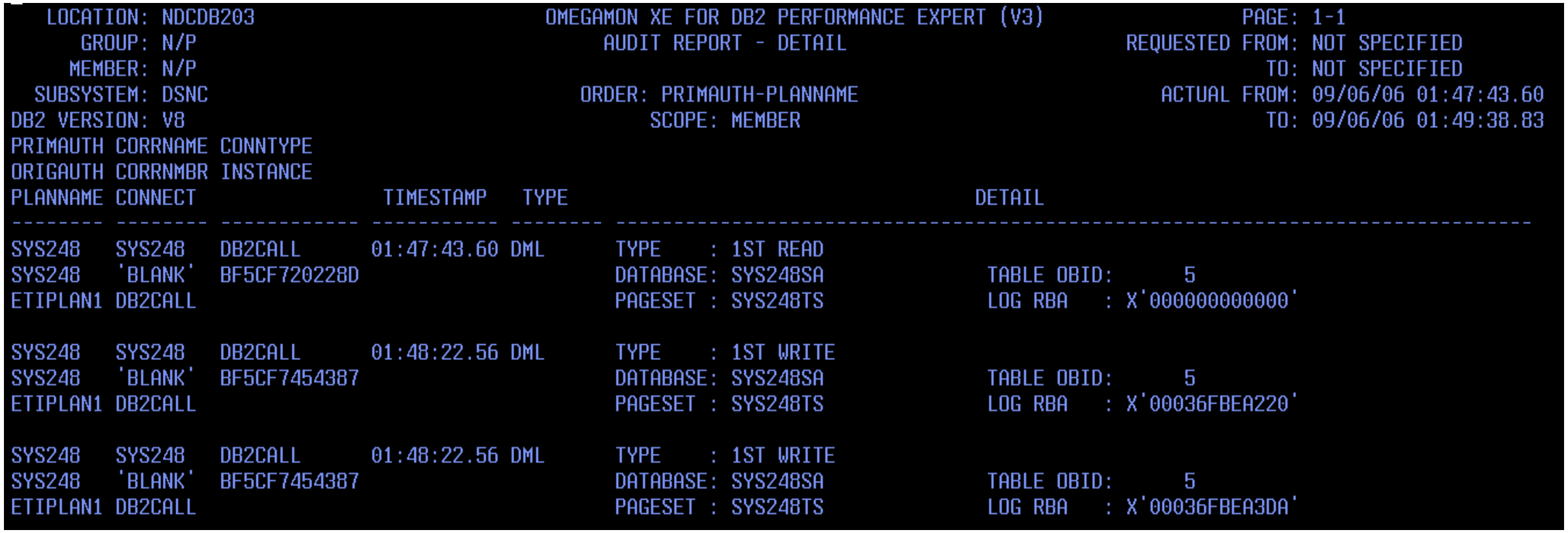
The OMPE “File” Report command is used to create DB2 Load compatible record formats

OMPE “File” report commands



```
MSG.ID.    DESCRIPTION
---------  ---------------------------------------------------------------------
FPEC2001I  COMMAND INPUT FROM DDNAME SYSIN
           AUDIT
                       REPORT
                                LEVEL(DETAIL)
                                TYPE(DDL DML)
                                DDNAME(AUDITDD)
                       FILE
                                TYPE(DDL)
                                DDNAME(AUFILDD1)
                       FILE
                                TYPE(DML)
                                DDNAME(AUFILDD2)
                       FILE
                                TYPE(AUTHFAIL)
                                DDNAME(AUFILDD3)
           EXEC
```

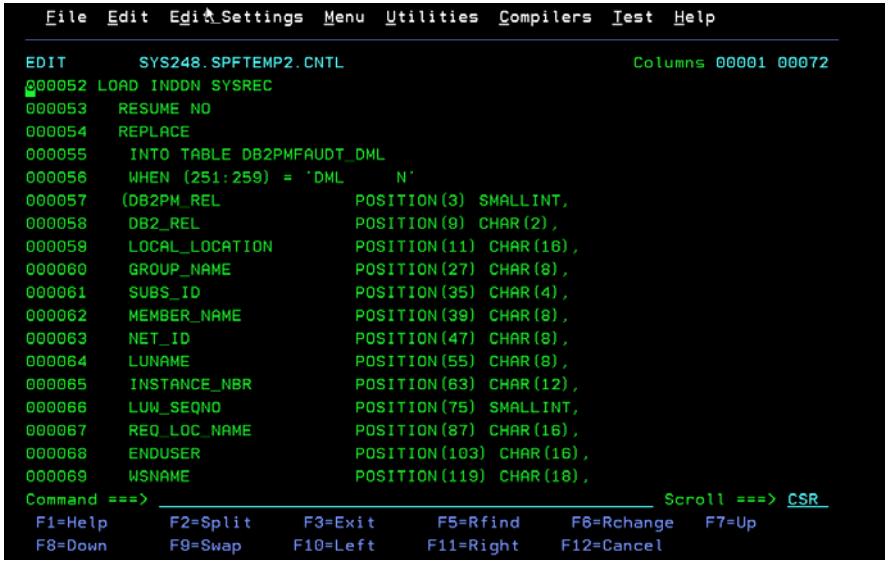
OMPE Audit Detail Report



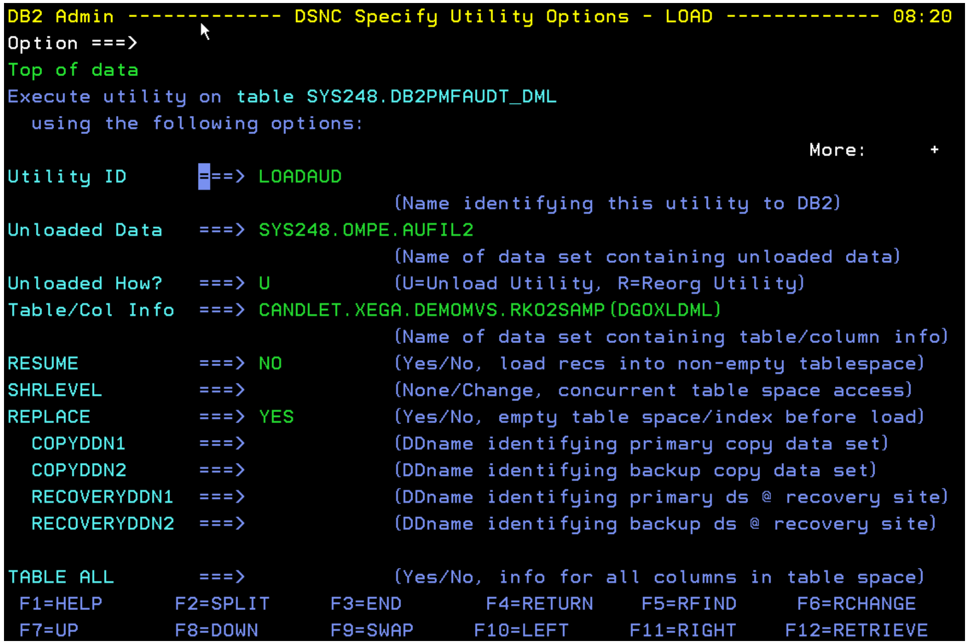
```
   LOCATION: NDCDB203                         OMEGAMON XE FOR DB2 PERFORMANCE EXPERT (V3)                 PAGE: 1-1
      GROUP: N/P                                   AUDIT REPORT - DETAIL                        REQUESTED FROM: NOT SPECIFIED
     MEMBER: N/P                                                                                            TO: NOT SPECIFIED
  SUBSYSTEM: DSNC                               ORDER: PRIMAUTH-PLANNAME                           ACTUAL FROM: 09/06/06 01:47:43.60
DB2 VERSION: V8                                        SCOPE: MEMBER                                        TO: 09/06/06 01:49:38.83
PRIMAUTH CORRNAME CONNTYPE
ORIGAUTH CORRNMBR INSTANCE
PLANNAME CONNECT                TIMESTAMP   TYPE                                   DETAIL
-------- -------- ------------ ----------- -------- -------------------------------------------------------------------------------
SYS248   SYS248   DB2CALL      01:47:43.60 DML      TYPE    : 1ST READ
SYS248   'BLANK'  BF5CF720228D                      DATABASE: SYS248SA              TABLE OBID:      5
ETIPLAN1 DB2CALL                                    PAGESET : SYS248TS              LOG RBA    : X'000000000000'

SYS248   SYS248   DB2CALL      01:48:22.56 DML      TYPE    : 1ST WRITE
SYS248   'BLANK'  BF5CF7454387                      DATABASE: SYS248SA              TABLE OBID:      5
ETIPLAN1 DB2CALL                                    PAGESET : SYS248TS              LOG RBA    : X'00036FBEA220'

SYS248   SYS248   DB2CALL      01:48:22.56 DML      TYPE    : 1ST WRITE
SYS248   'BLANK'  BF5CF7454387                      DATABASE: SYS248SA              TABLE OBID:      5
ETIPLAN1 DB2CALL                                    PAGESET : SYS248TS              LOG RBA    : X'00036FBEA3DA'
```

Invoking the DB2 load utility to populate the DB2 Performance DB with Audit data.

Load Control sample statements located in RKO2SAMP



```
EDIT       SYS248.SPFTEMP2.CNTL                              Columns 00001 00072
000052 LOAD INDDN SYSREC
000053   RESUME NO
000054   REPLACE
000055    INTO TABLE DB2PMFAUDT_DML
000056    WHEN (251:259) = 'DML      N'
000057   (DB2PM_REL                 POSITION(3)  SMALLINT,
000058    DB2_REL                   POSITION(9)  CHAR(2),
000059    LOCAL_LOCATION            POSITION(11) CHAR(16),
000060    GROUP_NAME                POSITION(27) CHAR(8),
000061    SUBS_ID                   POSITION(35) CHAR(4),
000062    MEMBER_NAME               POSITION(39) CHAR(8),
000063    NET_ID                    POSITION(47) CHAR(8),
000064    LUNAME                    POSITION(55) CHAR(8),
000065    INSTANCE_NBR              POSITION(63) CHAR(12),
000066    LUW_SEQNO                 POSITION(75) SMALLINT,
000067    REQ_LOC_NAME              POSITION(87) CHAR(16),
000068    ENDUSER                   POSITION(103) CHAR(16),
000069    WSNAME                    POSITION(119) CHAR(18),
Command ===> ____________________________________________________ Scroll ===> CSR
 F1=Help      F2=Split     F3=Exit      F5=Rfind     F6=Rchange   F7=Up
 F8=Down      F9=Swap     F10=Left     F11=Right    F12=Cancel
```

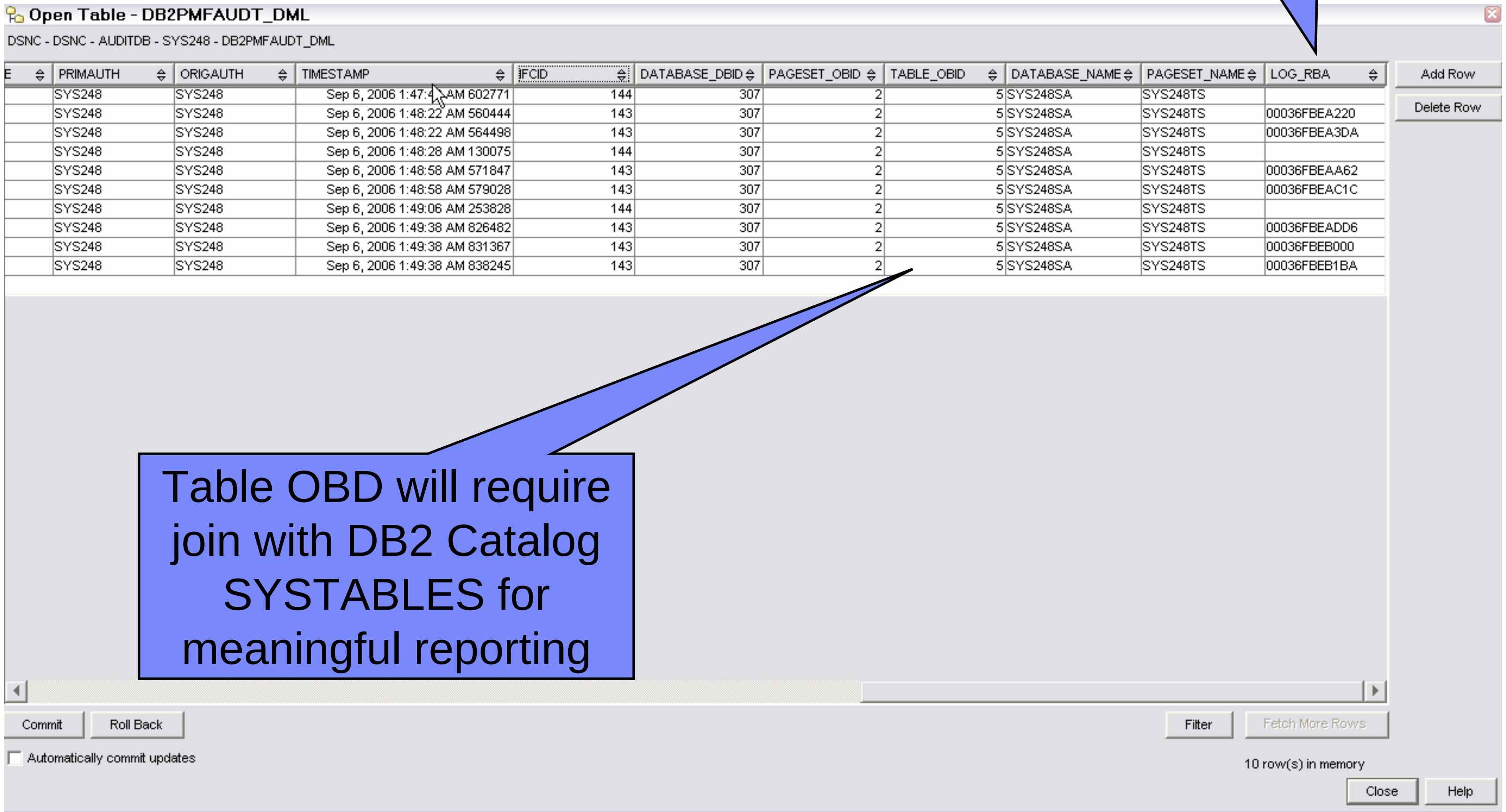


```
DB2 Admin ------------- DSNC Specify Utility Options - LOAD ------------- 08:20
Option ===>
Top of data
Execute utility on table SYS248.DB2PMFAUDT_DML
  using the following options:
                                                                    More:     +
Utility ID      ===> LOADAUD
                                 (Name identifying this utility to DB2)
Unloaded Data   ===> SYS248.OMPE.AUFIL2
                                 (Name of data set containing unloaded data)
Unloaded How?   ===> U           (U=Unload Utility, R=Reorg Utility)
Table/Col Info  ===> CANDLET.XEGA.DEMOMVS.RKO2SAMP(DGOXLDML)
                                 (Name of data set containing table/column info)
RESUME          ===> NO          (Yes/No, load recs into non-empty tablespace)
SHRLEVEL        ===>             (None/Change, concurrent table space access)
REPLACE         ===> YES         (Yes/No, empty table space/index before load)
  COPYDDN1      ===>             (DDname identifying primary copy data set)
  COPYDDN2      ===>             (DDname identifying backup copy data set)
  RECOVERYDDN1  ===>             (DDname identifying primary ds @ recovery site)
  RECOVERYDDN2  ===>             (DDname identifying backup ds @ recovery site)

TABLE ALL       ===>             (Yes/No, info for all columns in table space)
 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Creation of the LOAD utility statements and JCL using DB2 Administration Tool

A view of the audit data stored in the OMPE performance warehouse using DB2 Control Center

Log RBA can be used to locate details about other actions for the LUW



Open Table - DB2PMFAUDT_DML

DSNC - DSNC - AUDITDB - SYS248 - DB2PMFAUDT_DML

E	PRIMAUTH	ORIGAUTH	TIMESTAMP	IFCID	DATABASE_DBID	PAGESET_OBID	TABLE_OBID	DATABASE_NAME	PAGESET_NAME	LOG_RBA
	SYS248	SYS248	Sep 6, 2006 1:47:4[illegible] AM 602771	144	307	2	5	SYS248SA	SYS248TS	
	SYS248	SYS248	Sep 6, 2006 1:48:22 AM 560444	143	307	2	5	SYS248SA	SYS248TS	00036FBEA220
	SYS248	SYS248	Sep 6, 2006 1:48:22 AM 564498	143	307	2	5	SYS248SA	SYS248TS	00036FBEA3DA
	SYS248	SYS248	Sep 6, 2006 1:48:28 AM 130075	144	307	2	5	SYS248SA	SYS248TS	
	SYS248	SYS248	Sep 6, 2006 1:48:58 AM 571847	143	307	2	5	SYS248SA	SYS248TS	00036FBEAA62
	SYS248	SYS248	Sep 6, 2006 1:48:58 AM 579028	143	307	2	5	SYS248SA	SYS248TS	00036FBEAC1C
	SYS248	SYS248	Sep 6, 2006 1:49:06 AM 253828	144	307	2	5	SYS248SA	SYS248TS	
	SYS248	SYS248	Sep 6, 2006 1:49:38 AM 826482	143	307	2	5	SYS248SA	SYS248TS	00036FBEADD6
	SYS248	SYS248	Sep 6, 2006 1:49:38 AM 831367	143	307	2	5	SYS248SA	SYS248TS	00036FBEB000
	SYS248	SYS248	Sep 6, 2006 1:49:38 AM 838245	143	307	2	5	SYS248SA	SYS248TS	00036FBEB1BA

Table OBD will require join with DB2 Catalog SYSTABLES for meaningful reporting

OMPE – Audit Trace Management and Reporting

- **We've shown that using OMPE, we can manage the collection of the required DB2 Audit traces, formatting of the load file and population of the OMPE Performance Database**
- **While these processes can be set up and scheduled in batch, they require ongoing maintenance and intervention by the DBA in order to collect and load the data.**
- **To generate usable SQL based reports, some additional work is needed (join the catalog table to get the table name for example).**
- **Using RBA for first update access, more detail can be "manually" generated using a log analysis product (such as the IBM Log Analysis Tool), or DSN1LOGP.**
- **Using DB2 Audit Management Expert, a much more secure and functional solution is provided**
- **Which ever method is used, over time the collection of audit information in a DB2 table can grow exponentially could require significant amounts of storage and associated management issues.**
- **To help better control and manage the long term storage of DB2 audit data, we can introduce an archival methodology**

IBM’s Compliance Suite

DB2 V8 on z/OS : Analyzing and Auditing Data

Step 4 – Auditor Independence

Questions for the Auditor

- **Need information regarding the accessability of data stored in DB2 independent of the DBA staff**
  - How does DB2 work?
  - What kind of information can I get from DB2?
  - Where can the information be gathered?
  - Need to see not only updates or deletes, but read access as well
  - Need to retain this information
  - How can I monitor what the DBA's are doing
  - I really want to be independent and not have to rely on the DBA staff
  - How can I get the reports I need?
  - I only want to see information for specific users or transactions. How do I do that?

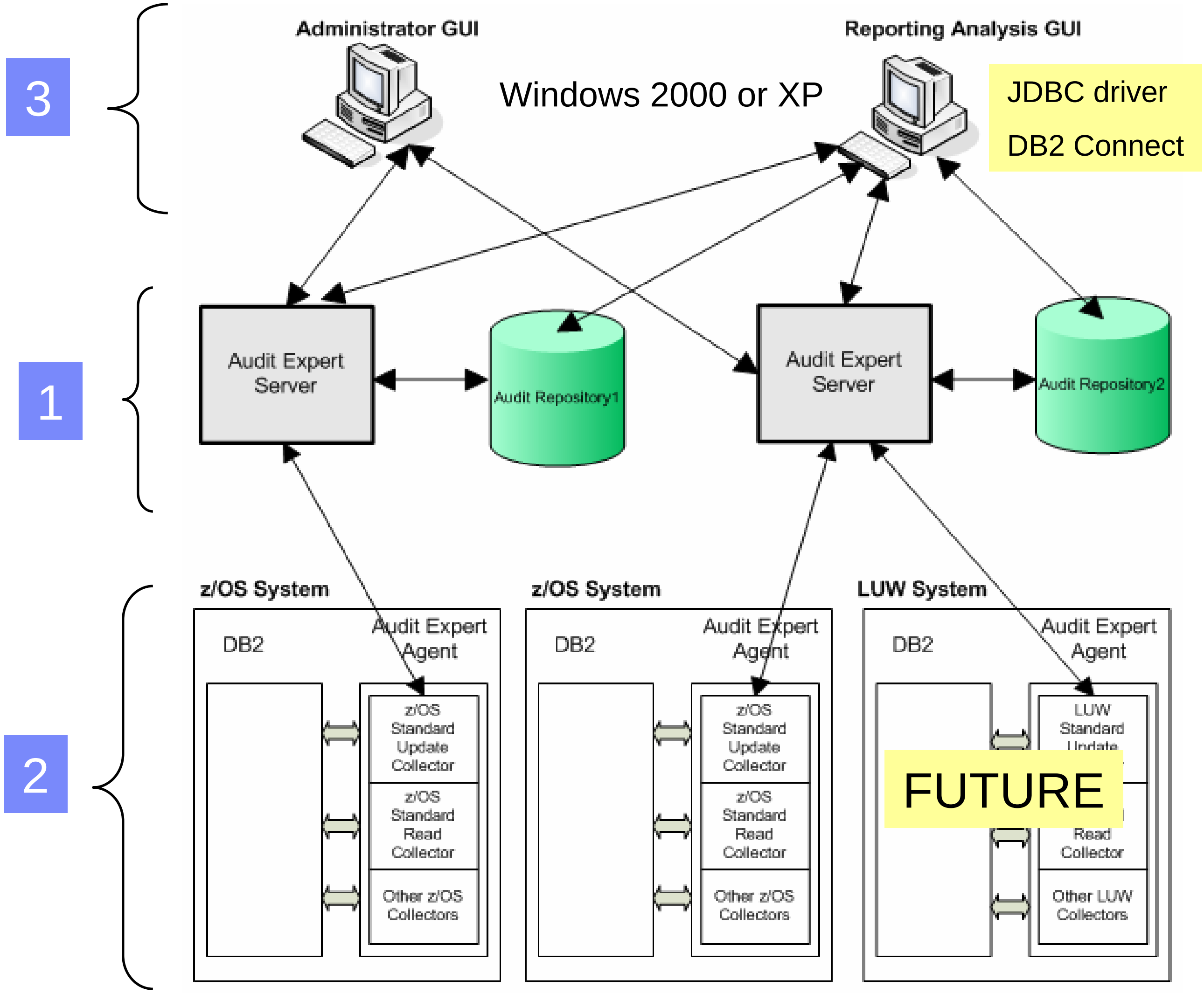
Questions for the DBA

- **Management said we have to audit access to tables with sensitive data in them so get with the auditors and take care of it!**
  - Which Audit Trace classes do we start?
    - What audit information do we want?
    - To what destination?
  - Which tables need ‘AUDIT ALL’ ?
  - How many audit trace records will we produce?
  - Do we run the Audit Trace all the time?
  - What is the overhead?
  - How do we get reports from the Audit Trace data?
  - What other sources of audit information is there?
  - How do I set up enough reports to keep the Auditors busy?
  - How do we get the Auditors to do it?
    - How much of my time will I have to spend with the Auditors?

Audit Management Solution

- **Collect and correlate information from a variety of DB2 resources.**
  - Audit Trace Data, Log Analysis data
- **Provides a central resource for auditors to produce a coherent view of DB2 access information.**
- **Auditors should be able to access:**
  - Access attempts that DB2 denied – lack of authorization
  - SELECT, INSERT, UPDATE, and DELETE activity by user or by object.
  - CREATE, ALTER, and DROP operations against an audited object
  - Utility access to an audited object
  - DB2 commands entered – ie. GRANT / REVOKE
  - Assignment or modification of an authorization ID
- **Provide auditors with flexible options for examining the data in a centralized repository.**

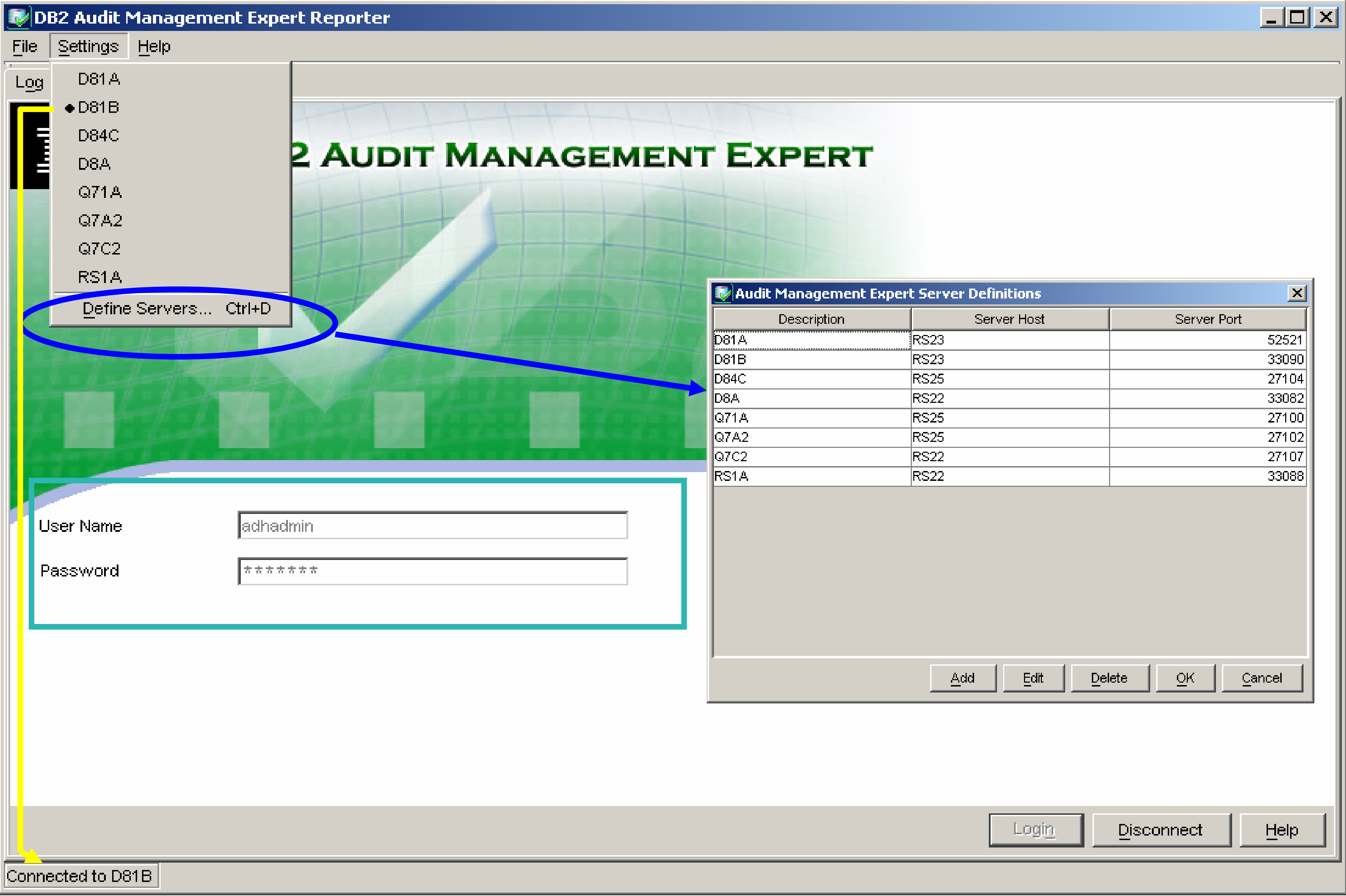
Audit Management Expert Architecture



IBM’s Compliance Suite

IBM Audit Management Expert Admin Client

ADMINISTRATION CLIENT



Description	Server Host	Server Port
D81A	RS23	52521
D81B	RS23	33090
D84C	RS25	27104
D8A	RS22	33082
Q71A	RS25	27100
Q7A2	RS25	27102
Q7C2	RS22	27107
RS1A	RS22	33088

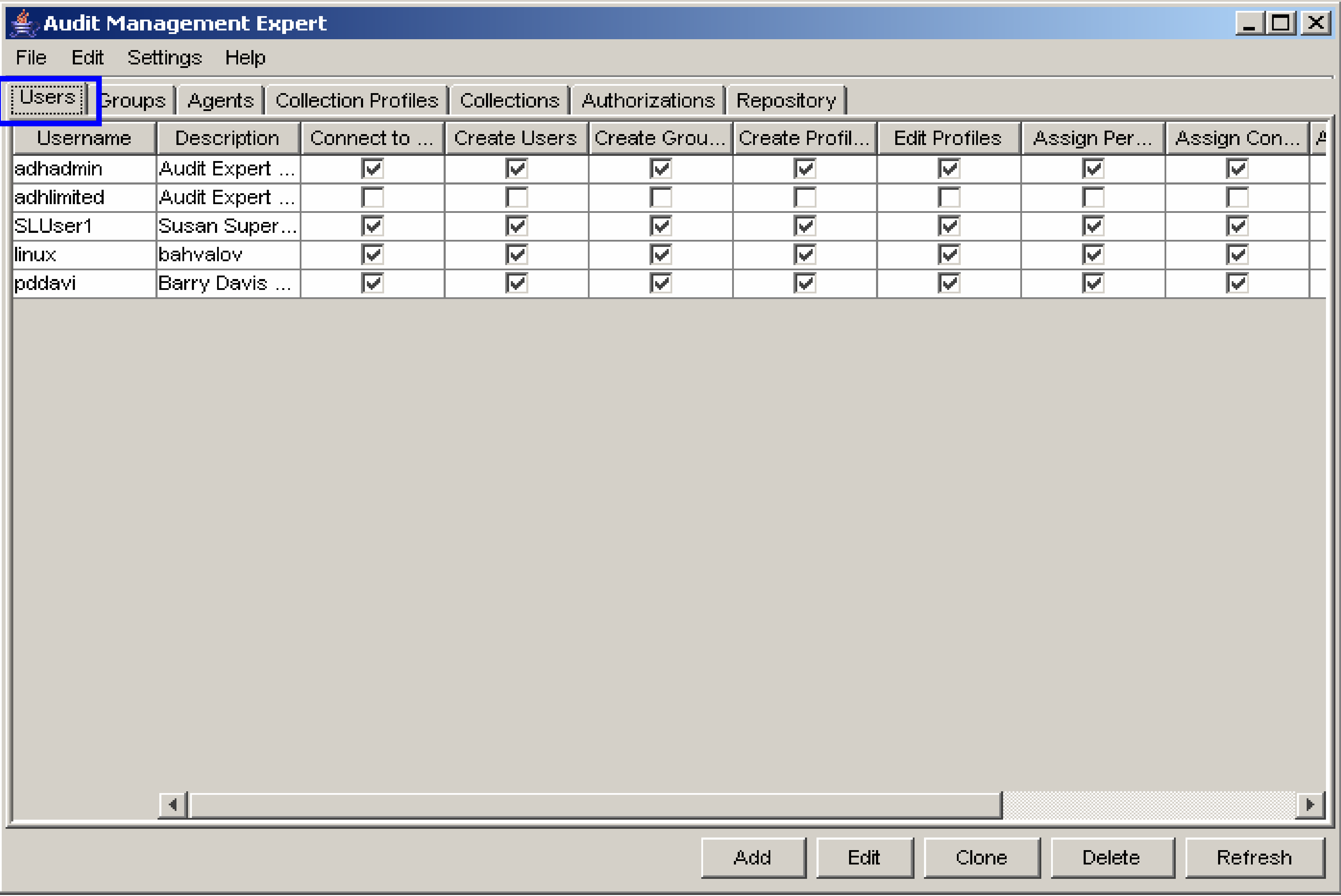
User Name: adhadmin

Password: *******

Connected to D81B

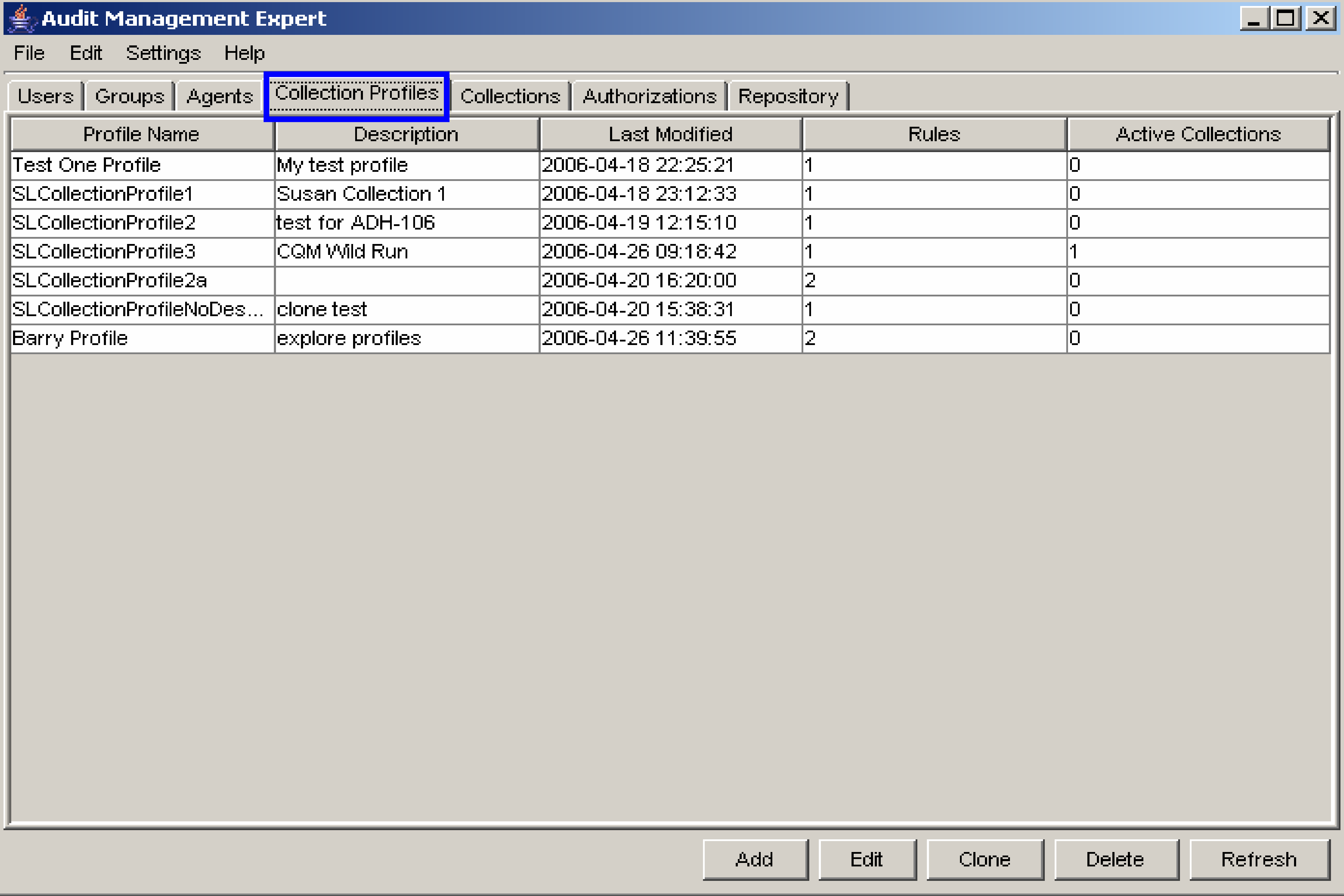
IBM Audit Management Expert

ADMINISTRATION CLIENT



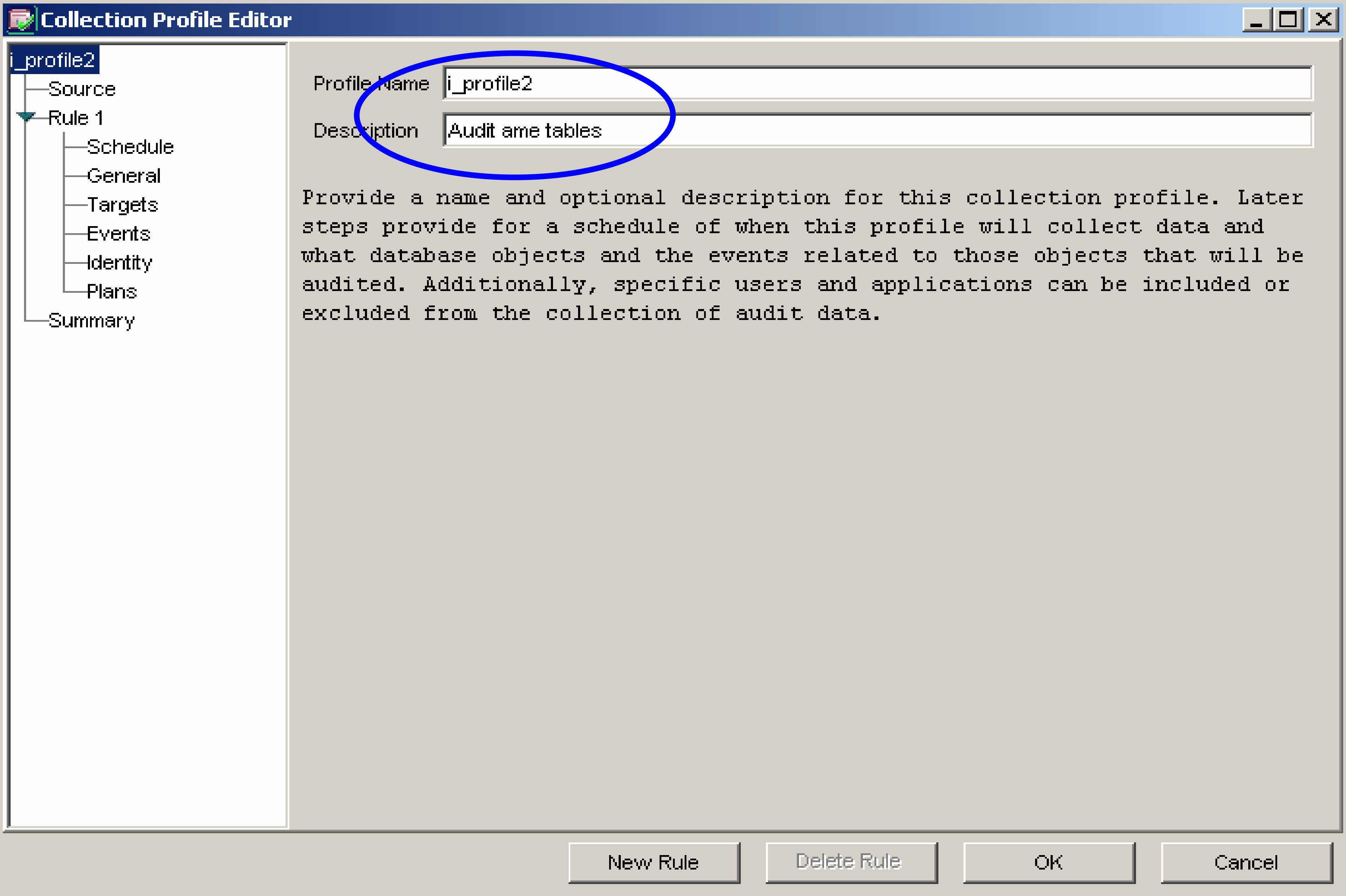
Username	Description	Connect to ...	Create Users	Create Grou...	Create Profil...	Edit Profiles	Assign Per...	Assign Con...
adhadmin	Audit Expert ...	☑	☑	☑	☑	☑	☑	☑
adhlimited	Audit Expert ...	□	□	□	□	□	□	□
SLUser1	Susan Super...	☑	☑	☑	☑	☑	☑	☑
linux	bahvalov	☑	☑	☑	☑	☑	☑	☑
pddavi	Barry Davis ...	☑	☑	☑	☑	☑	☑	☑

ADMINISTRATION CLIENT



Profile Name	Description	Last Modified	Rules	Active Collections
Test One Profile	My test profile	2006-04-18 22:25:21	1	0
SLCollectionProfile1	Susan Collection 1	2006-04-18 23:12:33	1	0
SLCollectionProfile2	test for ADH-106	2006-04-19 12:15:10	1	0
SLCollectionProfile3	CQM Wild Run	2006-04-26 09:18:42	1	1
SLCollectionProfile2a		2006-04-20 16:20:00	2	0
SLCollectionProfileNoDes...	clone test	2006-04-20 15:38:31	1	0
Barry Profile	explore profiles	2006-04-26 11:39:55	2	0

ADMINISTRATION CLIENT

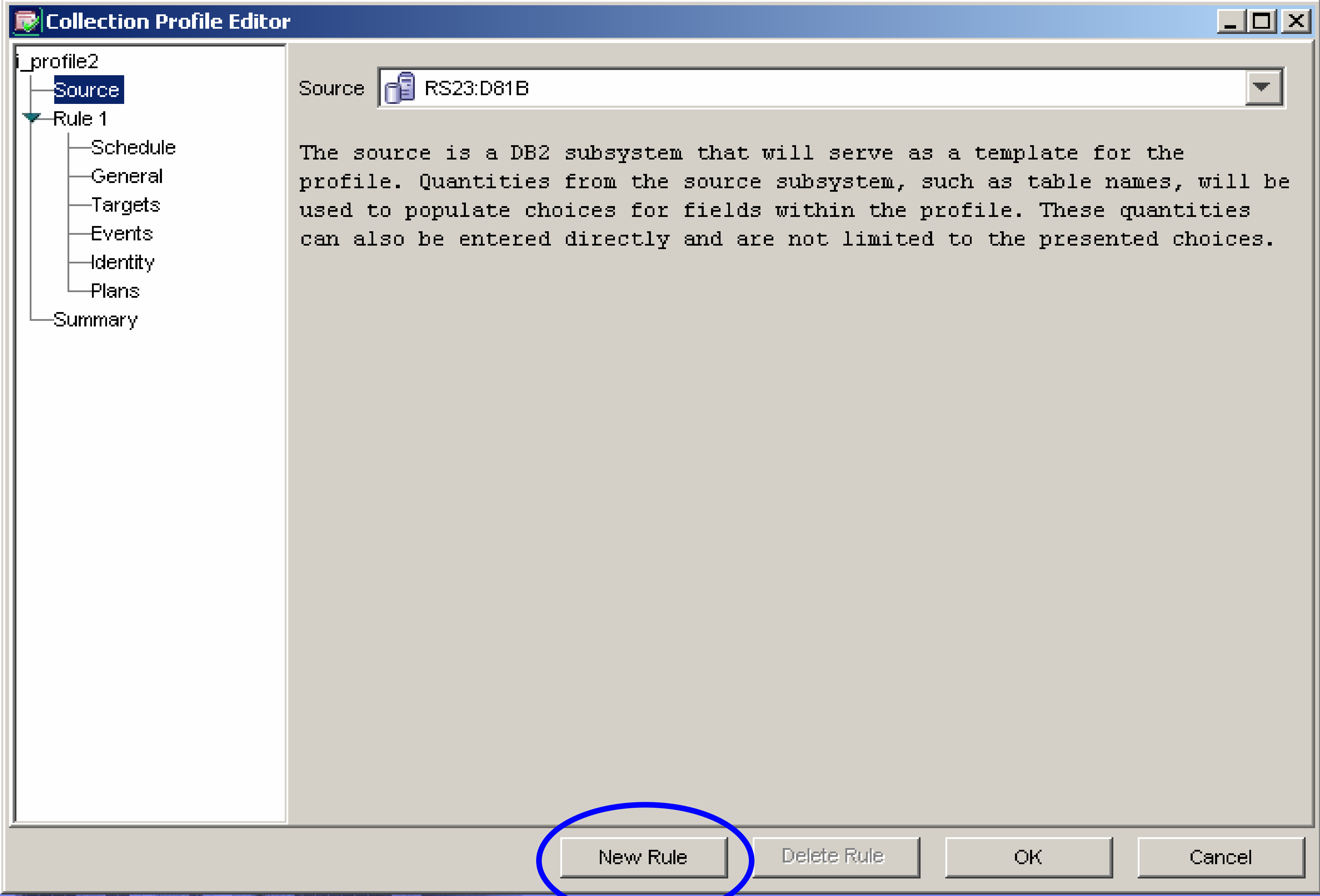


Collection Profile Editor

Profile Name: i_profile2

Description: Audit ame tables

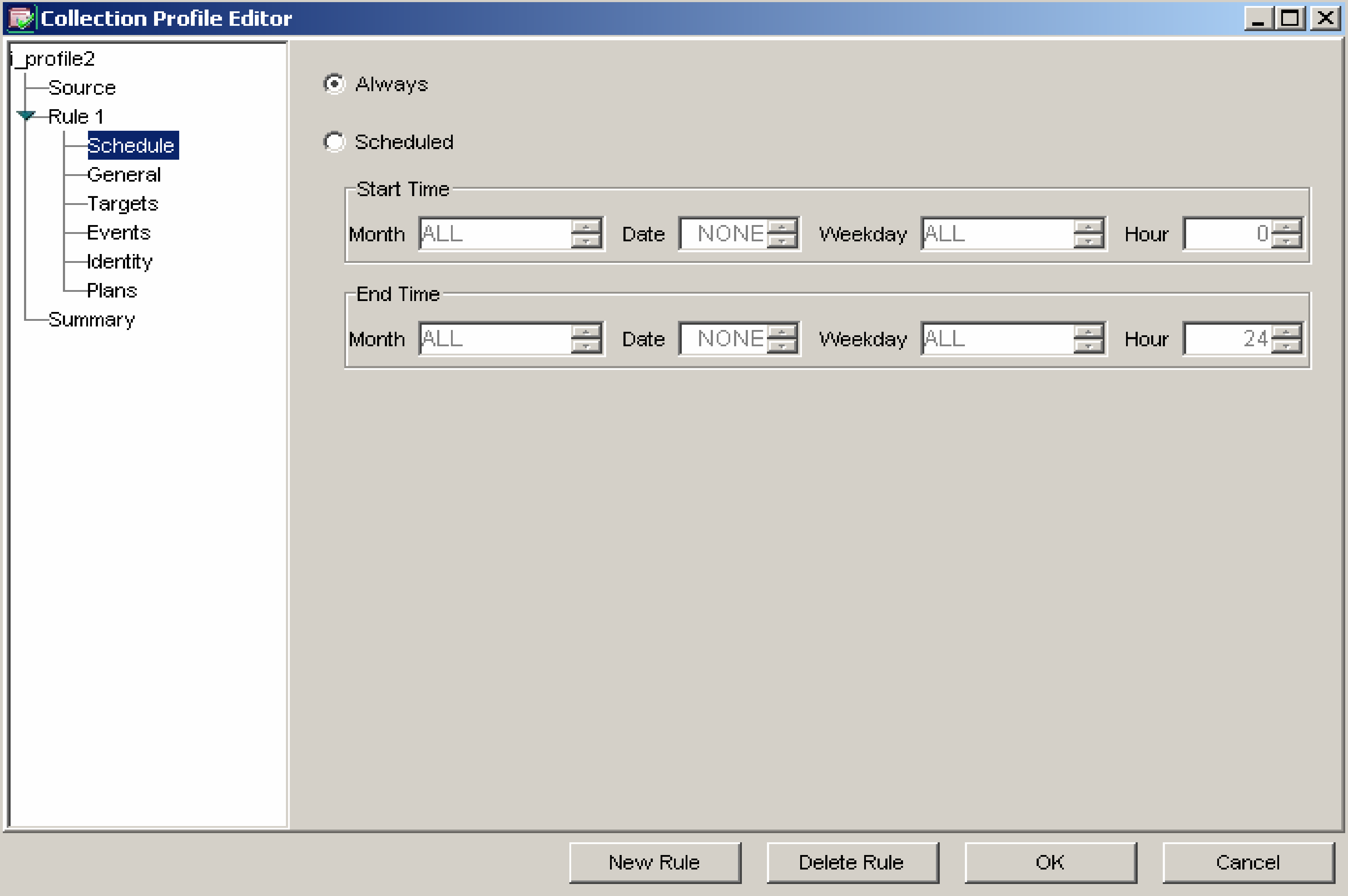
Provide a name and optional description for this collection profile. Later steps provide for a schedule of when this profile will collect data and what database objects and the events related to those objects that will be audited. Additionally, specific users and applications can be included or excluded from the collection of audit data.



Source: RS23:D81B

The source is a DB2 subsystem that will serve as a template for the profile. Quantities from the source subsystem, such as table names, will be used to populate choices for fields within the profile. These quantities can also be entered directly and are not limited to the presented choices.

ADMINISTRATION CLIENT



Collection Profile Editor

● Always

○ Scheduled

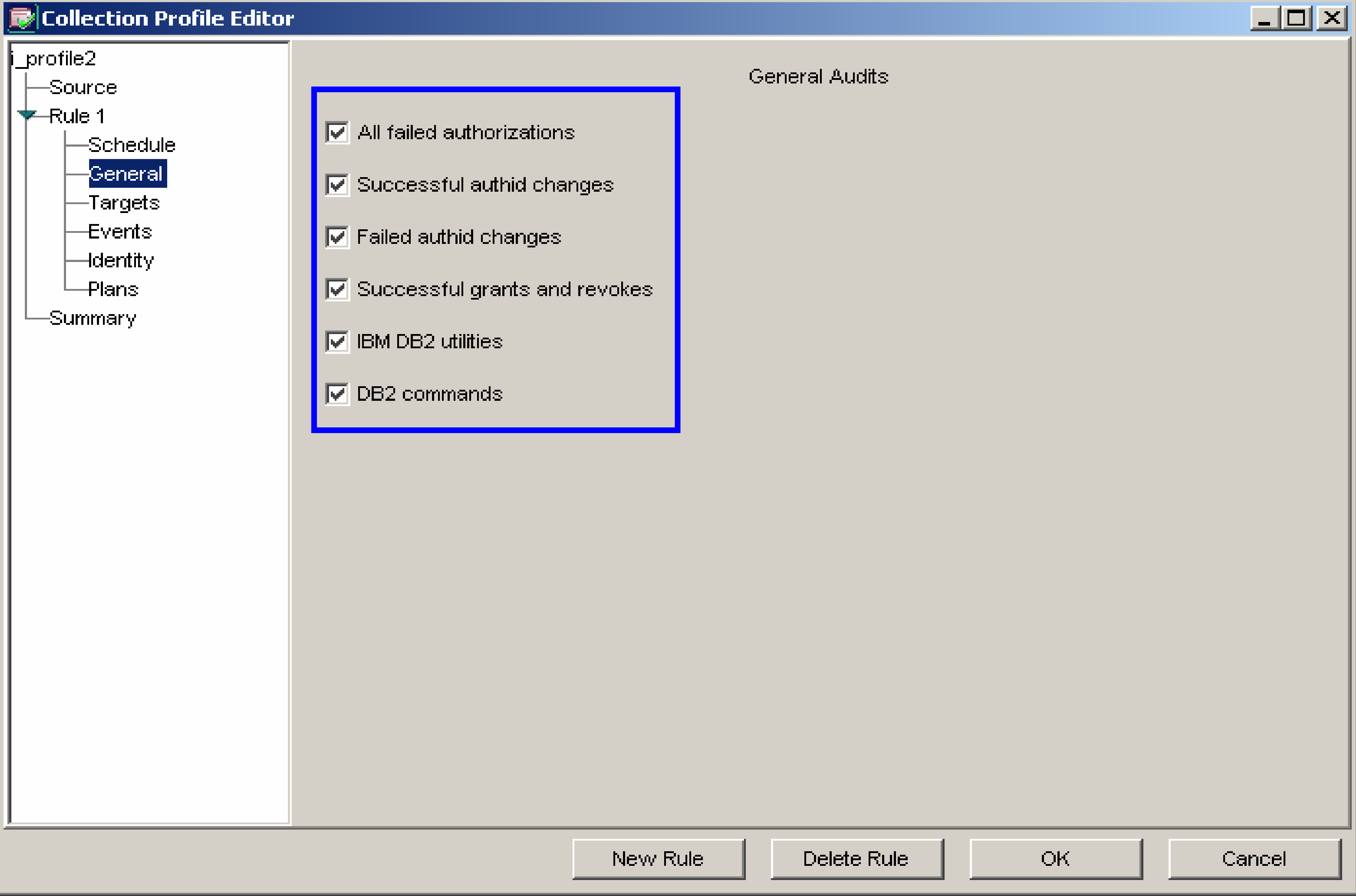
Start Time

Month: ALL Date: NONE Weekday: ALL Hour: 0

End Time

Month: ALL Date: NONE Weekday: ALL Hour: 24

ADMINISTRATION CLIENT



Collection Profile Editor

General Audits

☑ All failed authorizations

☑ Successful authid changes

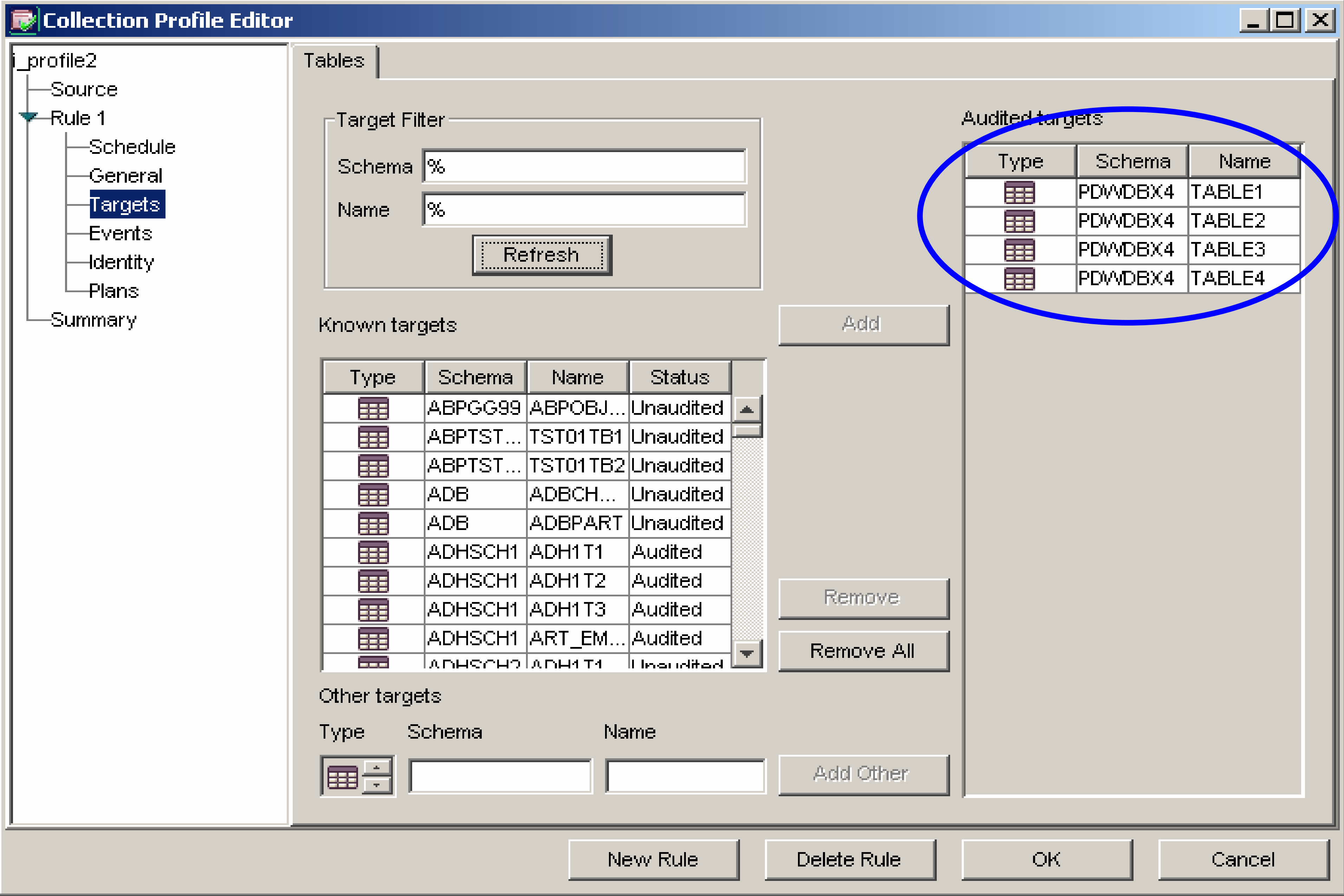
☑ Failed authid changes

☑ Successful grants and revokes

☑ IBM DB2 utilities

☑ DB2 commands

ADMINISTRATION CLIENT



Target Filter

Schema: %

Name: %

Known targets

Type	Schema	Name	Status
▦	ABPGG99	ABPOBJ...	Unaudited
▦	ABPTST...	TST01TB1	Unaudited
▦	ABPTST...	TST01TB2	Unaudited
▦	ADB	ADBCH...	Unaudited
▦	ADB	ADBPART	Unaudited
▦	ADHSCH1	ADH1T1	Audited
▦	ADHSCH1	ADH1T2	Audited
▦	ADHSCH1	ADH1T3	Audited
▦	ADHSCH1	ART_EM...	Audited
▦	ADHSCH2	ADH1T1	Unaudited

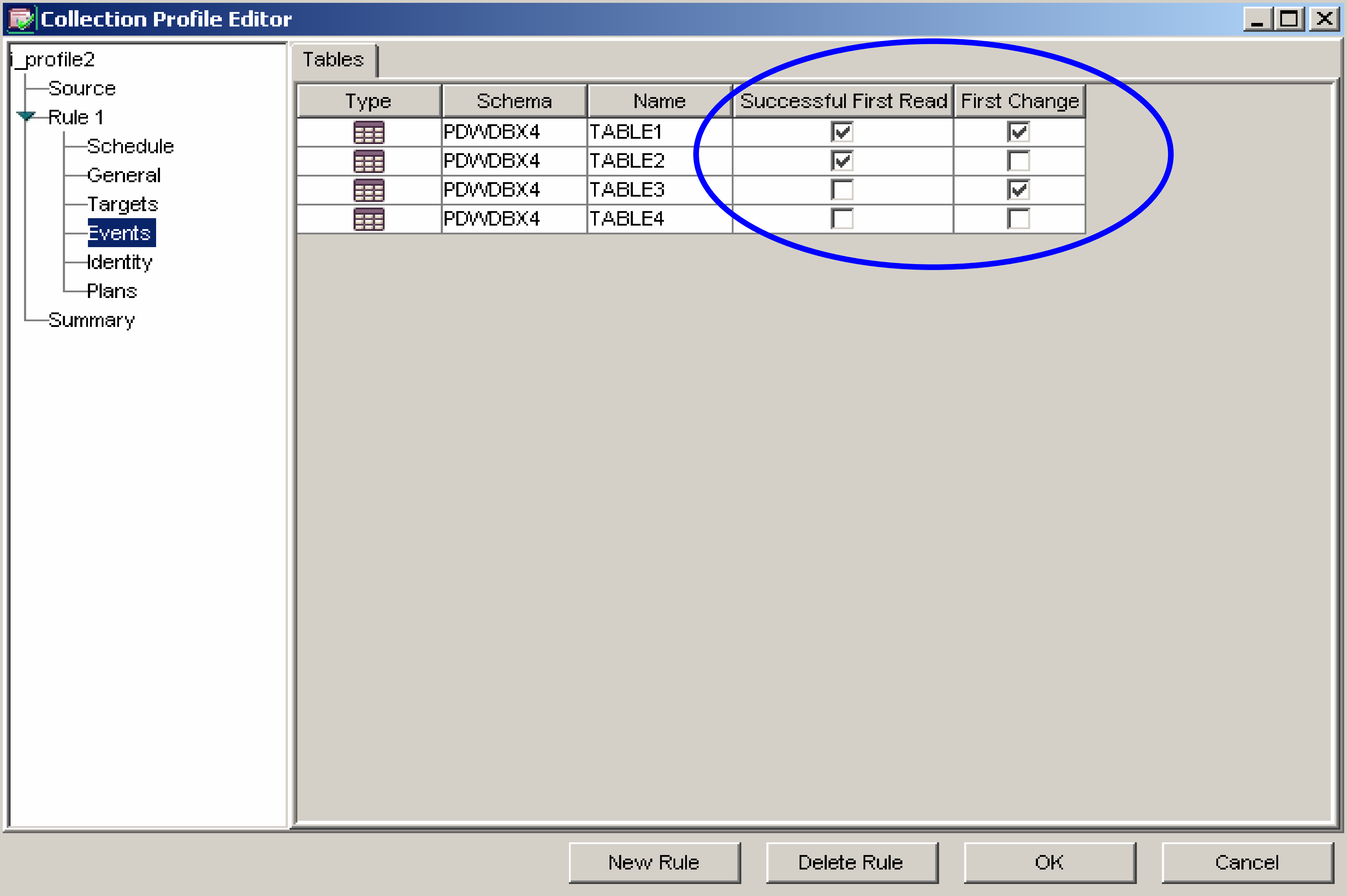
Other targets

Type: ▦ Schema: Name:

Audited targets

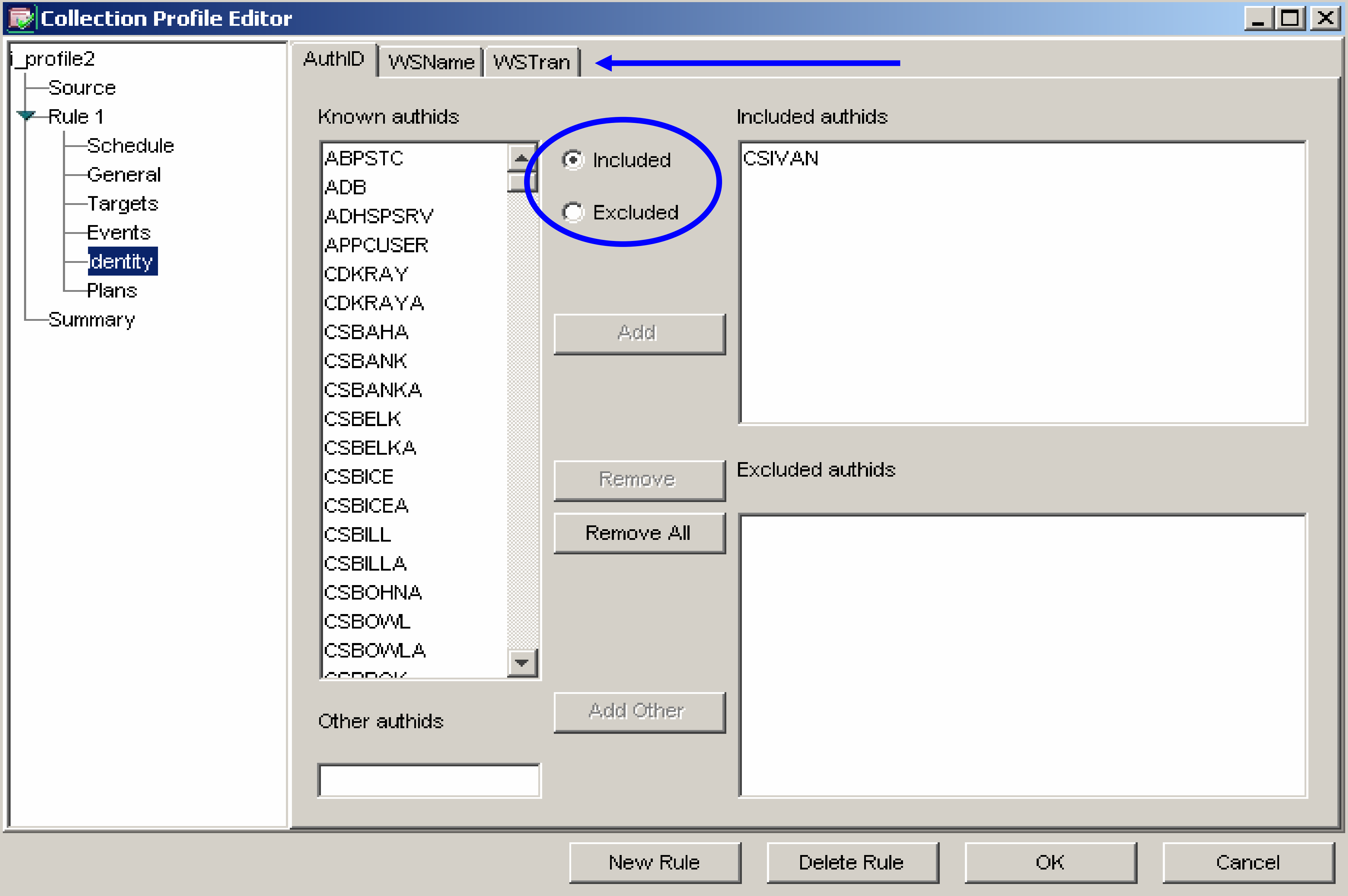
Type	Schema	Name
▦	PDWDBX4	TABLE1
▦	PDWDBX4	TABLE2
▦	PDWDBX4	TABLE3
▦	PDWDBX4	TABLE4

ADMINISTRATION CLIENT



Collection Profile Editor

Type	Schema	Name	Successful First Read	First Change
▦	PDWDBX4	TABLE1	☑	☑
▦	PDWDBX4	TABLE2	☑	□
▦	PDWDBX4	TABLE3	□	☑
▦	PDWDBX4	TABLE4	□	□



Known authids

ABPSTC
ADB
ADHSPSRV
APPCUSER
CDKRAY
CDKRAYA
CSBAHA
CSBANK
CSBANKA
CSBELK
CSBELKA
CSBICE
CSBICEA
CSBILL
CSBILLA
CSBOHNA
CSBOWL
CSBOWLA

● Included
○ Excluded

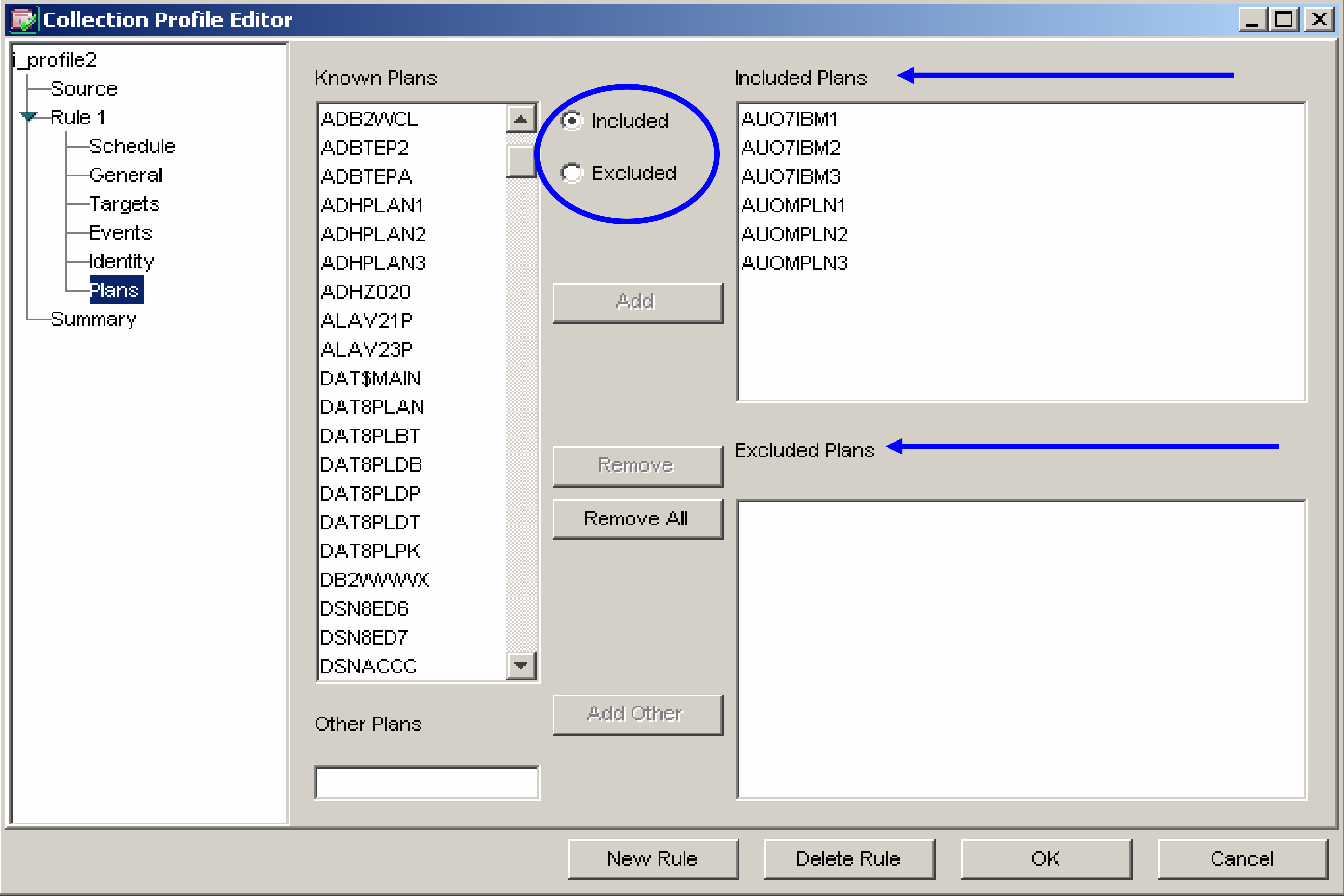
Included authids

CSIVAN

Excluded authids

Other authids

ADMINISTRATION CLIENT



Collection Profile Editor

- i_profile2
  - Source
  - Rule 1
    - Schedule
    - General
    - Targets
    - Events
    - Identity
    - Plans
  - Summary

Known Plans

ADB2WCL
ADBTEP2
ADBTEPA
ADHPLAN1
ADHPLAN2
ADHPLAN3
ADHZ020
ALAV21P
ALAV23P
DAT$MAIN
DAT8PLAN
DAT8PLBT
DAT8PLDB
DAT8PLDP
DAT8PLDT
DAT8PLPK
DB2WWWX
DSN8ED6
DSN8ED7
DSNACCC

● Included
○ Excluded

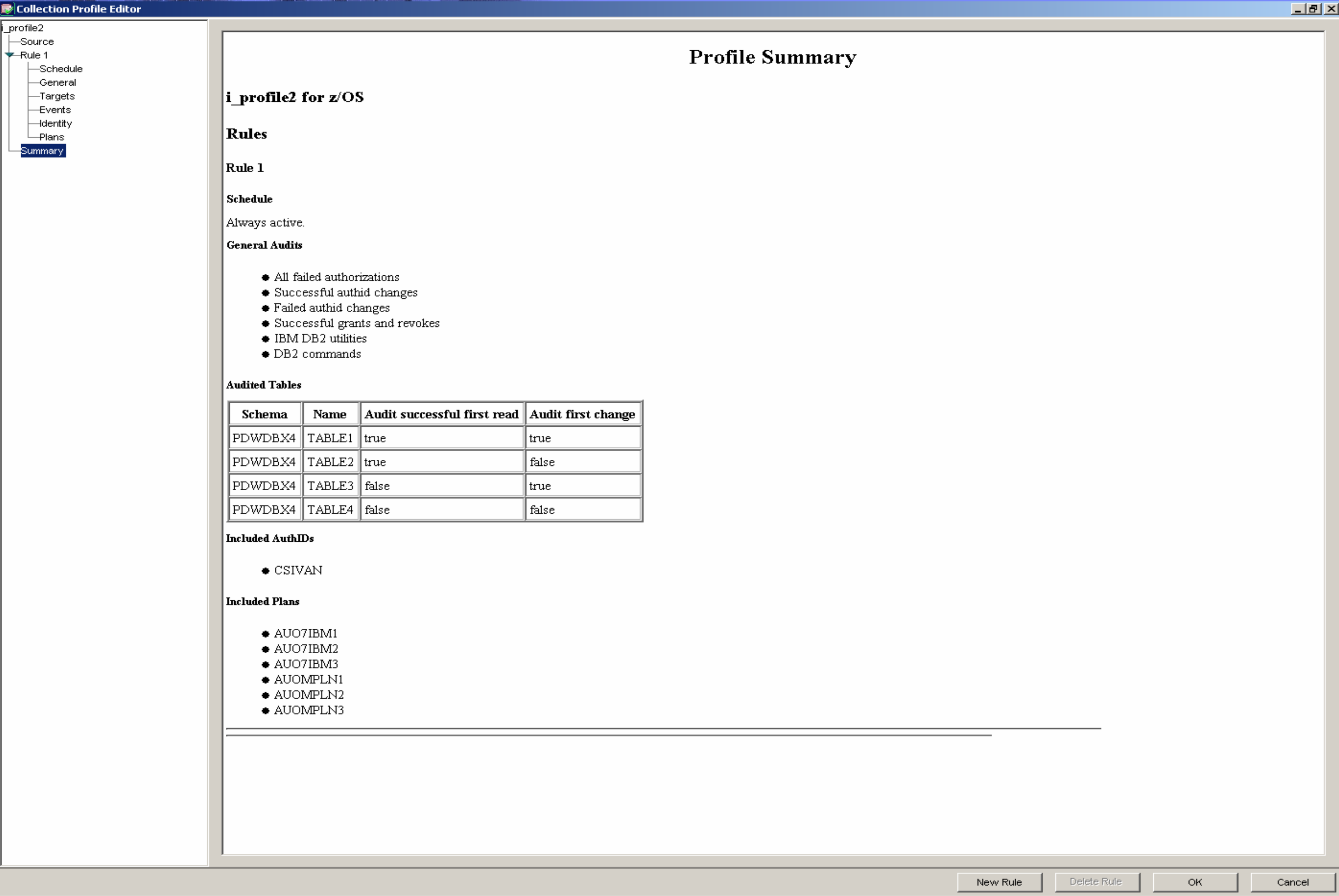
Included Plans

AUO7IBM1
AUO7IBM2
AUO7IBM3
AUOMPLN1
AUOMPLN2
AUOMPLN3

Excluded Plans

Other Plans

ADMINISTRATION CLIENT



Profile Summary

i_profile2 for z/OS

Rules

Rule 1

Schedule

Always active.

General Audits

- All failed authorizations
- Successful authid changes
- Failed authid changes
- Successful grants and revokes
- IBM DB2 utilities
- DB2 commands

Audited Tables

Schema	Name	Audit successful first read	Audit first change
PDWDBX4	TABLE1	true	true
PDWDBX4	TABLE2	true	false
PDWDBX4	TABLE3	false	true
PDWDBX4	TABLE4	false	false

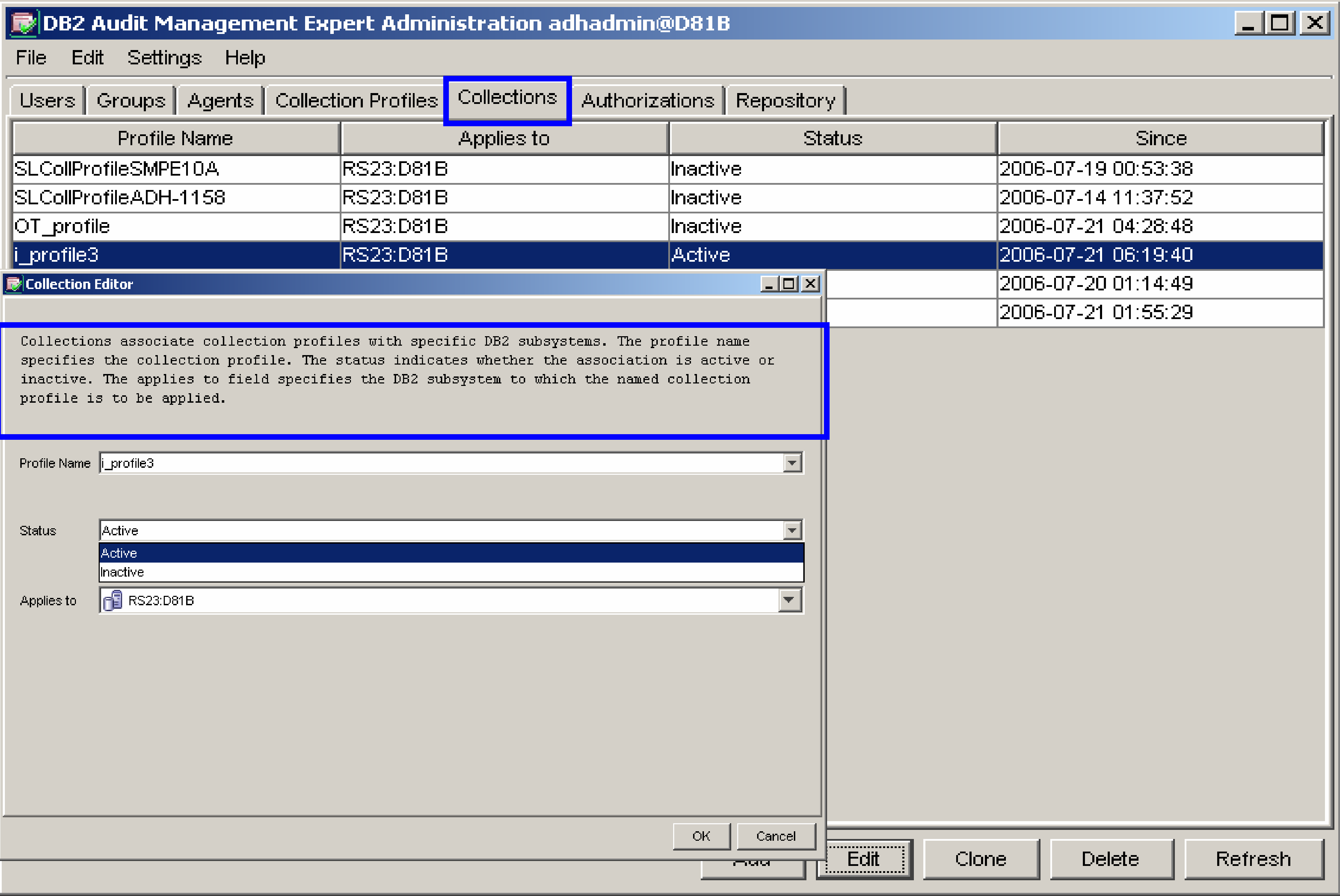
Included AuthIDs

- CSIVAN

Included Plans

- AUO7IBM1
- AUO7IBM2
- AUO7IBM3
- AUOMPLN1
- AUOMPLN2
- AUOMPLN3

ADMINISTRATION CLIENT



Profile Name	Applies to	Status	Since
SLCollProfileSMPE10A	RS23:D81B	Inactive	2006-07-19 00:53:38
SLCollProfileADH-1158	RS23:D81B	Inactive	2006-07-14 11:37:52
OT_profile	RS23:D81B	Inactive	2006-07-21 04:28:48
i_profile3	RS23:D81B	Active	2006-07-21 06:19:40
			2006-07-20 01:14:49
			2006-07-21 01:55:29

Collections associate collection profiles with specific DB2 subsystems. The profile name specifies the collection profile. The status indicates whether the association is active or inactive. The applies to field specifies the DB2 subsystem to which the named collection profile is to be applied.

Profile Name: i_profile3

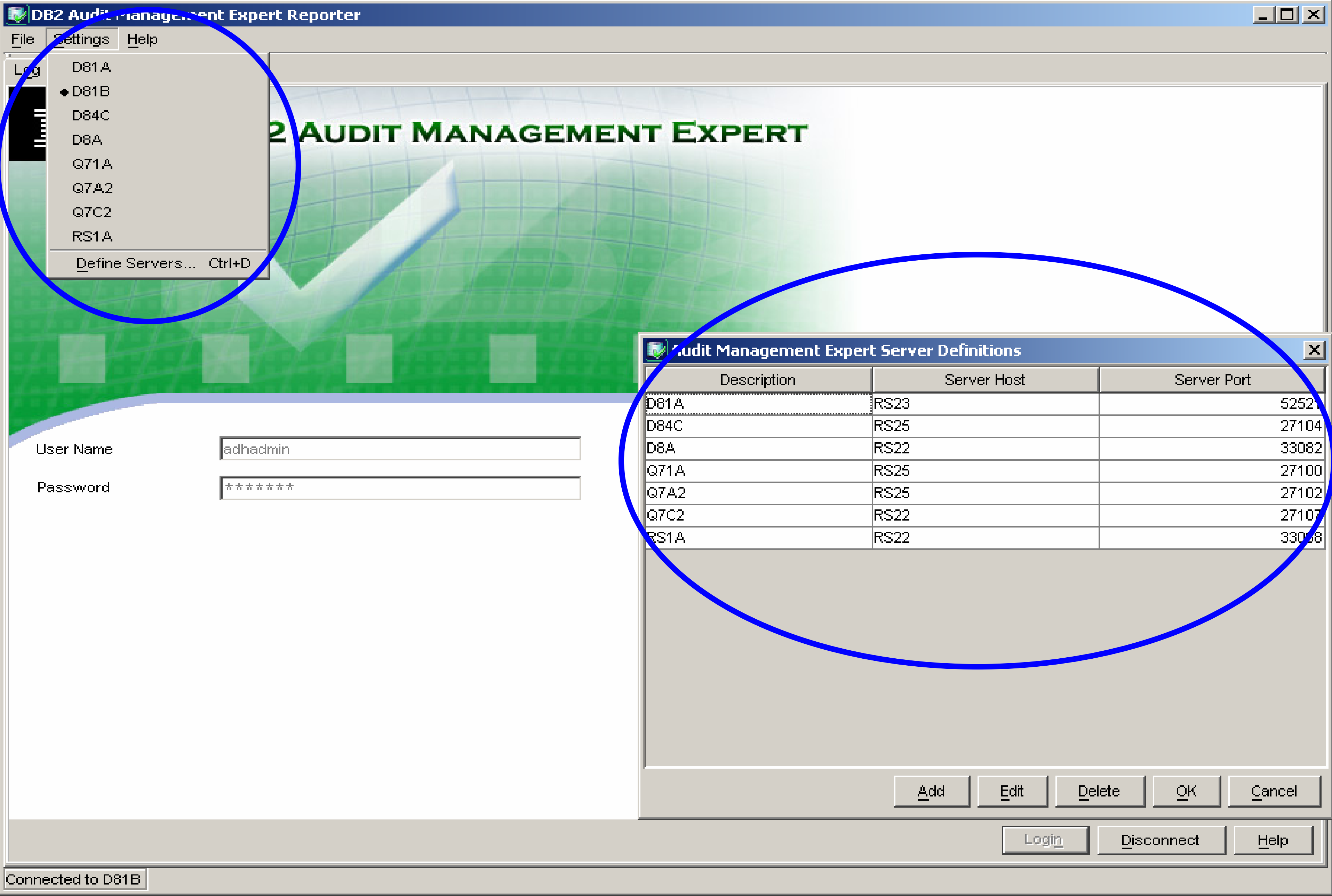
Status: Active

Applies to: RS23:D81B

IBM’s Compliance Suite

IBM Audit Management Expert Report Client

REPORT CLIENT



User Name adhadmin

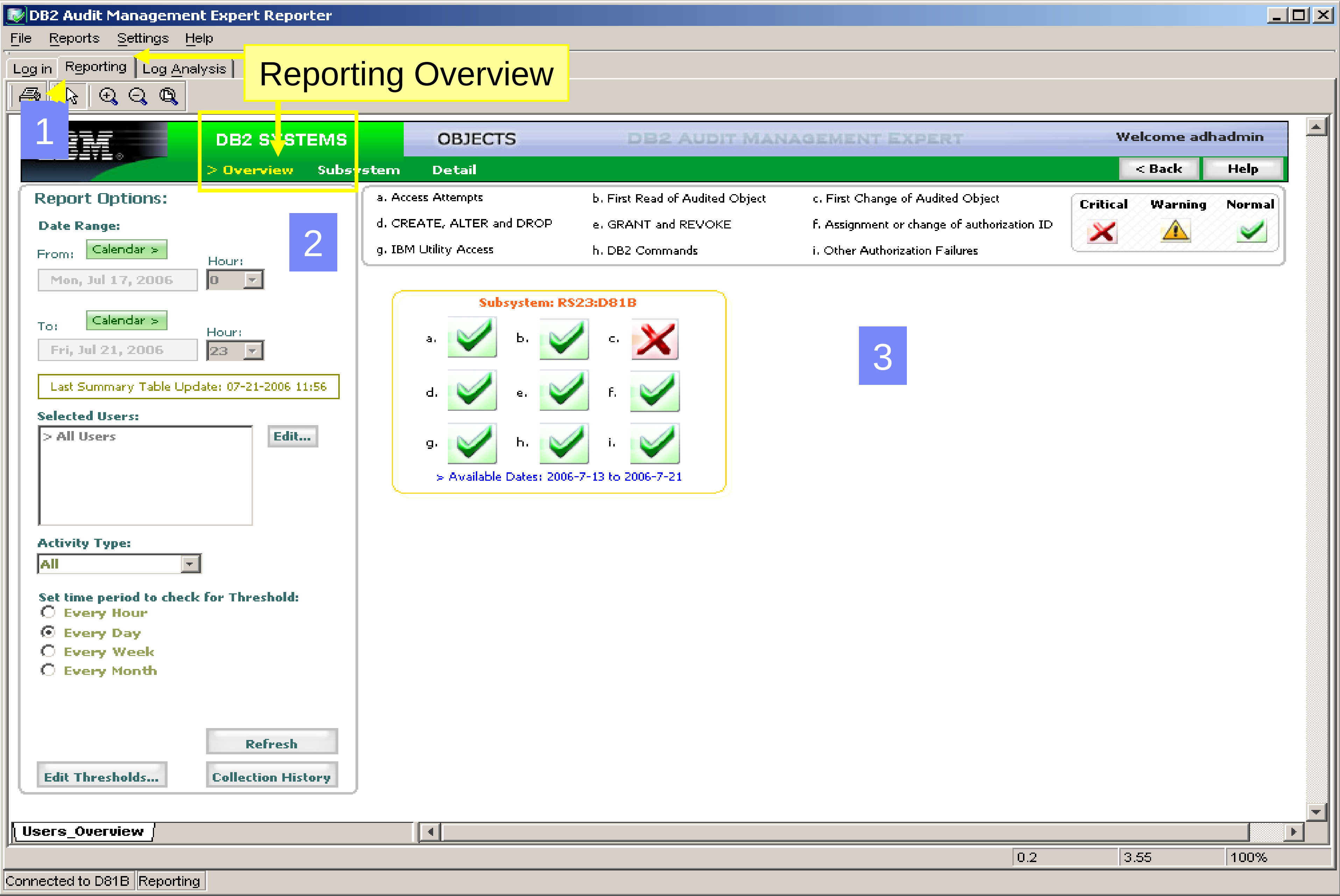
Password *******

Audit Management Expert Server Definitions

Description	Server Host	Server Port
D81A	RS23	52521
D84C	RS25	27104
D8A	RS22	33082
Q71A	RS25	27100
Q7A2	RS25	27102
Q7C2	RS22	27107
RS1A	RS22	33068

Connected to D81B

REPORT CLIENT



DB2 Audit Management Expert Reporter
File Reports Settings Help
Log in Reporting Log Analysis
Reporting Overview
1
2
3
DB2 SYSTEMS
OBJECTS
DB2 AUDIT MANAGEMENT EXPERT
Welcome adhadmin
> Overview Subsystem Detail
< Back
Help

Report Options:

Date Range:

From: Calendar > Mon, Jul 17, 2006 Hour: 0

To: Calendar > Fri, Jul 21, 2006 Hour: 23

Last Summary Table Update: 07-21-2006 11:56

Selected Users: > All Users Edit...

Activity Type: All

Set time period to check for Threshold:

○ Every Hour
● Every Day
○ Every Week
○ Every Month

Refresh

Edit Thresholds... Collection History

a. Access Attempts
b. First Read of Audited Object
c. First Change of Audited Object
d. CREATE, ALTER and DROP
e. GRANT and REVOKE
f. Assignment or change of authorization ID
g. IBM Utility Access
h. DB2 Commands
i. Other Authorization Failures

Critical	Warning	Normal
✗	⚠	✓

Subsystem: RS23:D81B

a.	✓	b.	✓	c.	✗
d.	✓	e.	✓	f.	✓
g.	✓	h.	✓	i.	✓

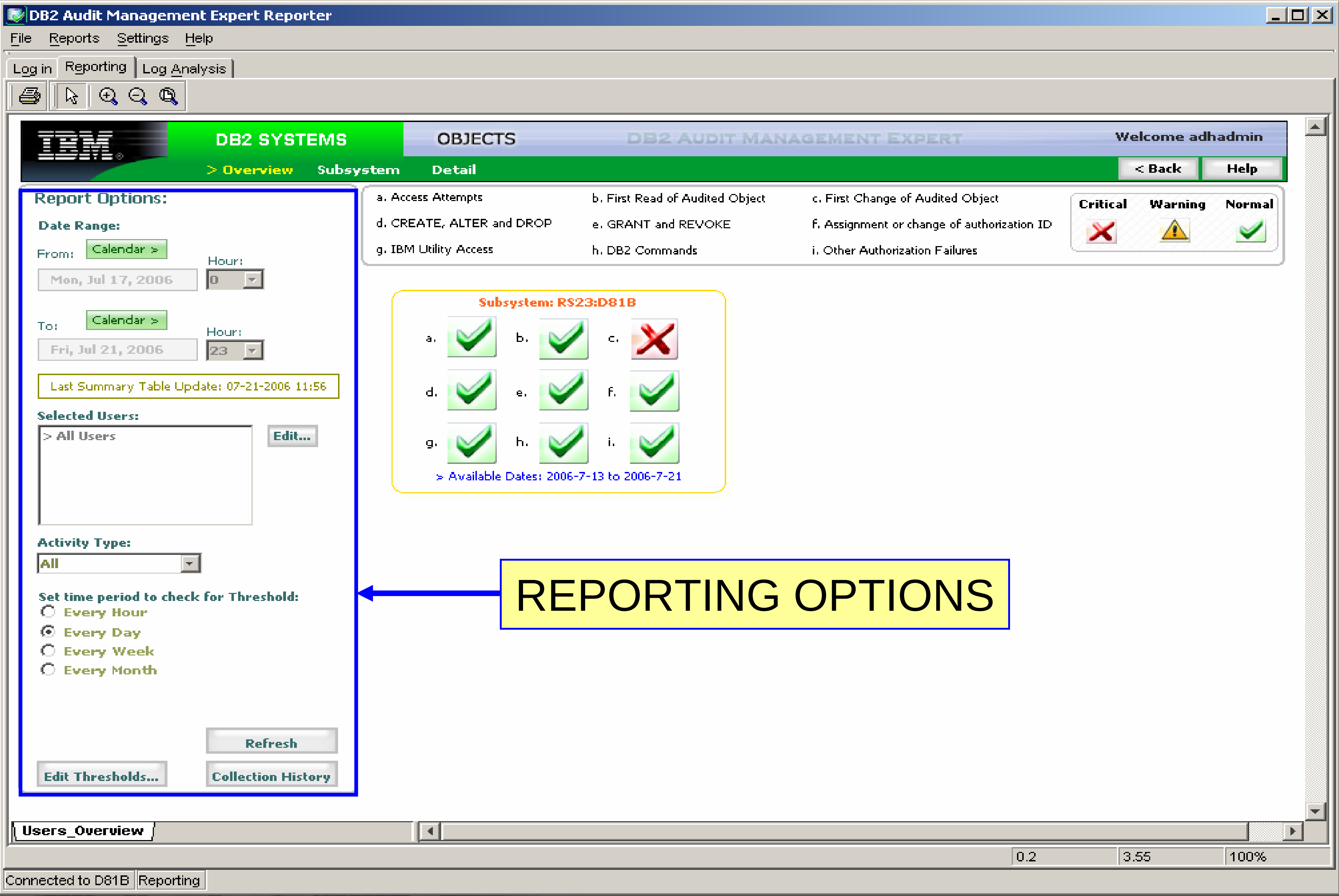
> Available Dates: 2006-7-13 to 2006-7-21

Users_Overview

0.2 3.55 100%

Connected to D81B Reporting

REPORT CLIENT



Welcome adhadmin

Report Options:

Date Range:

From: Mon, Jul 17, 2006 Hour: 0

To: Fri, Jul 21, 2006 Hour: 23

Last Summary Table Update: 07-21-2006 11:56

Selected Users: > All Users

Activity Type: All

Set time period to check for Threshold:

○ Every Hour
● Every Day
○ Every Week
○ Every Month

a. Access Attempts
b. First Read of Audited Object
c. First Change of Audited Object
d. CREATE, ALTER and DROP
e. GRANT and REVOKE
f. Assignment or change of authorization ID
g. IBM Utility Access
h. DB2 Commands
i. Other Authorization Failures

Critical	Warning	Normal
✗	⚠	✓

Subsystem: RS23:D81B

a.	✓	b.	✓	c.	✗
d.	✓	e.	✓	f.	✓
g.	✓	h.	✓	i.	✓

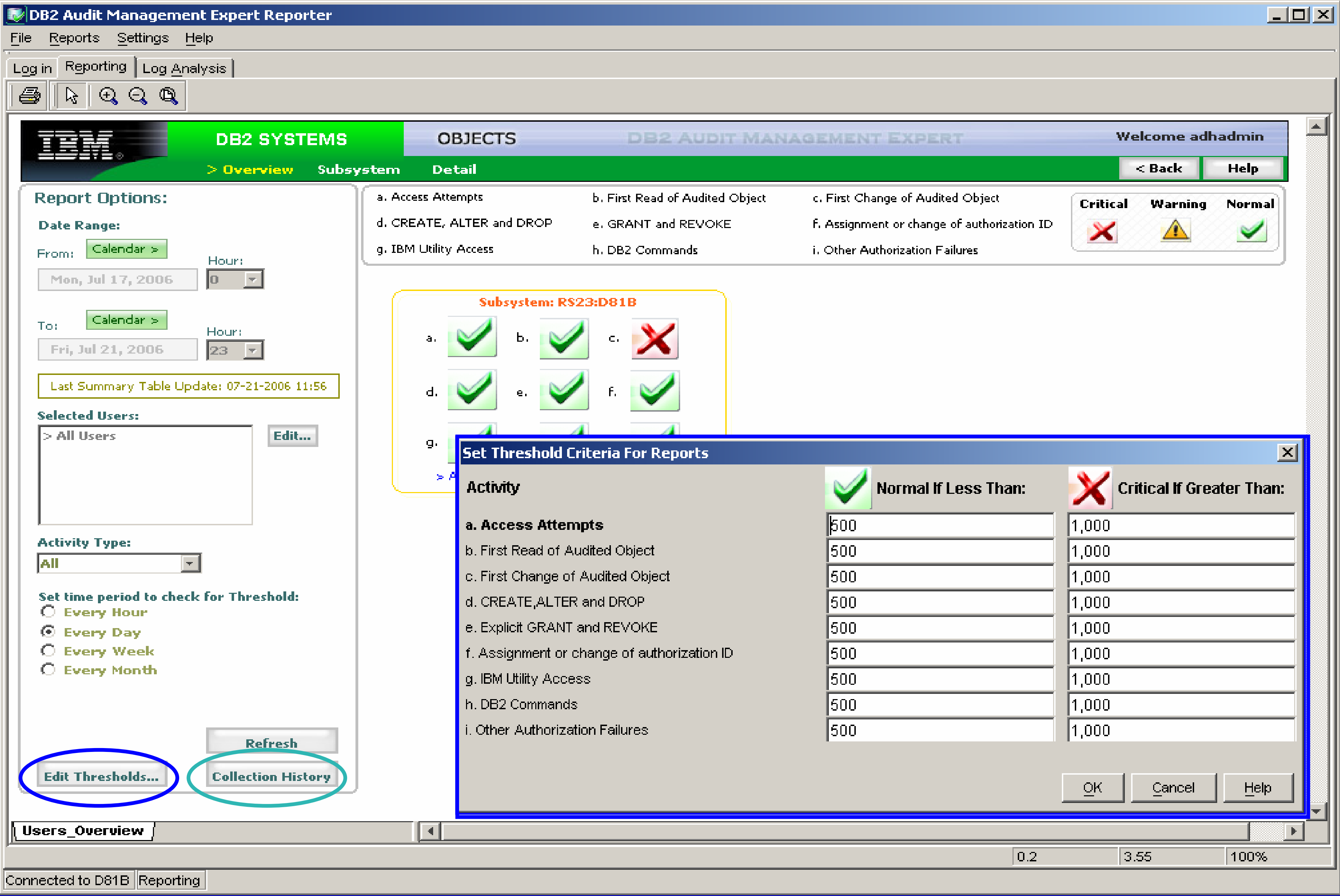
> Available Dates: 2006-7-13 to 2006-7-21

REPORTING OPTIONS

0.2 | 3.55 | 100%

Connected to D81B | Reporting

REPORT CLIENT


DB2 Audit Management Expert Reporter
File Reports Settings Help
Log in Reporting Log Analysis
DB2 SYSTEMS
OBJECTS
DB2 AUDIT MANAGEMENT EXPERT
Welcome adhadmin
> Overview Subsystem Detail
< Back
Help
Calendar >
Calendar >
Edit...
Refresh
Edit Thresholds...
Collection History
Users_Overview
OK
Cancel
Help

Report Options:

Date Range:

From: Mon, Jul 17, 2006 Hour: 0

To: Fri, Jul 21, 2006 Hour: 23

Last Summary Table Update: 07-21-2006 11:56

Selected Users: > All Users

Activity Type: All

Set time period to check for Threshold:

○ Every Hour
● Every Day
○ Every Week
○ Every Month

a. Access Attempts
b. First Read of Audited Object
c. First Change of Audited Object
d. CREATE, ALTER and DROP
e. GRANT and REVOKE
f. Assignment or change of authorization ID
g. IBM Utility Access
h. DB2 Commands
i. Other Authorization Failures

Critical	Warning	Normal
✗	⚠	✓

Subsystem: RS23:D81B

a.	✓	b.	✓	c.	✗
d.	✓	e.	✓	f.	✓
g.					

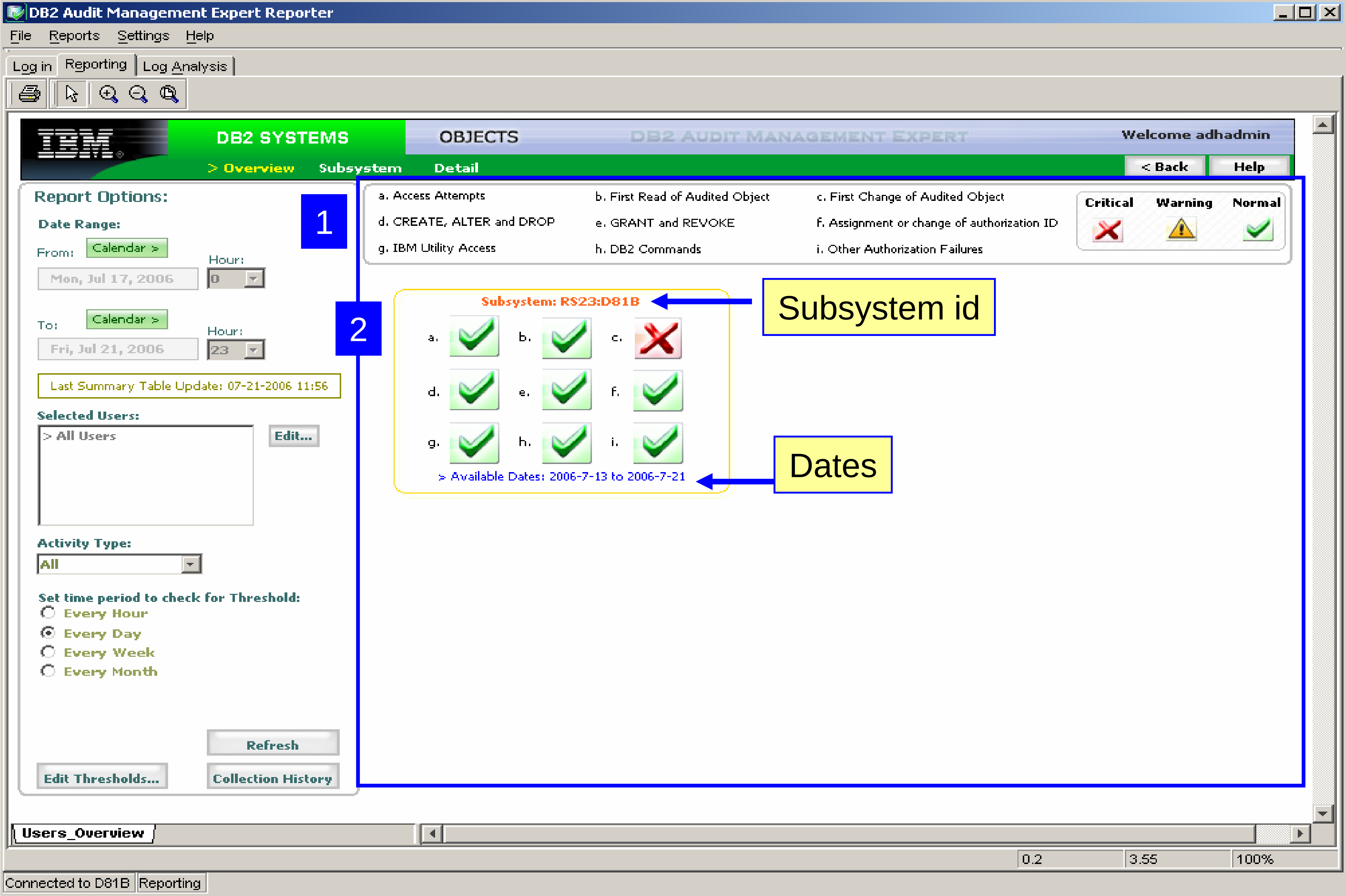
Set Threshold Criteria For Reports

Activity	✓ Normal If Less Than:	✗ Critical If Greater Than:
a. Access Attempts	500	1,000
b. First Read of Audited Object	500	1,000
c. First Change of Audited Object	500	1,000
d. CREATE,ALTER and DROP	500	1,000
e. Explicit GRANT and REVOKE	500	1,000
f. Assignment or change of authorization ID	500	1,000
g. IBM Utility Access	500	1,000
h. DB2 Commands	500	1,000
i. Other Authorization Failures	500	1,000

0.2 3.55 100%

Connected to D81B Reporting

REPORT CLIENT



Report Options:

Date Range:

From: Calendar > Mon, Jul 17, 2006 Hour: 0

To: Calendar > Fri, Jul 21, 2006 Hour: 23

Last Summary Table Update: 07-21-2006 11:56

Selected Users: > All Users

Activity Type: All

Set time period to check for Threshold:
○ Every Hour
● Every Day
○ Every Week
○ Every Month

a. Access Attempts
b. First Read of Audited Object
c. First Change of Audited Object
d. CREATE, ALTER and DROP
e. GRANT and REVOKE
f. Assignment or change of authorization ID
g. IBM Utility Access
h. DB2 Commands
i. Other Authorization Failures

Critical	Warning	Normal
✗	⚠	✓

Subsystem: RS23:D81B

a.	✓	b.	✓	c.	✗
d.	✓	e.	✓	f.	✓
g.	✓	h.	✓	i.	✓

> Available Dates: 2006-7-13 to 2006-7-21

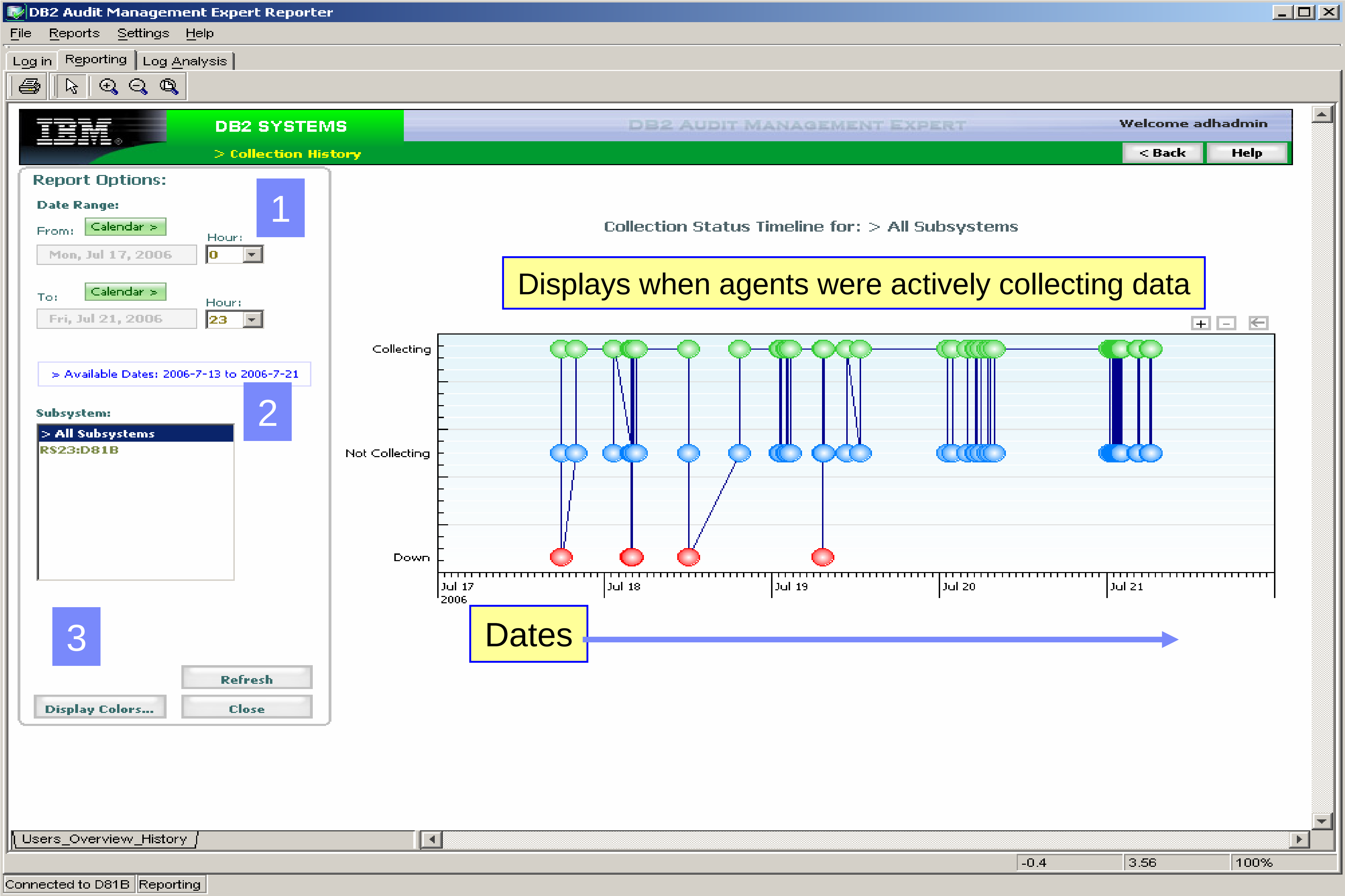
1

2

Subsystem id

Dates

REPORT CLIENT



Report Options:

Date Range:

From: Mon, Jul 17, 2006 Hour: 0

To: Fri, Jul 21, 2006 Hour: 23

> Available Dates: 2006-7-13 to 2006-7-21

Subsystem:

> All Subsystems

RS23:D81B

Collection Status Timeline for: > All Subsystems

1

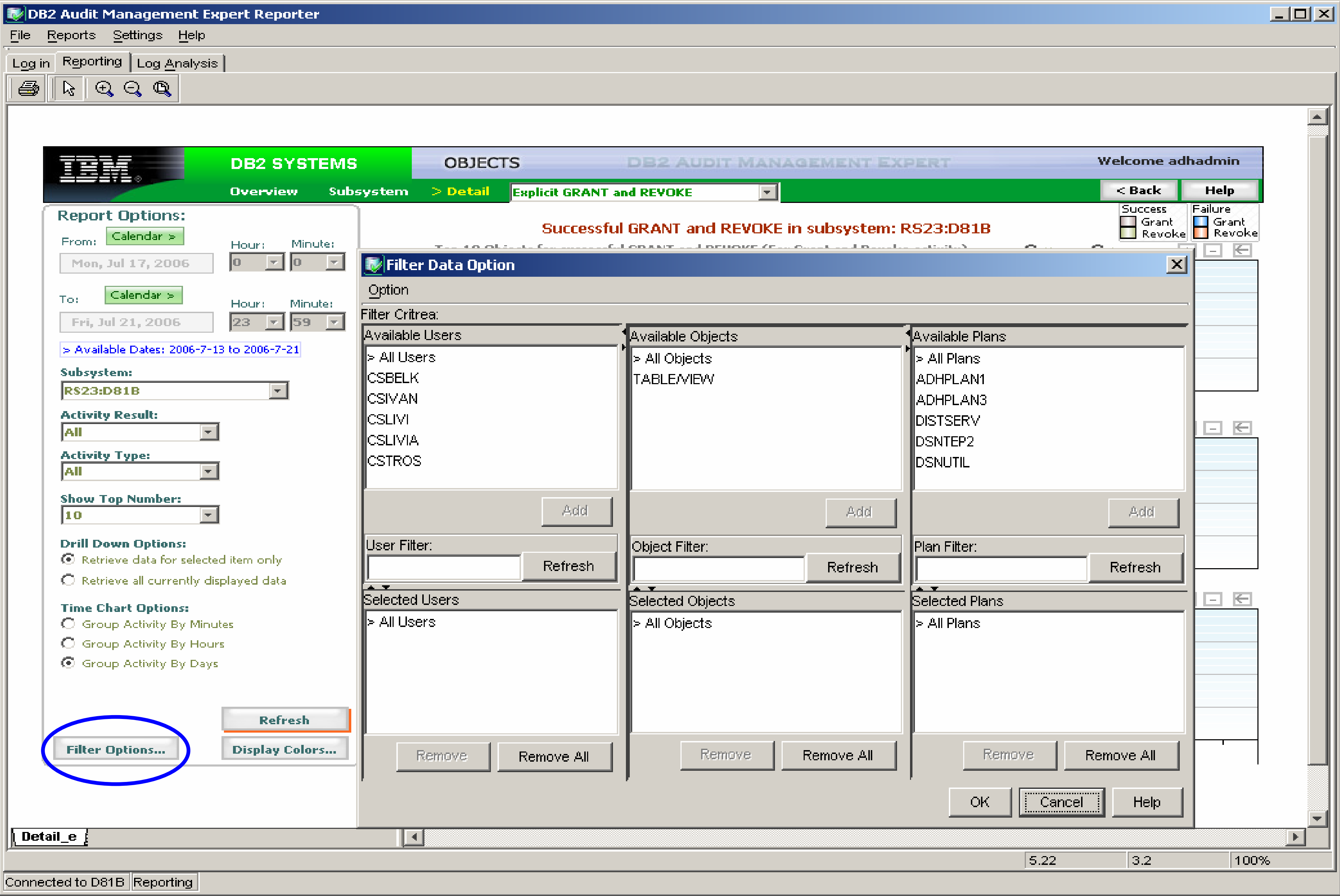
2

3

Displays when agents were actively collecting data

Dates

REPORT CLIENT



DB2 Audit Management Expert Reporter

File Reports Settings Help
Log in Reporting Log Analysis
DB2 SYSTEMS
OBJECTS
DB2 AUDIT MANAGEMENT EXPERT
Welcome adhadmin
Overview Subsystem > Detail
< Back
Help

Explicit GRANT and REVOKE

Success: Grant / Revoke — Failure: Grant / Revoke

Successful GRANT and REVOKE in subsystem: RS23:D81B

Report Options:

From: Mon, Jul 17, 2006 — Hour: 0 — Minute: 0

To: Fri, Jul 21, 2006 — Hour: 23 — Minute: 59

> Available Dates: 2006-7-13 to 2006-7-21

Subsystem: RS23:D81B

Activity Result: All

Activity Type: All

Show Top Number: 10

Drill Down Options:
- ● Retrieve data for selected item only
- ○ Retrieve all currently displayed data

Time Chart Options:
- ○ Group Activity By Minutes
- ○ Group Activity By Hours
- ● Group Activity By Days

Filter Data Option

Option

Filter Critrea:

Available Users	Available Objects	Available Plans
> All Users	> All Objects	> All Plans
CSBELK	TABLE/VIEW	ADHPLAN1
CSIVAN		ADHPLAN3
CSLIVI		DISTSERV
CSLIVIA		DSNTEP2
CSTROS		DSNUTIL

User Filter: — Object Filter: — Plan Filter:

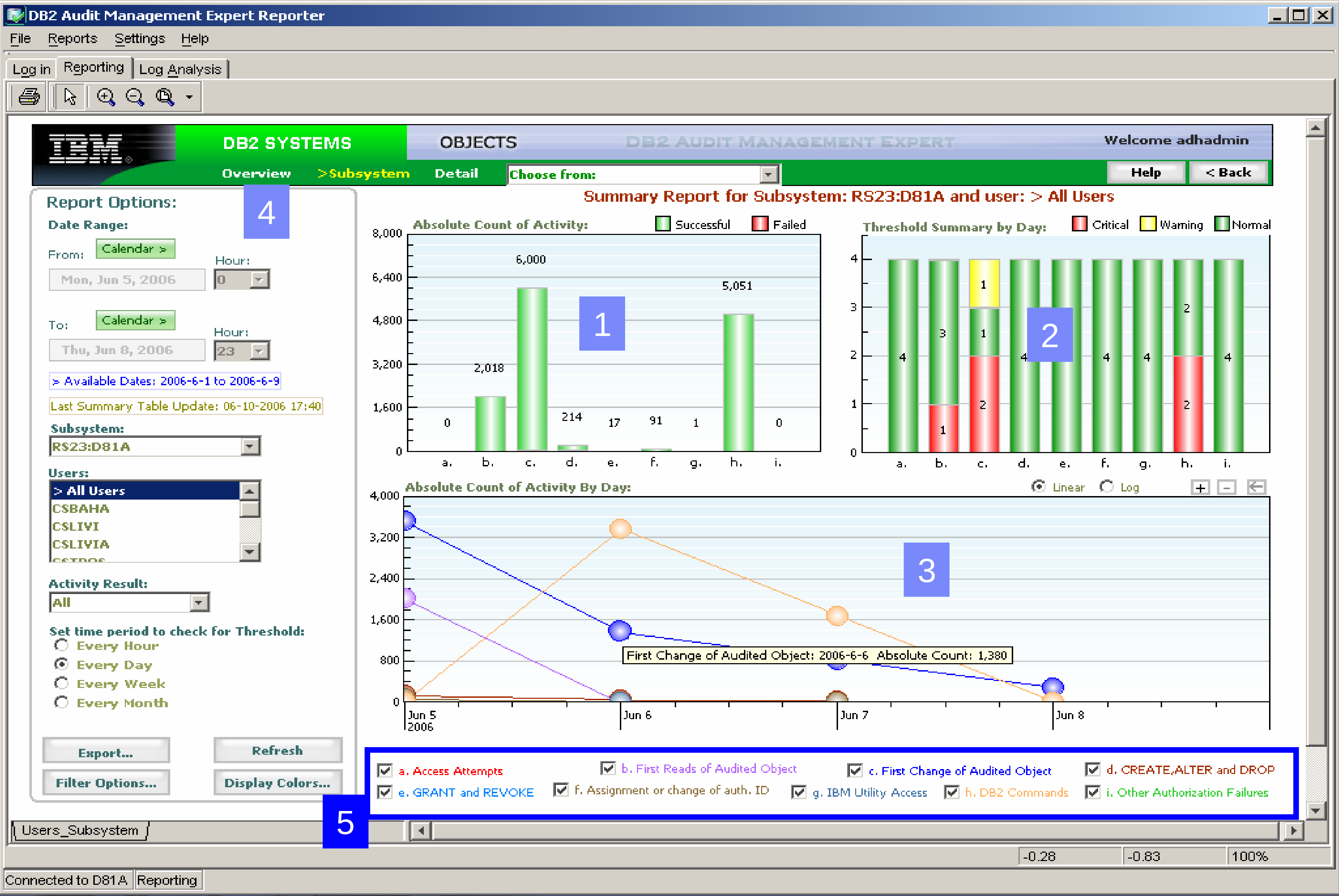
Selected Users	Selected Objects	Selected Plans
> All Users	> All Objects	> All Plans

5.22 | 3.2 | 100%

Connected to D81B | Reporting

IBM Audit Management Expert

REPORT CLIENT



DB2 Audit Management Expert Reporter

File Reports Settings Help

Log in | Reporting | Log Analysis

DB2 SYSTEMS | OBJECTS | DB2 AUDIT MANAGEMENT EXPERT | Welcome adhadmin

Overview | >Subsystem | Detail | Choose from: | Help | < Back

Report Options:

Date Range:

From: Calendar > Mon, Jun 5, 2006 Hour: 0

To: Calendar > Thu, Jun 8, 2006 Hour: 23

> Available Dates: 2006-6-1 to 2006-6-9

Last Summary Table Update: 06-10-2006 17:40

Subsystem: RS23:D81A

Users: > All Users, CSBAHA, CSLIVI, CSLIVIA, CSTROS

Activity Result: All

Set time period to check for Threshold:

○ Every Hour
● Every Day
○ Every Week
○ Every Month

Export... | Refresh | Filter Options... | Display Colors...

Summary Report for Subsystem: RS23:D81A and user: > All Users

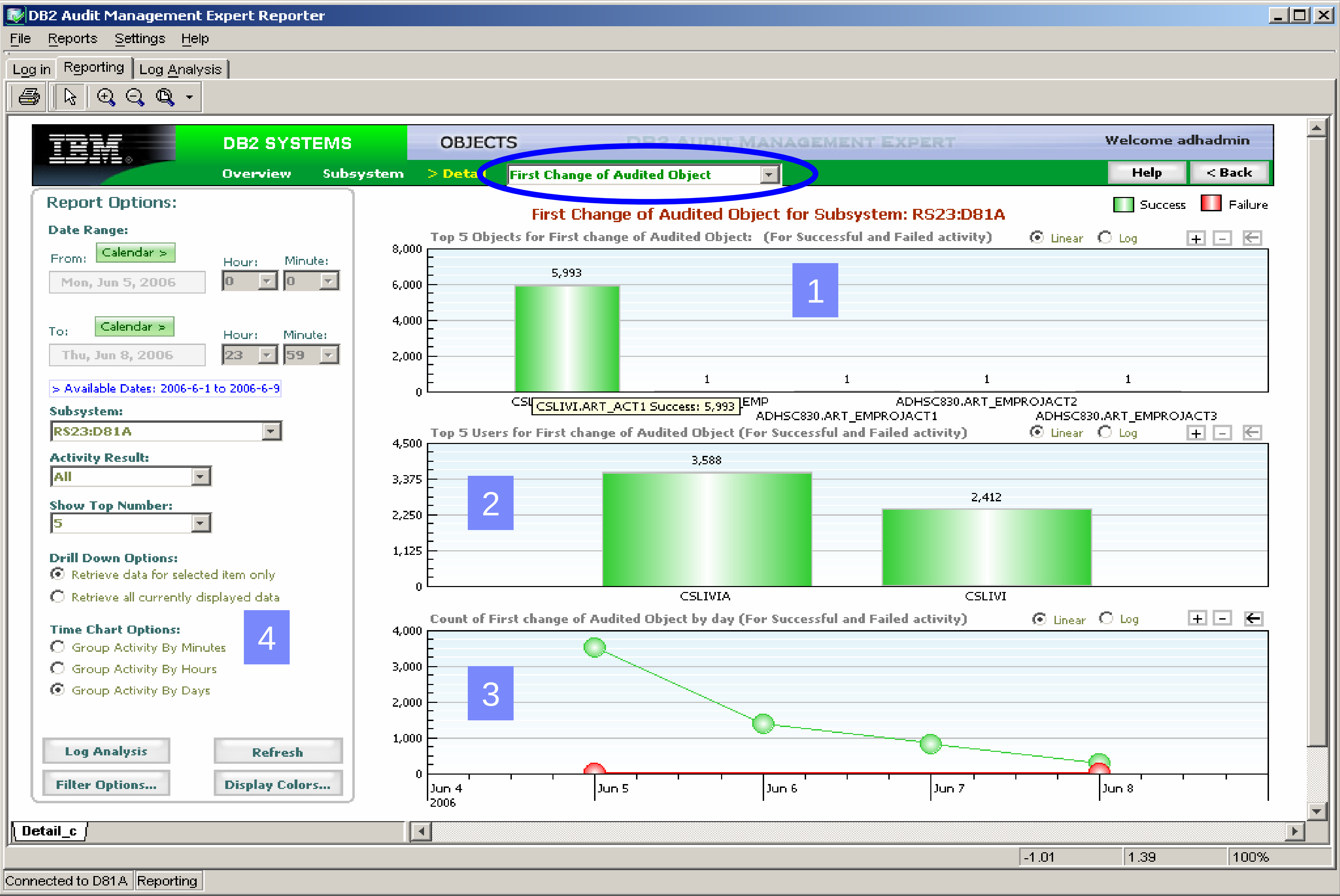
☑ a. Access Attempts
☑ b. First Reads of Audited Object
☑ c. First Change of Audited Object
☑ d. CREATE,ALTER and DROP
☑ e. GRANT and REVOKE
☑ f. Assignment or change of auth. ID
☑ g. IBM Utility Access
☑ h. DB2 Commands
☑ i. Other Authorization Failures

Users_Subsystem

-0.28 | -0.83 | 100%

Connected to D81A | Reporting

REPORT CLIENT



First Change of Audited Object

Report Options:

Date Range:

From: Mon, Jun 5, 2006 Hour: 0 Minute: 0

To: Thu, Jun 8, 2006 Hour: 23 Minute: 59

> Available Dates: 2006-6-1 to 2006-6-9

Subsystem: RS23:D81A

Activity Result: All

Show Top Number: 5

Drill Down Options:

- ● Retrieve data for selected item only
- ○ Retrieve all currently displayed data

Time Chart Options:

- ○ Group Activity By Minutes
- ○ Group Activity By Hours
- ● Group Activity By Days

First Change of Audited Object for Subsystem: RS23:D81A

Top 5 Objects for First change of Audited Object: (For Successful and Failed activity) ● Linear ○ Log

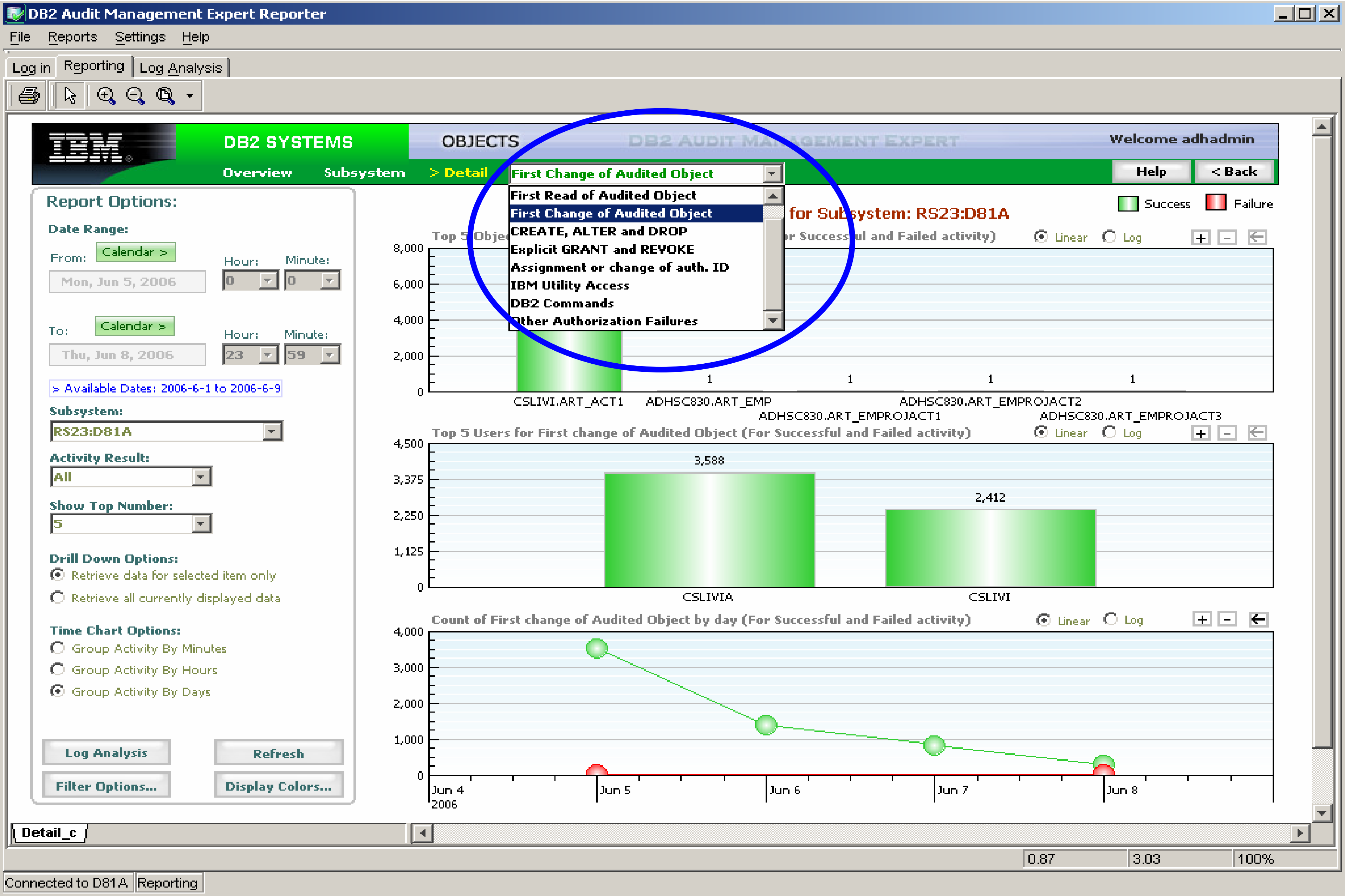
Top 5 Users for First change of Audited Object (For Successful and Failed activity) ● Linear ○ Log

Count of First change of Audited Object by day (For Successful and Failed activity) ● Linear ○ Log

-1.01 1.39 100%

Connected to D81A Reporting

REPORT CLIENT



DB2 Audit Management Expert Reporter
File Reports Settings Help
Log in | Reporting | Log Analysis
DB2 SYSTEMS | OBJECTS | DB2 AUDIT MANAGEMENT EXPERT
Welcome adhadmin
Overview | Subsystem | > Detail
Help | < Back
First Change of Audited Object
First Read of Audited Object
First Change of Audited Object
CREATE, ALTER and DROP
Explicit GRANT and REVOKE
Assignment or change of auth. ID
IBM Utility Access
DB2 Commands
Other Authorization Failures
🟩 Success 🟥 Failure
Log Analysis | Refresh | Filter Options... | Display Colors...
Detail_c
0.87 | 3.03 | 100%
Connected to D81A | Reporting

Report Options:

Date Range:

From: Calendar > Mon, Jun 5, 2006 Hour: 0 Minute: 0

To: Calendar > Thu, Jun 8, 2006 Hour: 23 Minute: 59

> Available Dates: 2006-6-1 to 2006-6-9

Subsystem: RS23:D81A

Activity Result: All

Show Top Number: 5

Drill Down Options:
- ● Retrieve data for selected item only
- ○ Retrieve all currently displayed data

Time Chart Options:
- ○ Group Activity By Minutes
- ○ Group Activity By Hours
- ● Group Activity By Days

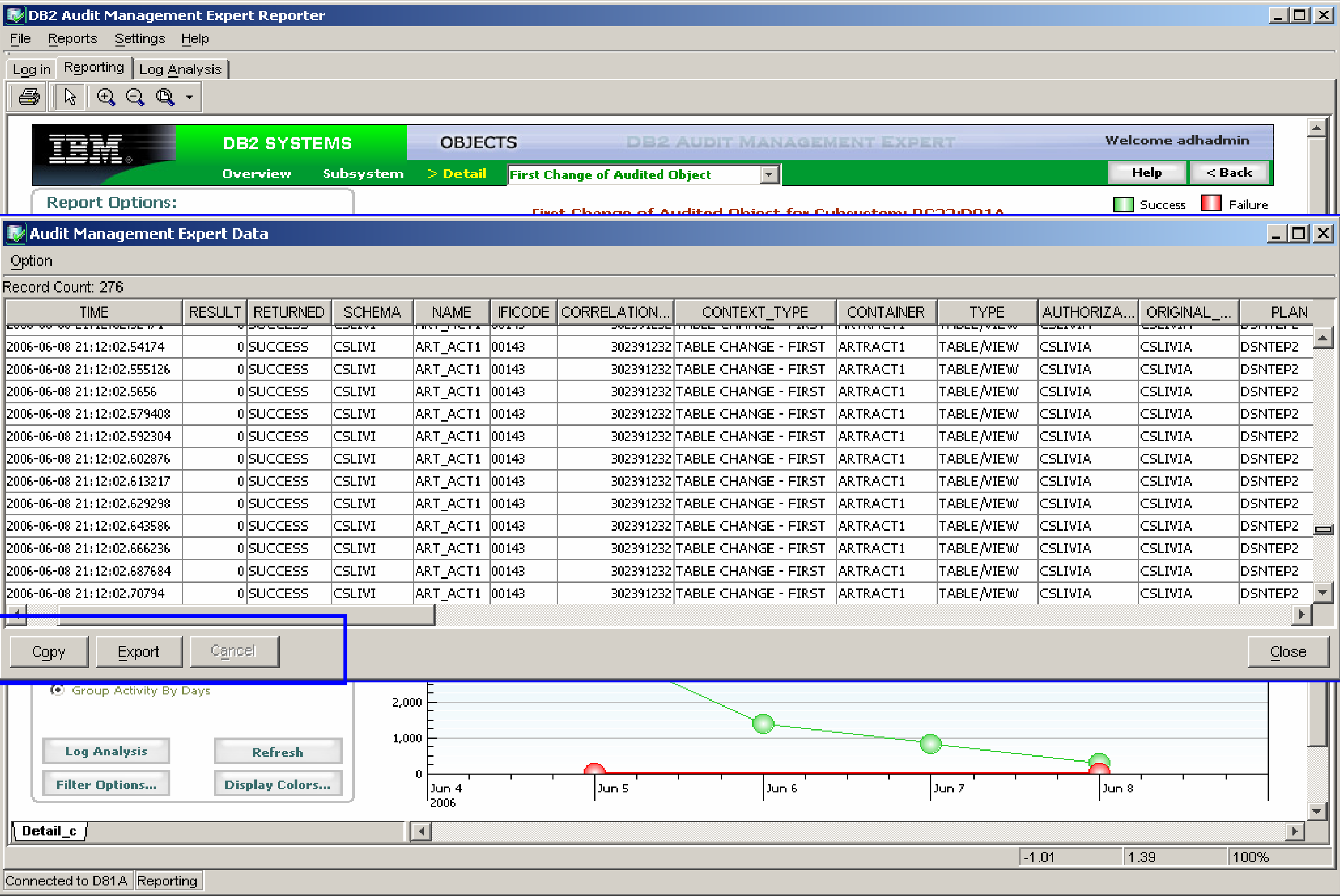
... for Subsystem: RS23:D81A

Top 5 Objec... (For Successful and Failed activity) ● Linear ○ Log

Top 5 Users for First change of Audited Object (For Successful and Failed activity) ● Linear ○ Log

Count of First change of Audited Object by day (For Successful and Failed activity) ● Linear ○ Log

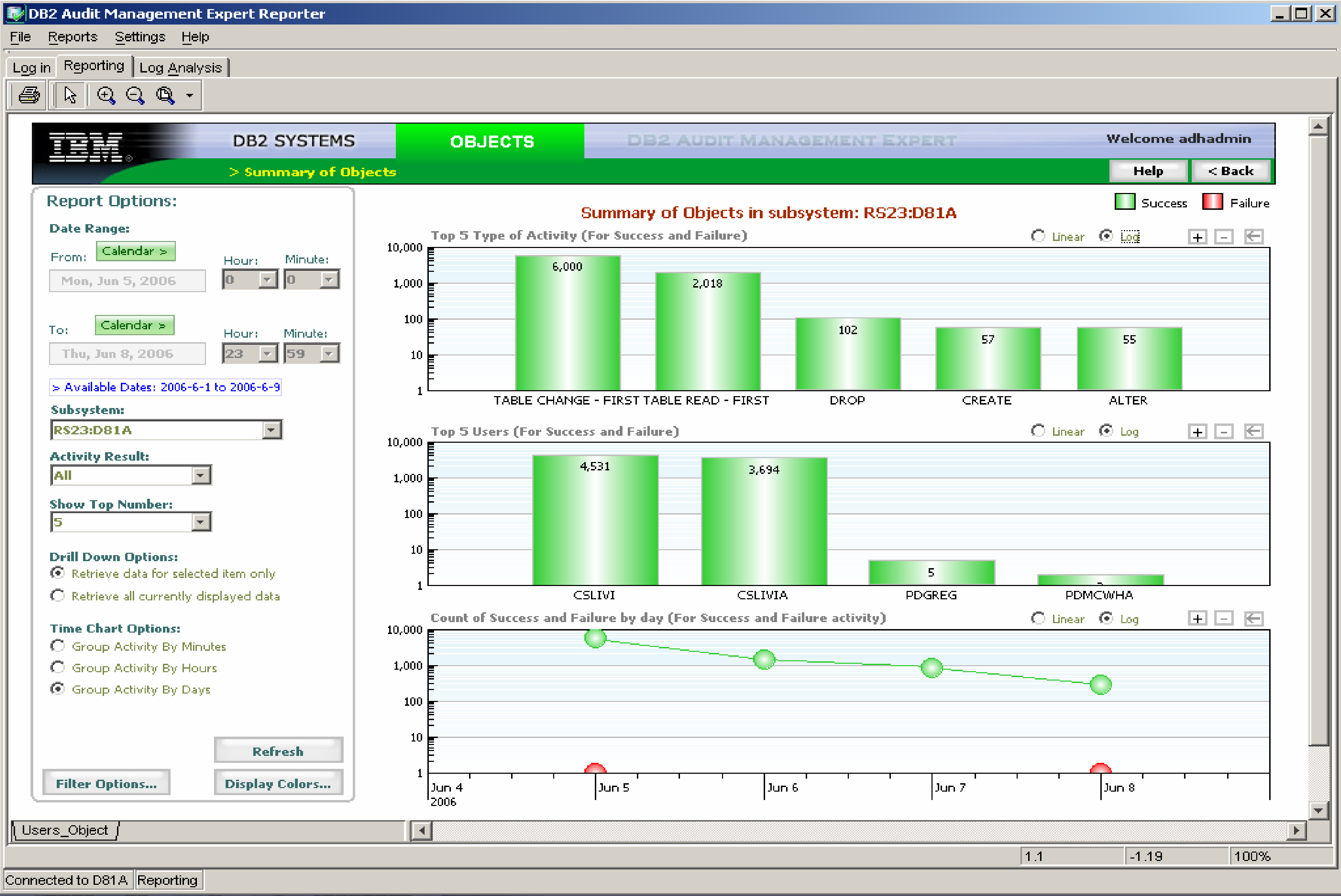
REPORT CLIENT



Record Count: 276

TIME	RESULT	RETURNED	SCHEMA	NAME	IFICODE	CORRELATION...	CONTEXT_TYPE	CONTAINER	TYPE	AUTHORIZA...	ORIGINAL_...	PLAN
2006-06-08 21:12:02.54174	0	SUCCESS	CSLIVI	ART_ACT1	00143	302391232	TABLE CHANGE - FIRST	ARTRACT1	TABLE/VIEW	CSLIVIA	CSLIVIA	DSNTEP2
2006-06-08 21:12:02.555126	0	SUCCESS	CSLIVI	ART_ACT1	00143	302391232	TABLE CHANGE - FIRST	ARTRACT1	TABLE/VIEW	CSLIVIA	CSLIVIA	DSNTEP2
2006-06-08 21:12:02.5656	0	SUCCESS	CSLIVI	ART_ACT1	00143	302391232	TABLE CHANGE - FIRST	ARTRACT1	TABLE/VIEW	CSLIVIA	CSLIVIA	DSNTEP2
2006-06-08 21:12:02.579408	0	SUCCESS	CSLIVI	ART_ACT1	00143	302391232	TABLE CHANGE - FIRST	ARTRACT1	TABLE/VIEW	CSLIVIA	CSLIVIA	DSNTEP2
2006-06-08 21:12:02.592304	0	SUCCESS	CSLIVI	ART_ACT1	00143	302391232	TABLE CHANGE - FIRST	ARTRACT1	TABLE/VIEW	CSLIVIA	CSLIVIA	DSNTEP2
2006-06-08 21:12:02.602876	0	SUCCESS	CSLIVI	ART_ACT1	00143	302391232	TABLE CHANGE - FIRST	ARTRACT1	TABLE/VIEW	CSLIVIA	CSLIVIA	DSNTEP2
2006-06-08 21:12:02.613217	0	SUCCESS	CSLIVI	ART_ACT1	00143	302391232	TABLE CHANGE - FIRST	ARTRACT1	TABLE/VIEW	CSLIVIA	CSLIVIA	DSNTEP2
2006-06-08 21:12:02.629298	0	SUCCESS	CSLIVI	ART_ACT1	00143	302391232	TABLE CHANGE - FIRST	ARTRACT1	TABLE/VIEW	CSLIVIA	CSLIVIA	DSNTEP2
2006-06-08 21:12:02.643586	0	SUCCESS	CSLIVI	ART_ACT1	00143	302391232	TABLE CHANGE - FIRST	ARTRACT1	TABLE/VIEW	CSLIVIA	CSLIVIA	DSNTEP2
2006-06-08 21:12:02.666236	0	SUCCESS	CSLIVI	ART_ACT1	00143	302391232	TABLE CHANGE - FIRST	ARTRACT1	TABLE/VIEW	CSLIVIA	CSLIVIA	DSNTEP2
2006-06-08 21:12:02.687684	0	SUCCESS	CSLIVI	ART_ACT1	00143	302391232	TABLE CHANGE - FIRST	ARTRACT1	TABLE/VIEW	CSLIVIA	CSLIVIA	DSNTEP2
2006-06-08 21:12:02.70794	0	SUCCESS	CSLIVI	ART_ACT1	00143	302391232	TABLE CHANGE - FIRST	ARTRACT1	TABLE/VIEW	CSLIVIA	CSLIVIA	DSNTEP2

REPORT CLIENT



Report Options:

Date Range:

From: Calendar > Mon, Jun 5, 2006 Hour: 0 Minute: 0

To: Calendar > Thu, Jun 8, 2006 Hour: 23 Minute: 59

> Available Dates: 2006-6-1 to 2006-6-9

Subsystem: RS23:D81A

Activity Result: All

Show Top Number: 5

Drill Down Options:

- ● Retrieve data for selected item only
- ○ Retrieve all currently displayed data

Time Chart Options:

- ○ Group Activity By Minutes
- ○ Group Activity By Hours
- ● Group Activity By Days

Summary of Objects in subsystem: RS23:D81A

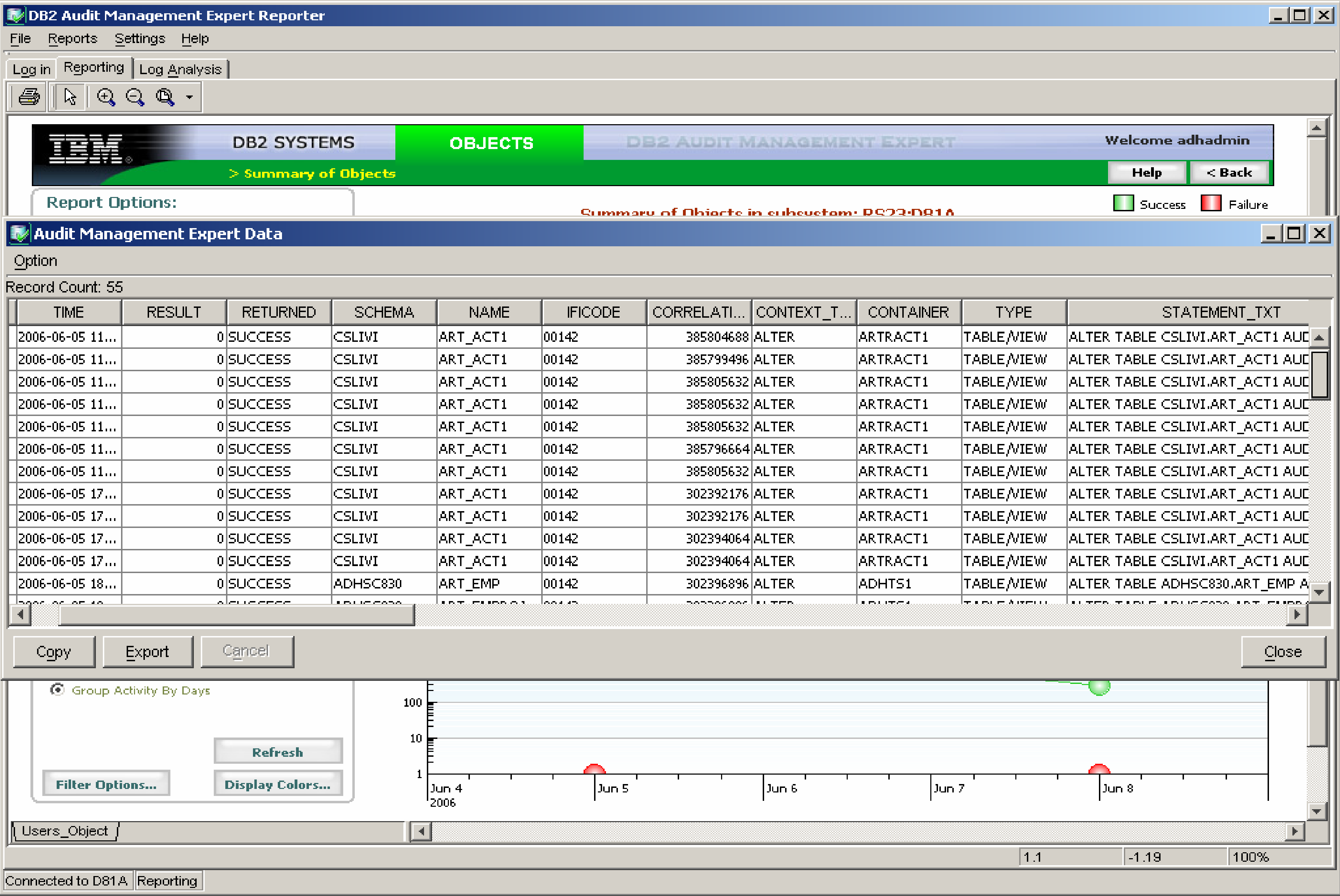
Top 5 Type of Activity (For Success and Failure) ○ Linear ● Log

Top 5 Users (For Success and Failure) ○ Linear ● Log

Count of Success and Failure by day (For Success and Failure activity) ○ Linear ● Log

Connected to D81A Reporting

REPORT CLIENT



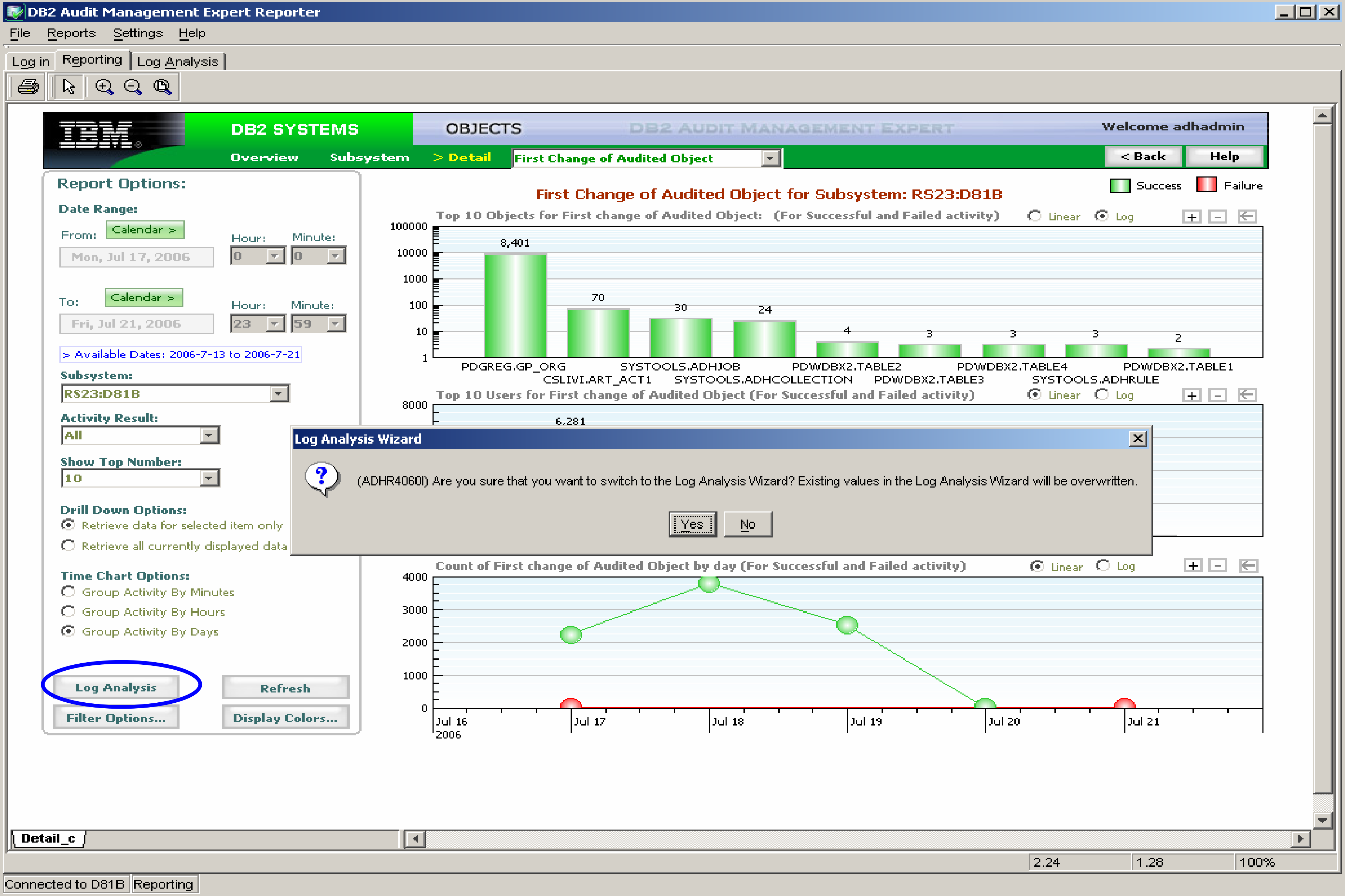
DB2 Audit Management Expert Reporter
File Reports Settings Help
Log in | Reporting | Log Analysis
DB2 SYSTEMS
OBJECTS
DB2 AUDIT MANAGEMENT EXPERT
Welcome adhadmin
> Summary of Objects
Help
< Back
Report Options:
Summary of Objects in subsystem: RS23:D81A
🟩 Success
🟥 Failure

Audit Management Expert Data

Record Count: 55

TIME	RESULT	RETURNED	SCHEMA	NAME	IFICODE	CORRELATI...	CONTEXT_T...	CONTAINER	TYPE	STATEMENT_TXT
2006-06-05 11...	0	SUCCESS	CSLIVI	ART_ACT1	00142	385804688	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUD
2006-06-05 11...	0	SUCCESS	CSLIVI	ART_ACT1	00142	385799496	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUD
2006-06-05 11...	0	SUCCESS	CSLIVI	ART_ACT1	00142	385805632	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUD
2006-06-05 11...	0	SUCCESS	CSLIVI	ART_ACT1	00142	385805632	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUD
2006-06-05 11...	0	SUCCESS	CSLIVI	ART_ACT1	00142	385805632	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUD
2006-06-05 11...	0	SUCCESS	CSLIVI	ART_ACT1	00142	385796664	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUD
2006-06-05 11...	0	SUCCESS	CSLIVI	ART_ACT1	00142	385805632	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUD
2006-06-05 17...	0	SUCCESS	CSLIVI	ART_ACT1	00142	302392176	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUD
2006-06-05 17...	0	SUCCESS	CSLIVI	ART_ACT1	00142	302392176	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUD
2006-06-05 17...	0	SUCCESS	CSLIVI	ART_ACT1	00142	302394064	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUD
2006-06-05 17...	0	SUCCESS	CSLIVI	ART_ACT1	00142	302394064	ALTER	ARTRACT1	TABLE/VIEW	ALTER TABLE CSLIVI.ART_ACT1 AUD
2006-06-05 18...	0	SUCCESS	ADHSC830	ART_EMP	00142	302396896	ALTER	ADHTS1	TABLE/VIEW	ALTER TABLE ADHSC830.ART_EMP A

REPORT CLIENT



DB2 Audit Management Expert Reporter

First Change of Audited Object

Report Options:

Date Range:

From: Calendar > Mon, Jul 17, 2006 Hour: 0 Minute: 0

To: Calendar > Fri, Jul 21, 2006 Hour: 23 Minute: 59

> Available Dates: 2006-7-13 to 2006-7-21

Subsystem: RS23:D81B

Activity Result: All

Show Top Number: 10

Drill Down Options:

- ● Retrieve data for selected item only
- ○ Retrieve all currently displayed data

Time Chart Options:

- ○ Group Activity By Minutes
- ○ Group Activity By Hours
- ● Group Activity By Days

First Change of Audited Object for Subsystem: RS23:D81B

Top 10 Objects for First change of Audited Object: (For Successful and Failed activity) ○ Linear ● Log

Top 10 Users for First change of Audited Object (For Successful and Failed activity) ● Linear ○ Log

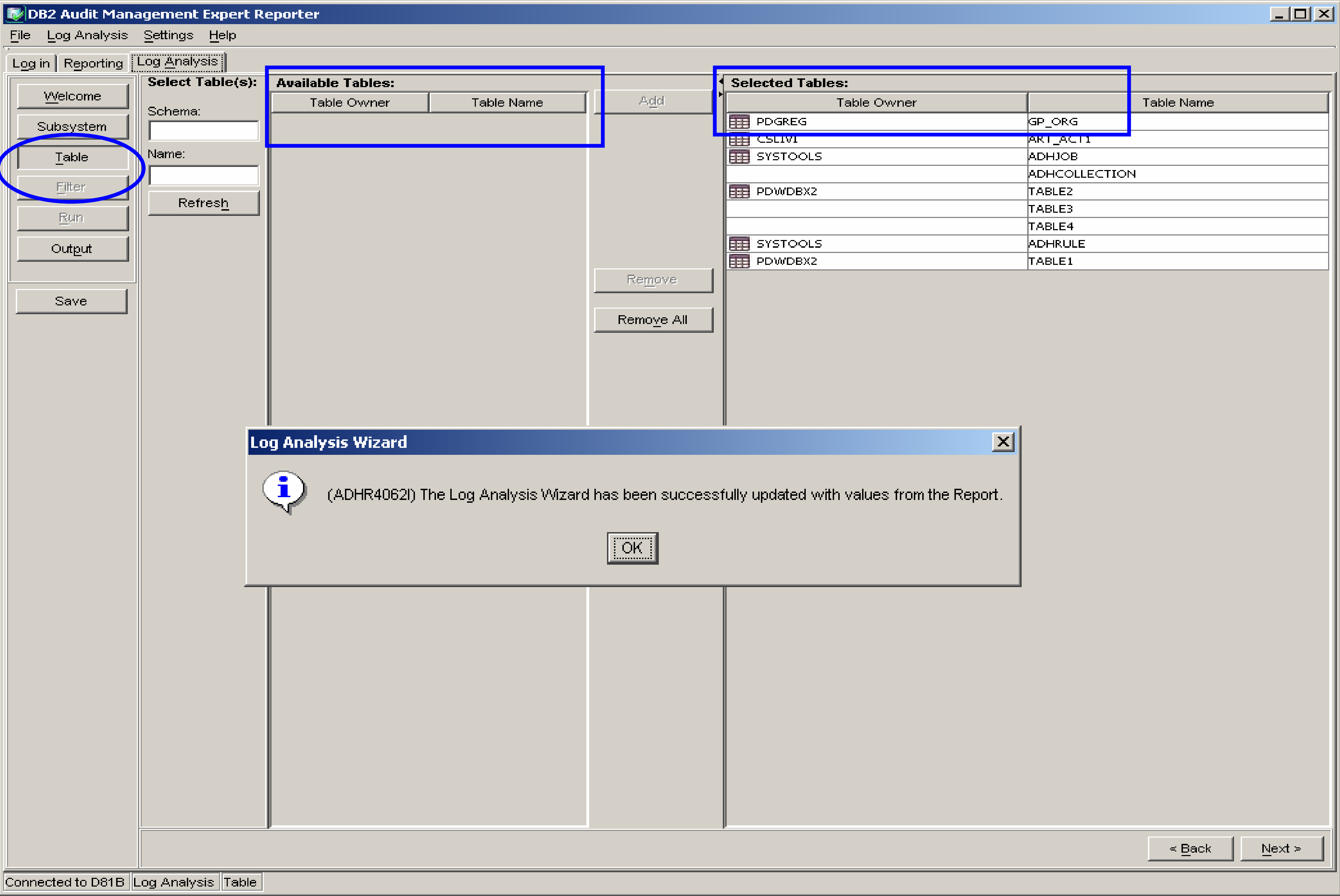
Log Analysis Wizard

(ADHR4060I) Are you sure that you want to switch to the Log Analysis Wizard? Existing values in the Log Analysis Wizard will be overwritten.

Count of First change of Audited Object by day (For Successful and Failed activity) ● Linear ○ Log

Connected to D81B Reporting

REPORT CLIENT



Selected Tables:

Table Owner	Table Name
▦ PDGREG	GP_ORG
▦ CSLIVI	ART_ACT1
▦ SYSTOOLS	ADHJOB
	ADHCOLLECTION
▦ PDWDBX2	TABLE2
	TABLE3
	TABLE4
▦ SYSTOOLS	ADHRULE
▦ PDWDBX2	TABLE1

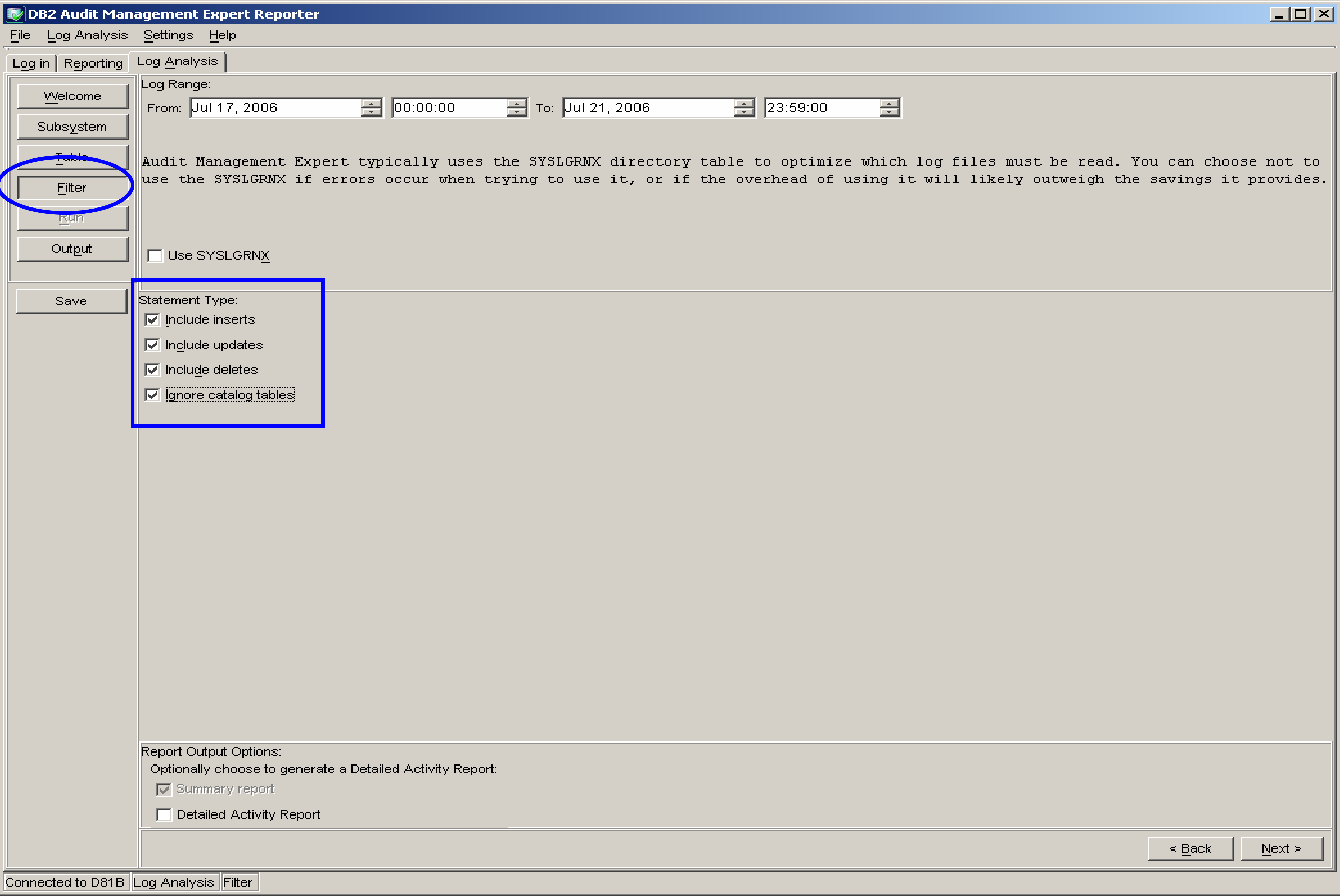
Log Analysis Wizard

(ADHR4062I) The Log Analysis Wizard has been successfully updated with values from the Report.

OK

Connected to D81B | Log Analysis | Table

REPORT CLIENT



Log Range:

From: Jul 17, 2006 00:00:00 To: Jul 21, 2006 23:59:00

Audit Management Expert typically uses the SYSLGRNX directory table to optimize which log files must be read. You can choose not to use the SYSLGRNX if errors occur when trying to use it, or if the overhead of using it will likely outweigh the savings it provides.

□ Use SYSLGRNX

Statement Type:

☑ Include inserts

☑ Include updates

☑ Include deletes

☑ Ignore catalog tables

Report Output Options:

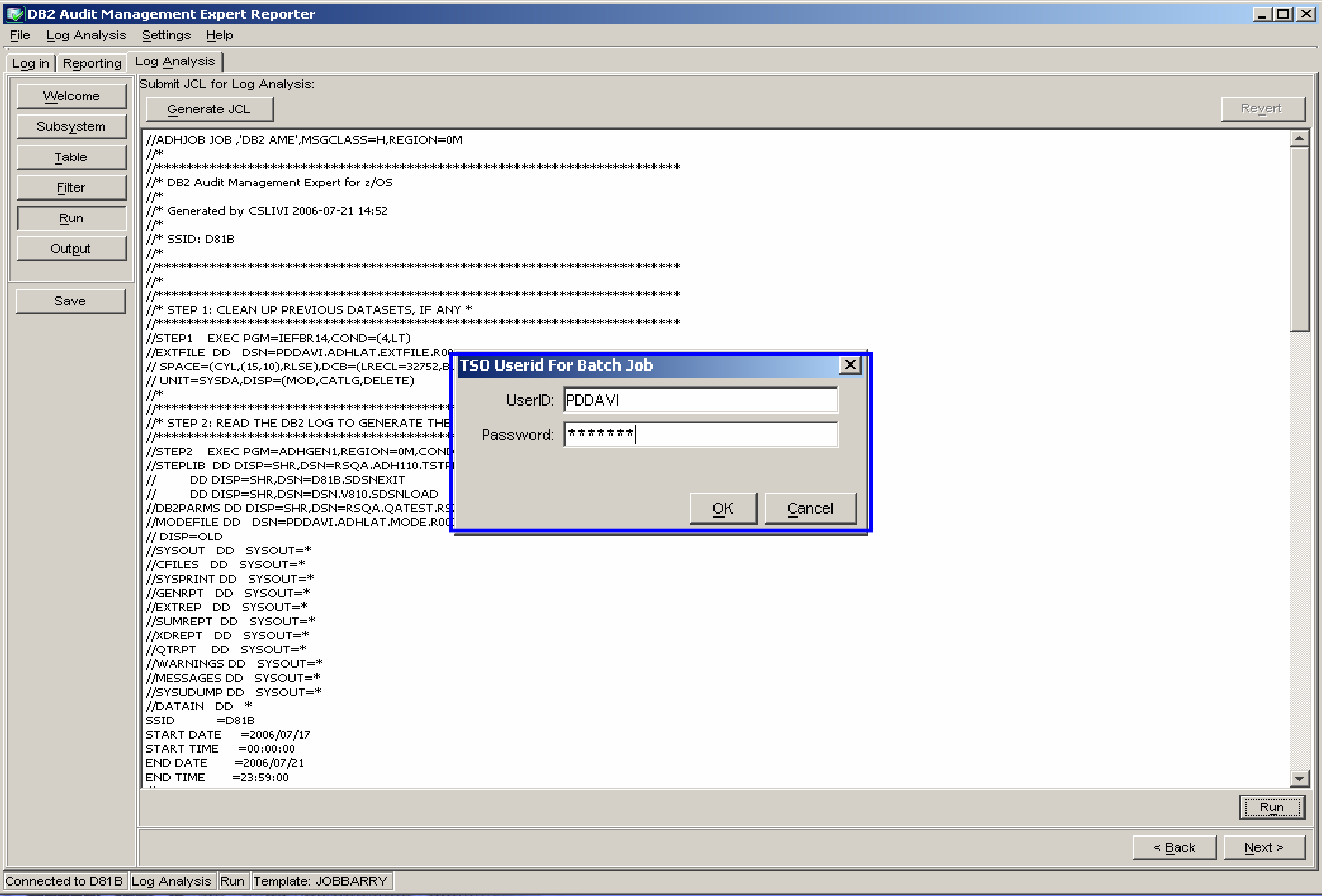
Optionally choose to generate a Detailed Activity Report:

☑ Summary report

□ Detailed Activity Report

Connected to D81B | Log Analysis | Filter

REPORT CLIENT



Submit JCL for Log Analysis:

```
//ADHJOB JOB ,'DB2 AME',MSGCLASS=H,REGION=0M
//*
//*********************************************************************
//* DB2 Audit Management Expert for z/OS
//*
//* Generated by CSLIVI 2006-07-21 14:52
//*
//* SSID: D81B
//*
//*********************************************************************
//*
//*********************************************************************
//* STEP 1: CLEAN UP PREVIOUS DATASETS, IF ANY *
//*********************************************************************
//STEP1    EXEC PGM=IEFBR14,COND=(4,LT)
//EXTFILE  DD   DSN=PDDAVI.ADHLAT.EXTFILE.R0
// SPACE=(CYL,(15,10),RLSE),DCB=(LRECL=32752,B
// UNIT=SYSDA,DISP=(MOD,CATLG,DELETE)
//*
//*****************************************
//* STEP 2: READ THE DB2 LOG TO GENERATE THE
//*****************************************
//STEP2    EXEC PGM=ADHGEN1,REGION=0M,COND
//STEPLIB  DD DISP=SHR,DSN=RSQA.ADH110.TSTP
//         DD DISP=SHR,DSN=D81B.SDSNEXIT
//         DD DISP=SHR,DSN=DSN.V810.SDSNLOAD
//DB2PARMS DD DISP=SHR,DSN=RSQA.QATEST.RS
//MODEFILE DD   DSN=PDDAVI.ADHLAT.MODE.R00
// DISP=OLD
//SYSOUT   DD   SYSOUT=*
//CFILES   DD   SYSOUT=*
//SYSPRINT DD   SYSOUT=*
//GENRPT   DD   SYSOUT=*
//EXTREP   DD   SYSOUT=*
//SUMREPT  DD   SYSOUT=*
//XDREPT   DD   SYSOUT=*
//QTRPT    DD   SYSOUT=*
//WARNINGS DD   SYSOUT=*
//MESSAGES DD   SYSOUT=*
//SYSUDUMP DD   SYSOUT=*
//DATAIN   DD   *
SSID          =D81B
START DATE    =2006/07/17
START TIME    =00:00:00
END DATE      =2006/07/21
END TIME      =23:59:00
```

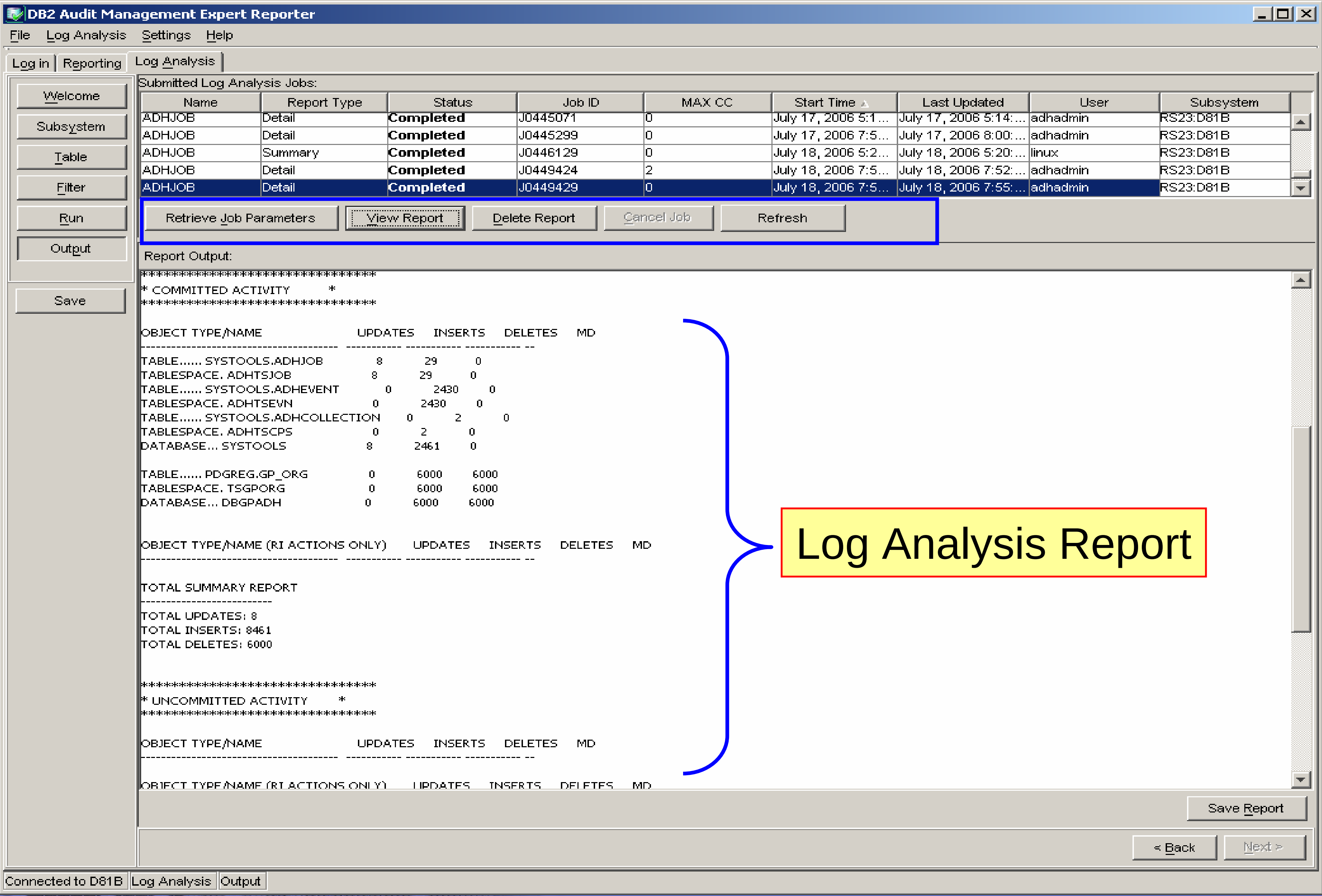
TSO Userid For Batch Job

UserID: PDDAVI

Password: *******

Connected to D81B | Log Analysis | Run | Template: JOBBARRY

REPORT CLIENT



Submitted Log Analysis Jobs:

Name	Report Type	Status	Job ID	MAX CC	Start Time	Last Updated	User	Subsystem
ADHJOB	Detail	**Completed**	J0445071	0	July 17, 2006 5:1...	July 17, 2006 5:14:...	adhadmin	RS23:D81B
ADHJOB	Detail	**Completed**	J0445299	0	July 17, 2006 7:5...	July 17, 2006 8:00:...	adhadmin	RS23:D81B
ADHJOB	Summary	**Completed**	J0446129	0	July 18, 2006 5:2...	July 18, 2006 5:20:...	linux	RS23:D81B
ADHJOB	Detail	**Completed**	J0449424	2	July 18, 2006 7:5...	July 18, 2006 7:52:...	adhadmin	RS23:D81B
ADHJOB	Detail	**Completed**	J0449429	0	July 18, 2006 7:5...	July 18, 2006 7:55:...	adhadmin	RS23:D81B

Report Output:

```
*********************************
* COMMITTED ACTIVITY           *
*********************************

OBJECT TYPE/NAME                    UPDATES    INSERTS    DELETES    MD
----------------------------------- ----------- ----------- ----------- --
TABLE...... SYSTOOLS.ADHJOB             8         29         0
TABLESPACE. ADHTSJOB                   8         29         0
TABLE...... SYSTOOLS.ADHEVENT           0         2430       0
TABLESPACE. ADHTSEVN                   0         2430       0
TABLE...... SYSTOOLS.ADHCOLLECTION      0          2          0
TABLESPACE. ADHTSCPS                   0          2          0
DATABASE... SYSTOOLS                  8         2461       0

TABLE...... PDGREG.GP_ORG              0         6000       6000
TABLESPACE. TSGPORG                    0         6000       6000
DATABASE... DBGPADH                   0         6000       6000


OBJECT TYPE/NAME (RI ACTIONS ONLY)      UPDATES    INSERTS    DELETES    MD
----------------------------------- ----------- ----------- ----------- --


TOTAL SUMMARY REPORT
-------------------------
TOTAL UPDATES: 8
TOTAL INSERTS: 8461
TOTAL DELETES: 6000


*********************************
* UNCOMMITTED ACTIVITY         *
*********************************

OBJECT TYPE/NAME                    UPDATES    INSERTS    DELETES    MD
----------------------------------- ----------- ----------- ----------- --

OBJECT TYPE/NAME (RI ACTIONS ONLY)      UPDATES    INSERTS    DELETES    MD
```

Log Analysis Report

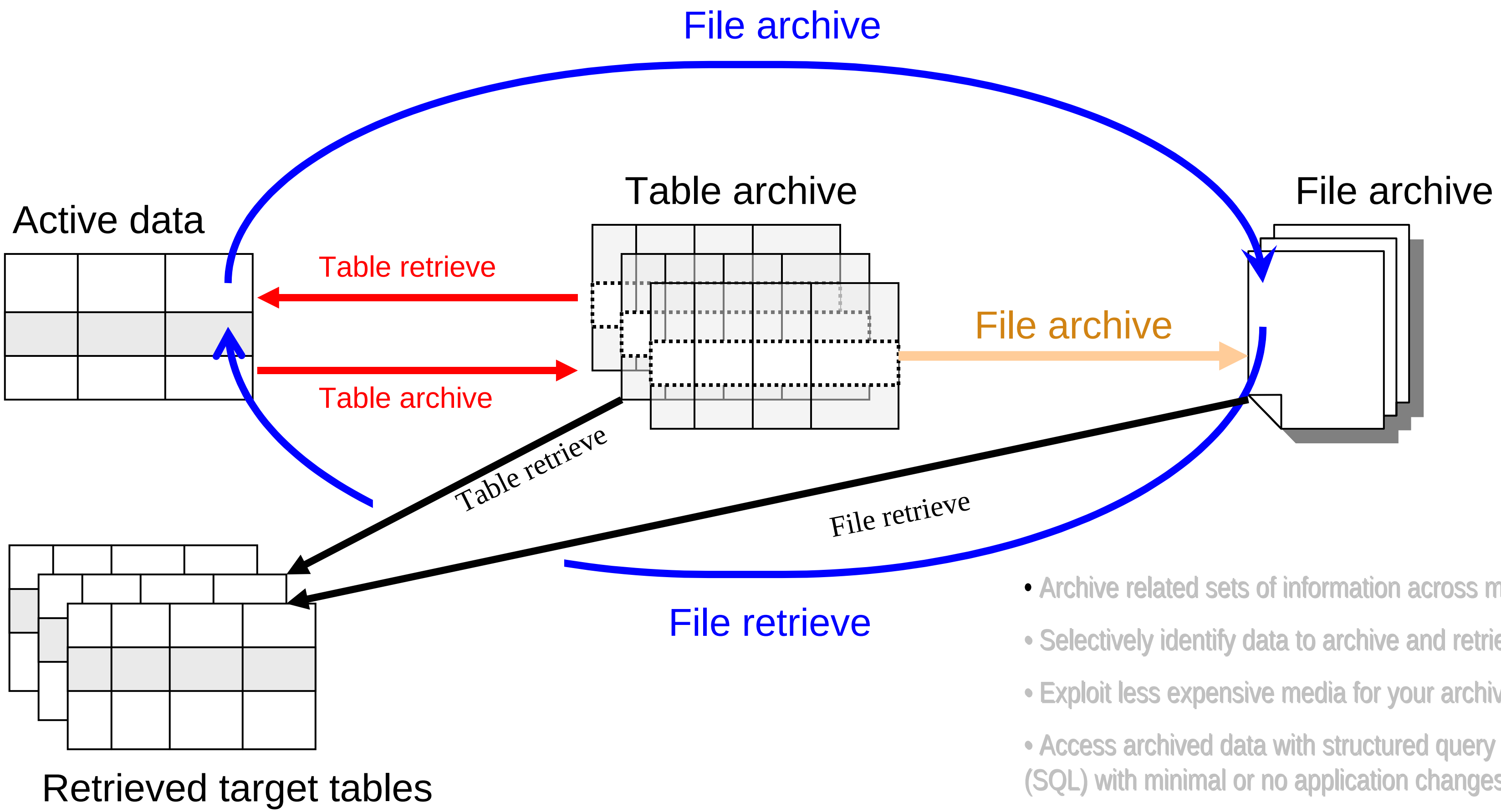
In Summary

- **Audit Management Expert**
  - Centralized auditing tools that can bring together information from different sources into a correlated, coherent view of the system
  - Enable auditors to collect, view, analyze, and report on data via the audit repository
  - Enable administrators to define customized filters for the collection of audit data
    - By data of interest – not by audit trace classes
  - Provides an administration user interface
    - allows product administrators to easily define
      - users and groups, assign privileges, define data collection policies
  - Provides an auditor-friendly reporting user interface
    - Many user friendly options for examining data in the repository
    - Allows detailed analysis and visualization of data collected by the DB2 auditing tool
    - Auditors can export audit data into other applications such as Excel®.
  - Product provides Batch reporting
  - Can perform Log Analysis to view changed data values

IBM DB2 Data Archive Expert Version 2

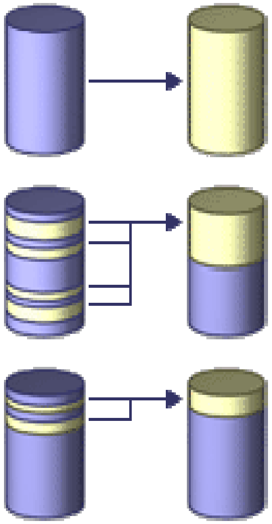
Step 5 – Retain your audit trail history for a period that is consistent with its effective use

DAE Multi-tiered Archiving Strategy



- Archive related sets of information across multiple tables
- Selectively identify data to archive and retrieve
- Exploit less expensive media for your archived data
- Access archived data with structured query language (SQL) with minimal or no application changes
- Defer the delete portion of the archive process
- Compress archived data with hardware data compression

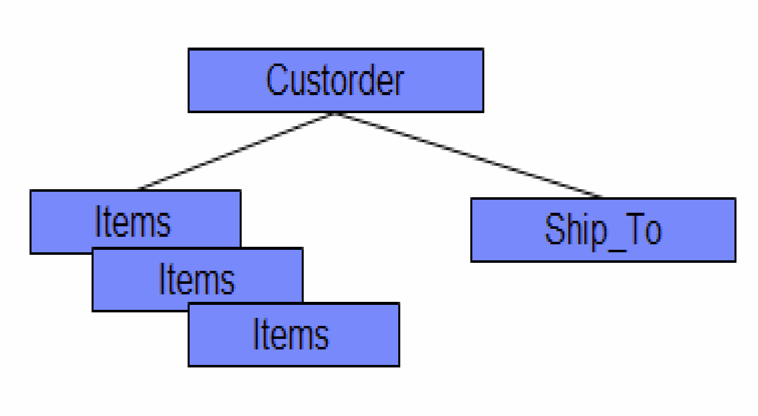
DB2 Data Archive Expert For z/OS Benefits

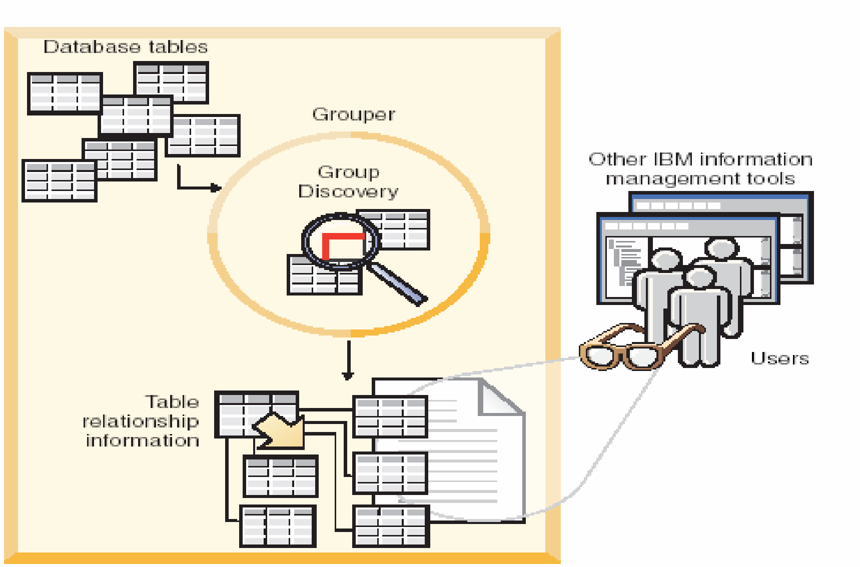


- **By providing a choice of archiving strategies**
  - To table
  - To file
  - To both (multi-tier)
  - MP as archive target (table only) – Version 2
- **By reducing operational costs**
- **By freeing up developers from writing customized archiving software**
- **By discovering related tables using the DB2 Grouper component**
- **By allowing the data to be removed/deleted from the source independently from the copy to the archive**
- **By working with data hardware compression**
- **By capturing all pertinent information about the archive**

DB2 Grouper

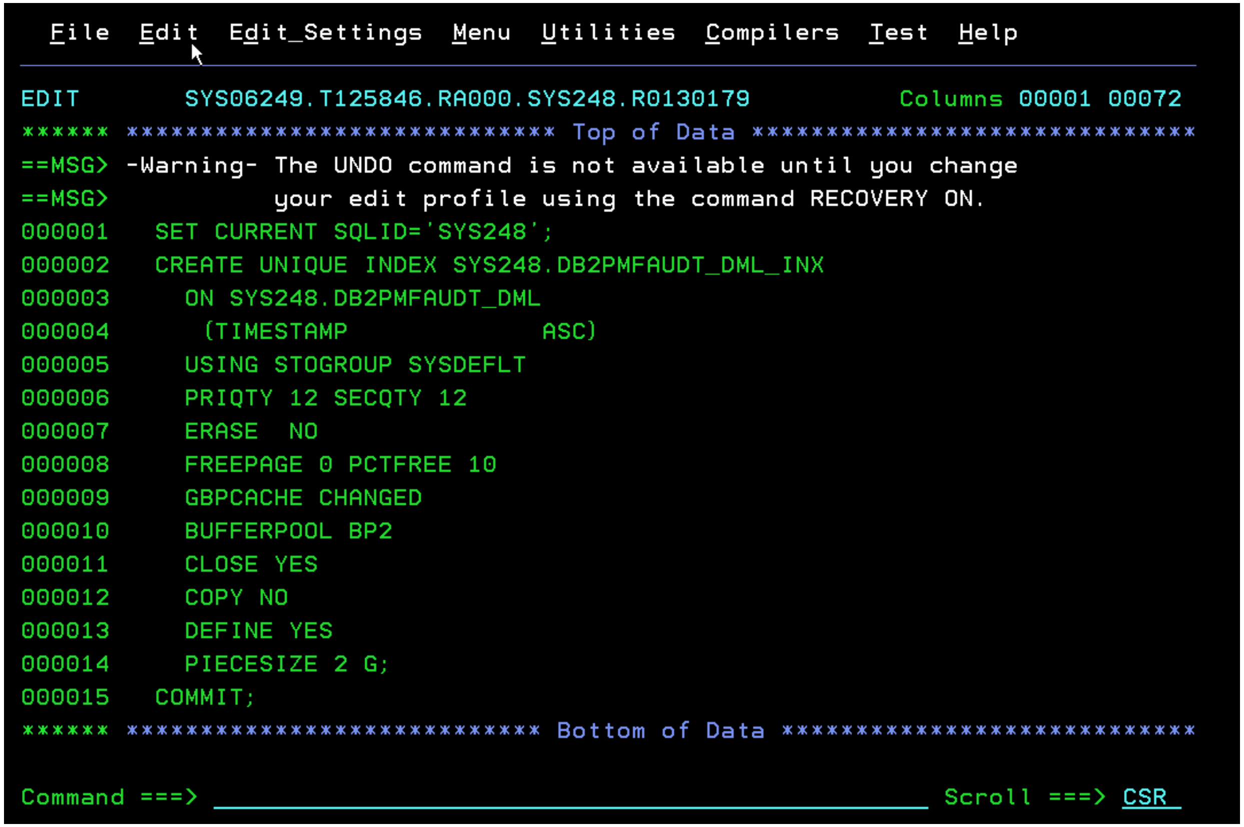
- **A common component of some IBM DB2 Tools**
- The Problem
  - Many Relationships between DB2 objects, such as tables, in a business application -- Some relationships can be discovered easily, while others cannot.
- The Objective
  - Enable the location, augmentation, and management of this information as the basis for consistent data management activities
- The Solution
  - Grouper is a component for discovering, recording, and managing groups of related objects (tables) that comprise a business application




Database tables
Grouper
Group Discovery
Table relationship information
Other IBM information management tools
Users

DB2 DAE needs to ensure uniqueness in his application of the row filter in order to prevent inadvertent loss of data during the archive process. The OMPE Audit tables do not contain any indexes. For purposes of this demonstration, I've selected the timestamp column of the Audit DML table and created a unique index on that column.

Creating the unique index using DB2 Administration Tool

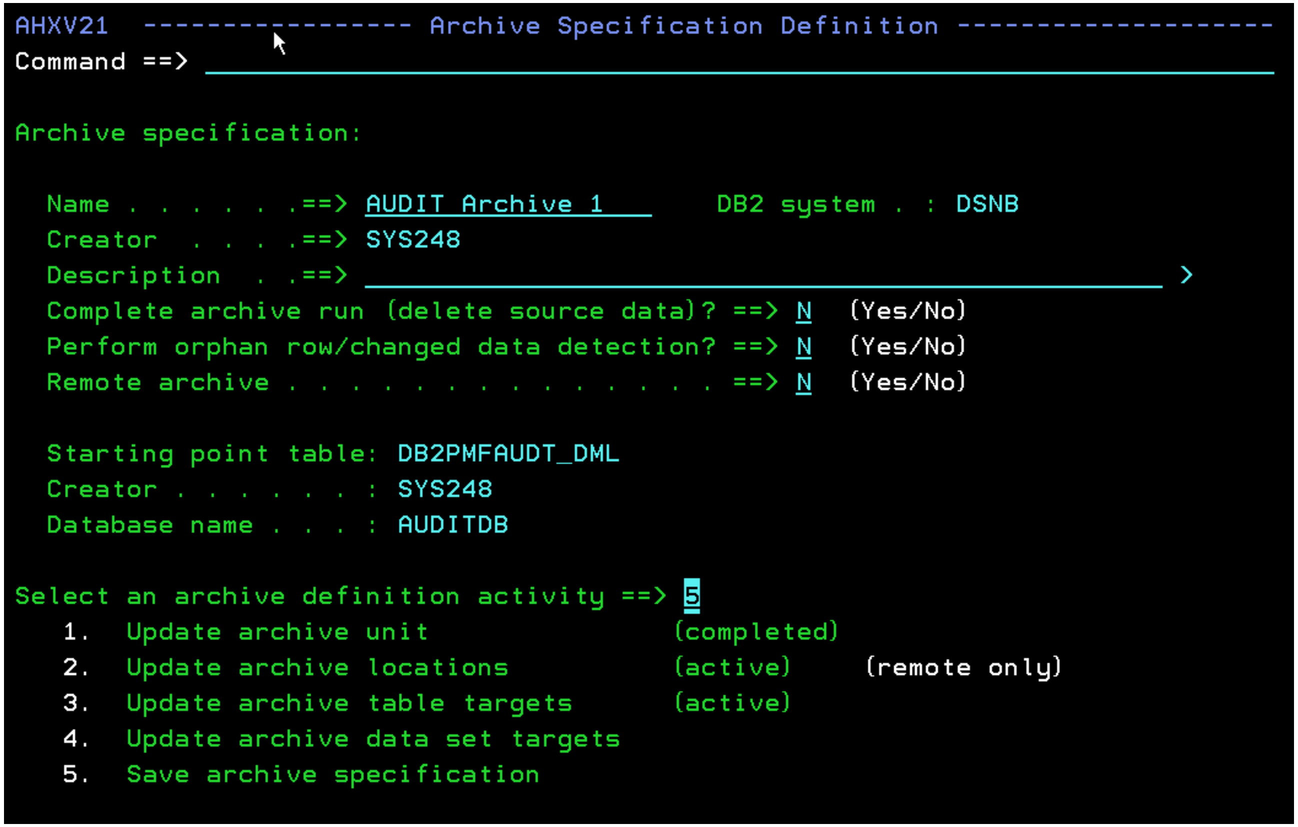


```
EDIT       SYS06249.T125846.RA000.SYS248.R0130179          Columns 00001 00072
****** ***************************** Top of Data ******************************
==MSG> -Warning- The UNDO command is not available until you change
==MSG>           your edit profile using the command RECOVERY ON.
000001   SET CURRENT SQLID='SYS248';
000002   CREATE UNIQUE INDEX SYS248.DB2PMFAUDT_DML_INX
000003     ON SYS248.DB2PMFAUDT_DML
000004      (TIMESTAMP                ASC)
000005     USING STOGROUP SYSDEFLT
000006     PRIQTY 12 SECQTY 12
000007     ERASE  NO
000008     FREEPAGE 0 PCTFREE 10
000009     GBPCACHE CHANGED
000010     BUFFERPOOL BP2
000011     CLOSE YES
000012     COPY NO
000013     DEFINE YES
000014     PIECESIZE 2 G;
000015   COMMIT;
****** **************************** Bottom of Data ****************************

Command ===> ________________________________________________ Scroll ===> CSR
```

Archive Specification Definition

- Name
- Description
- Default actions

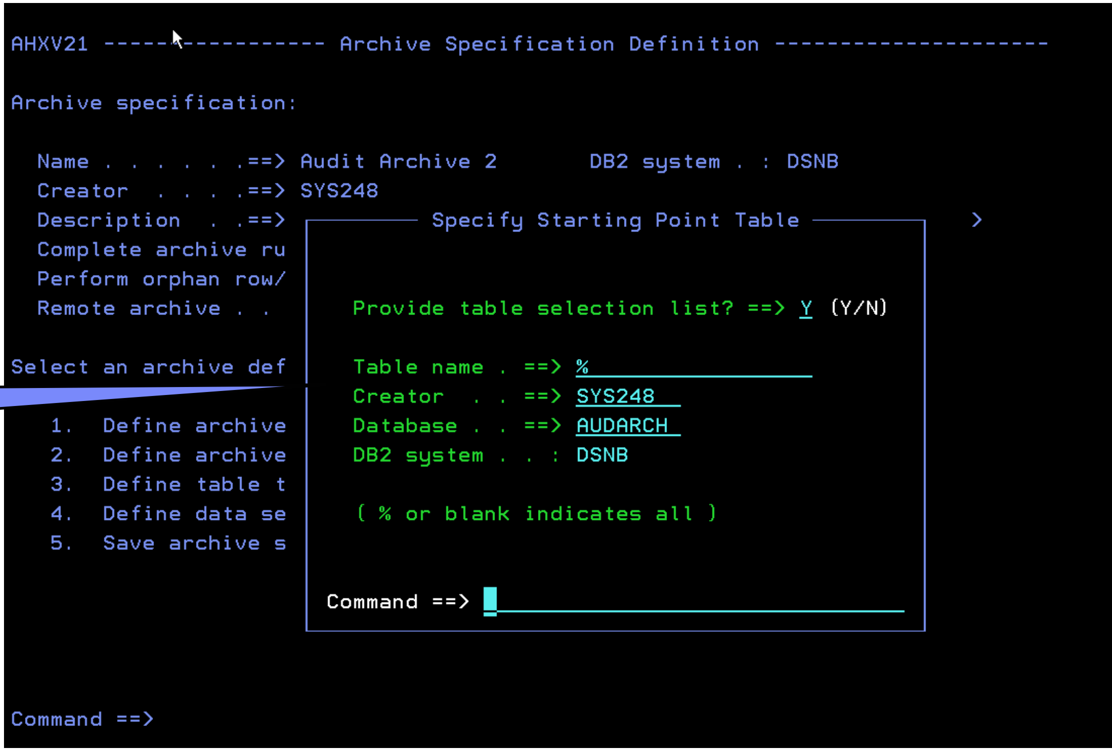
Remote Targets supported



```
AHXV21  ----------------- Archive Specification Definition --------------------
Command ==> ___________________________________________________________________

Archive specification:

  Name . . . . . .==> AUDIT Archive 1         DB2 system . : DSNB
  Creator   . . . .==> SYS248
  Description  . .==> __________________________________________________ >
  Complete archive run (delete source data)? ==> N  (Yes/No)
  Perform orphan row/changed data detection? ==> N  (Yes/No)
  Remote archive . . . . . . . . . . . . . . ==> N  (Yes/No)

  Starting point table: DB2PMFAUDT_DML
  Creator . . . . . . : SYS248
  Database name . . . : AUDITDB

Select an archive definition activity ==> 5
   1.  Update archive unit                  (completed)
   2.  Update archive locations             (active)    (remote only)
   3.  Update archive table targets         (active)
   4.  Update archive data set targets
   5.  Save archive specification
```

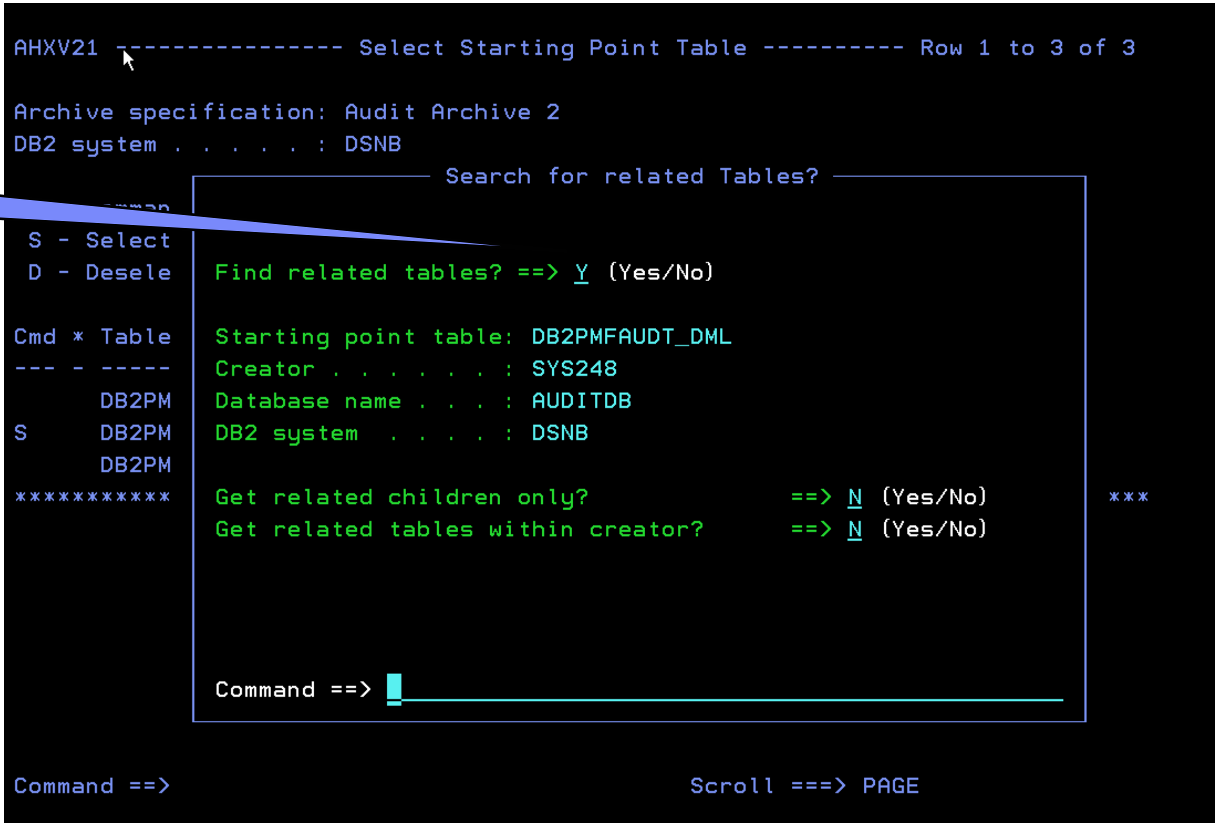
Every archive specification requires at least a starting point (parent) table. In our scenario we'll only archive one table, but there would typically be a total of 7 audit tables in the Performance Database

Masking and wildcarding supported



```
AHXV21 ----------------- Archive Specification Definition ---------------------

Archive specification:

  Name . . . . . . .==> Audit Archive 2       DB2 system . : DSNB
  Creator  . . . . .==> SYS248
  Description  . .==>  ---------- Specify Starting Point Table ----------      >
  Complete archive ru |                                                  |
  Perform orphan row/ |                                                  |
  Remote archive . .  |   Provide table selection list? ==> Y  (Y/N)     |
                      |                                                  |
Select an archive def |   Table name . ==> %                             |
                      |   Creator  . . ==> SYS248                        |
   1.  Define archive |   Database . . ==> AUDARCH                       |
   2.  Define archive |   DB2 system . . : DSNB                          |
   3.  Define table t |                                                  |
   4.  Define data se |   ( % or blank indicates all )                   |
   5.  Save archive s |                                                  |
                      |                                                  |
                      | Command ==>                                      |
                       --------------------------------------------------


Command ==>
```

This is where DAE will make the call to GROUPER for RI discovery. In our case, we have no RI, but we could build some unenforced RI between the PDB audit tables

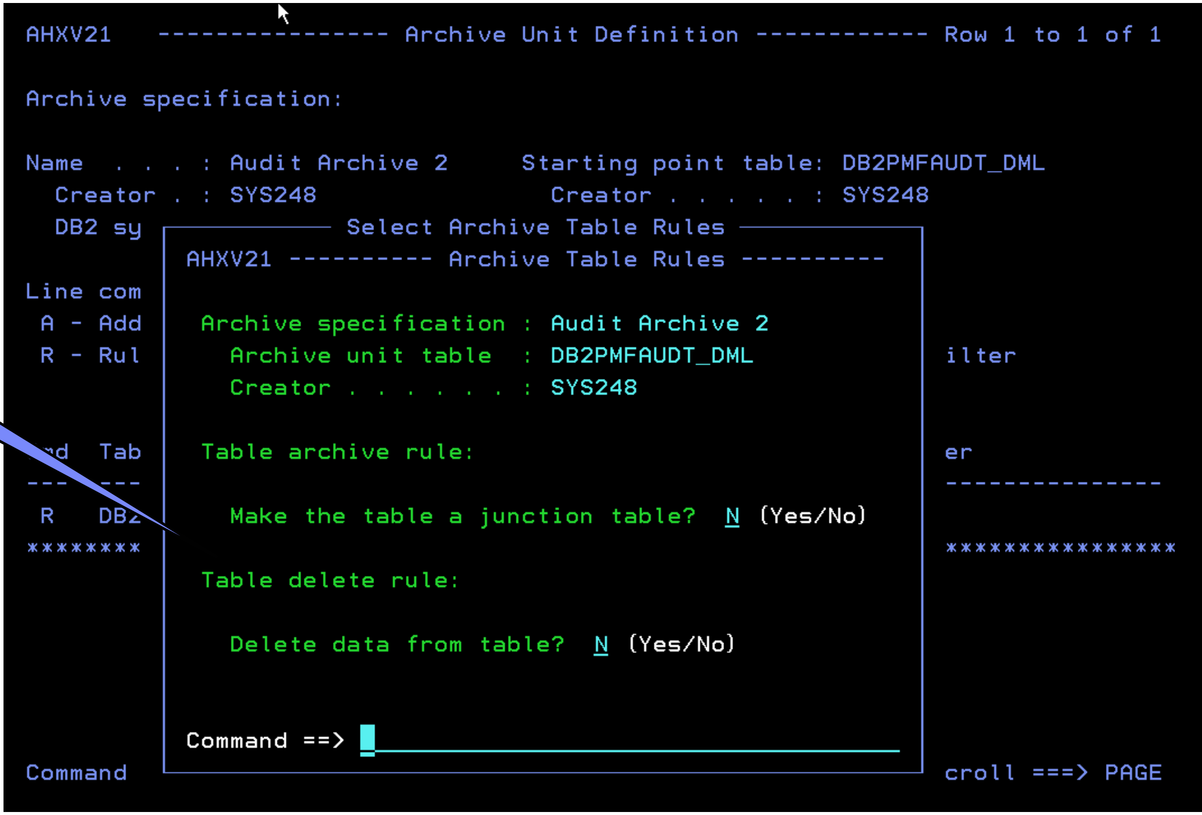


```
AHXV21 ---------------- Select Starting Point Table ---------- Row 1 to 3 of 3

Archive specification: Audit Archive 2
DB2 system . . . . . : DSNB
             ---------------- Search for related Tables? ------------------
             |                                                            |
      Comman |                                                            |
 S - Select  |                                                            |
 D - Desele  |  Find related tables? ==> Y (Yes/No)                        |
             |                                                            |
Cmd * Table  |  Starting point table: DB2PMFAUDT_DML                      |
--- - -----  |  Creator . . . . . . : SYS248                              |
      DB2PM  |  Database name . . . : AUDITDB                             |
S     DB2PM  |  DB2 system  . . . . : DSNB                                |
      DB2PM  |                                                            |
***********  |  Get related children only?           ==> N (Yes/No)      |   ***
             |  Get related tables within creator?   ==> N (Yes/No)      |
             |                                                            |
             |                                                            |
             |                                                            |
             |                                                            |
             |  Command ==> _                                             |
             --------------------------------------------------------------

Command ==>                                               Scroll ===> PAGE
```

“N”

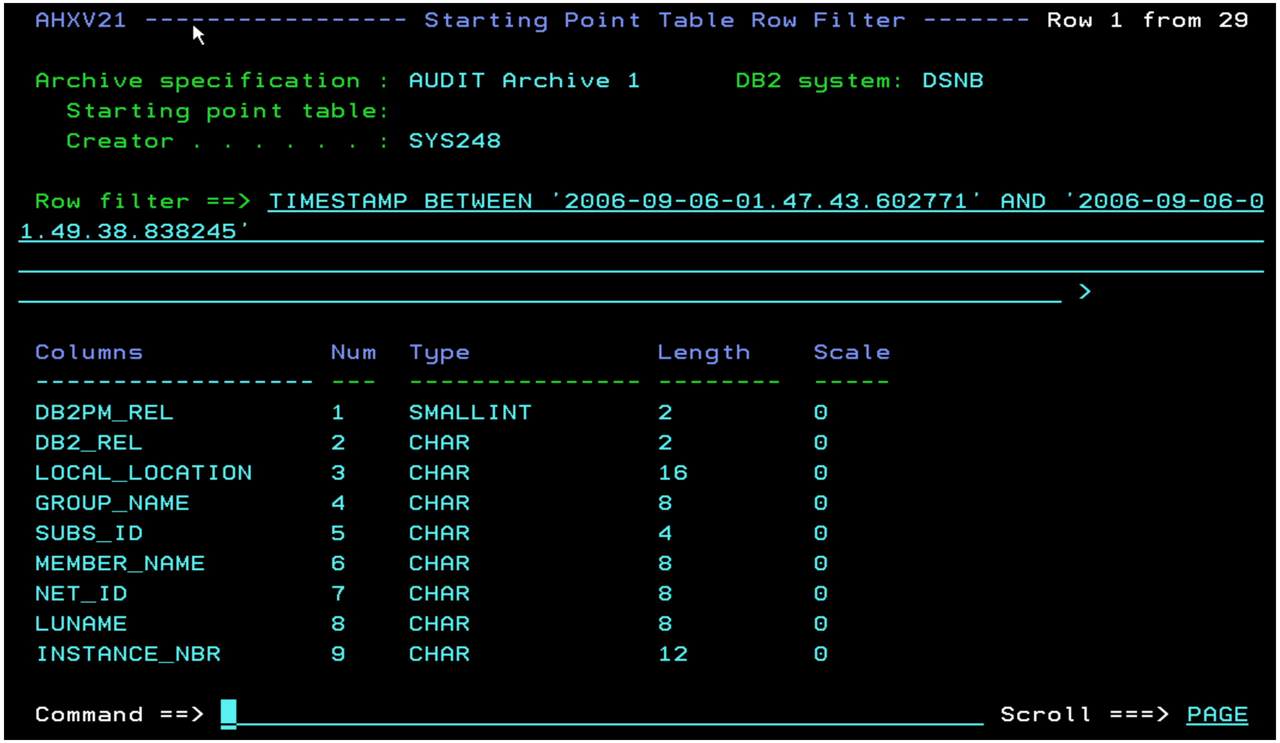
Deleting the source rows is optional and can be deferred until a future point in time

We'll say "Y"



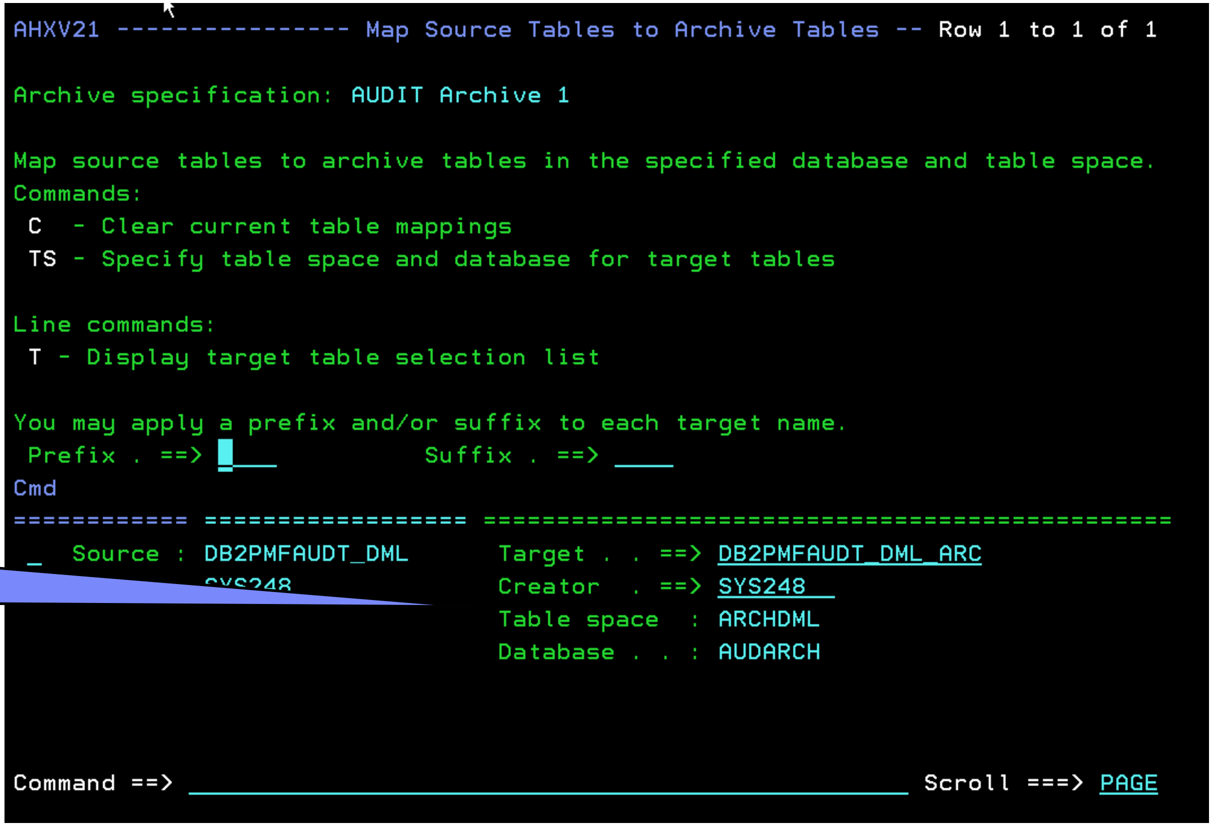
```
AHXV21   ---------------- Archive Unit Definition ------------ Row 1 to 1 of 1

Archive specification:

Name  . . . : Audit Archive 2     Starting point table: DB2PMFAUDT_DML
  Creator . : SYS248                Creator . . . . . : SYS248
  DB2 sy   ----------- Select Archive Table Rules ------------
           AHXV21 ---------- Archive Table Rules ----------
Line com
 A - Add    Archive specification : Audit Archive 2
 R - Rul      Archive unit table  : DB2PMFAUDT_DML              ilter
              Creator . . . . . . : SYS248

 nd  Tab    Table archive rule:                                 er
 --- ---                                                        ---------------
 R   DB2      Make the table a junction table? N (Yes/No)
********                                                        ****************
            Table delete rule:

              Delete data from table? N (Yes/No)


           Command ==> _
Command                                                         croll ===> PAGE
```

Row filter is applied to determine what gets deleted. If there were multiple tables involved, we'd have multiple row filters….unless RI with cascade was in place.



```
 AHXV21 ----------------- Starting Point Table Row Filter ------- Row 1 from 29

 Archive specification : AUDIT Archive 1       DB2 system: DSNB
   Starting point table:
   Creator . . . . . . . : SYS248

 Row filter ==> TIMESTAMP BETWEEN '2006-09-06-01.47.43.602771' AND '2006-09-06-0
1.49.38.838245'

                                                                    >

 Columns              Num   Type              Length    Scale
 ------------------ ---   ---------------  --------   -----
 DB2PM_REL            1     SMALLINT          2         0
 DB2_REL              2     CHAR              2         0
 LOCAL_LOCATION       3     CHAR              16        0
 GROUP_NAME           4     CHAR              8         0
 SUBS_ID              5     CHAR              4         0
 MEMBER_NAME          6     CHAR              8         0
 NET_ID               7     CHAR              8         0
 LUNAME               8     CHAR              8         0
 INSTANCE_NBR         9     CHAR              12        0

 Command ==>                                                  Scroll ===> PAGE
```

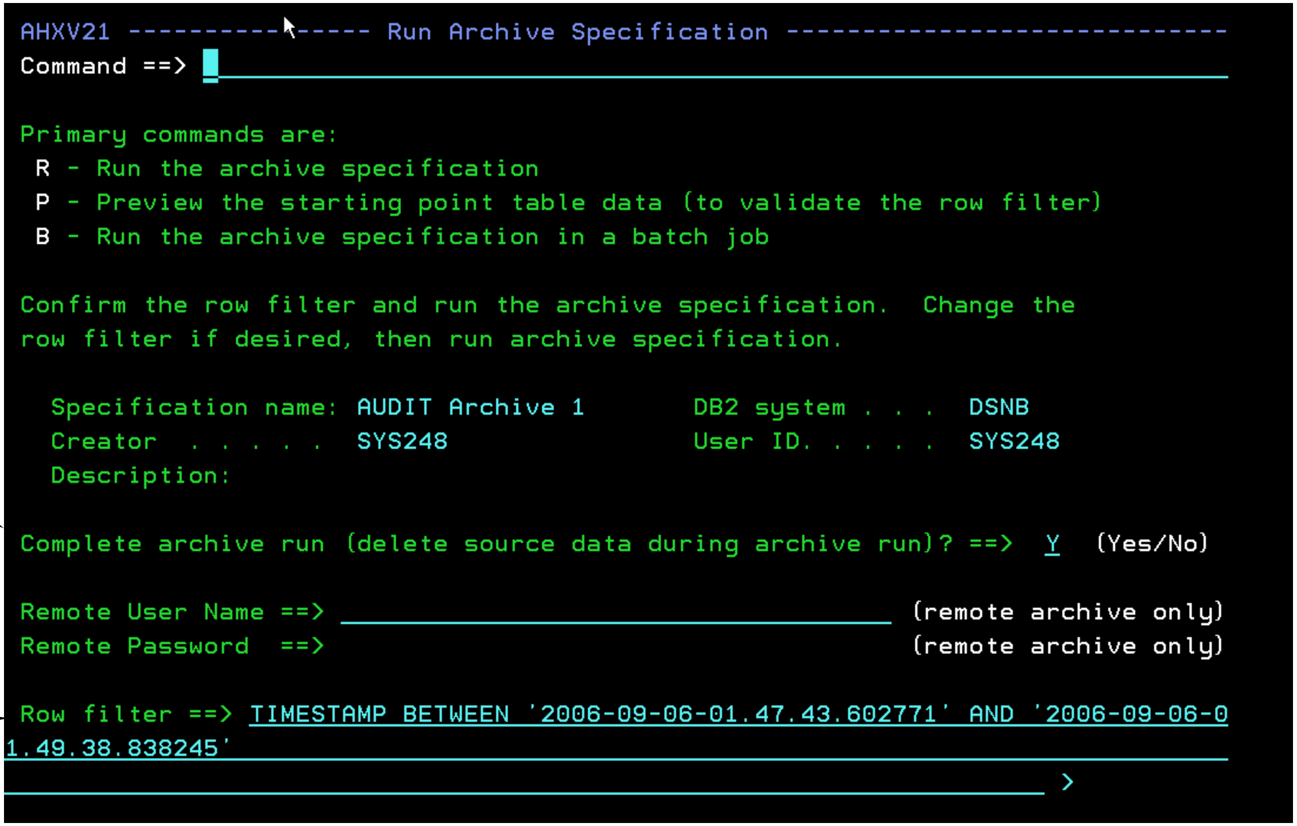
For this exercise, we’ll archive to a table archive. For file archive, we make different choices. Here we map the source table to the archive target. We can direct DAE to pre-existing target Database / Tablespace, or have them dynamically created for us.



```
AHXV21 ---------------- Map Source Tables to Archive Tables -- Row 1 to 1 of 1

Archive specification: AUDIT Archive 1

Map source tables to archive tables in the specified database and table space.
Commands:
 C  - Clear current table mappings
 TS - Specify table space and database for target tables

Line commands:
 T - Display target table selection list

You may apply a prefix and/or suffix to each target name.
 Prefix . ==> ____           Suffix . ==> ____
Cmd
============ ================== ===============================================
 _  Source : DB2PMFAUDT_DML      Target . . ==> DB2PMFAUDT_DML_ARC
            SYS248               Creator  . ==> SYS248
                                 Table space  : ARCHDML
                                 Database . . : AUDARCH



Command ==> __________________________________________________ Scroll ===> PAGE
```

My archives in AUDARCH

Run options are to execute in foreground or submit in batch. The Row Filter is validated for correct SQL syntax at specification time, but the “preview” option allows us to see what the result set will be prior to executing the specification.

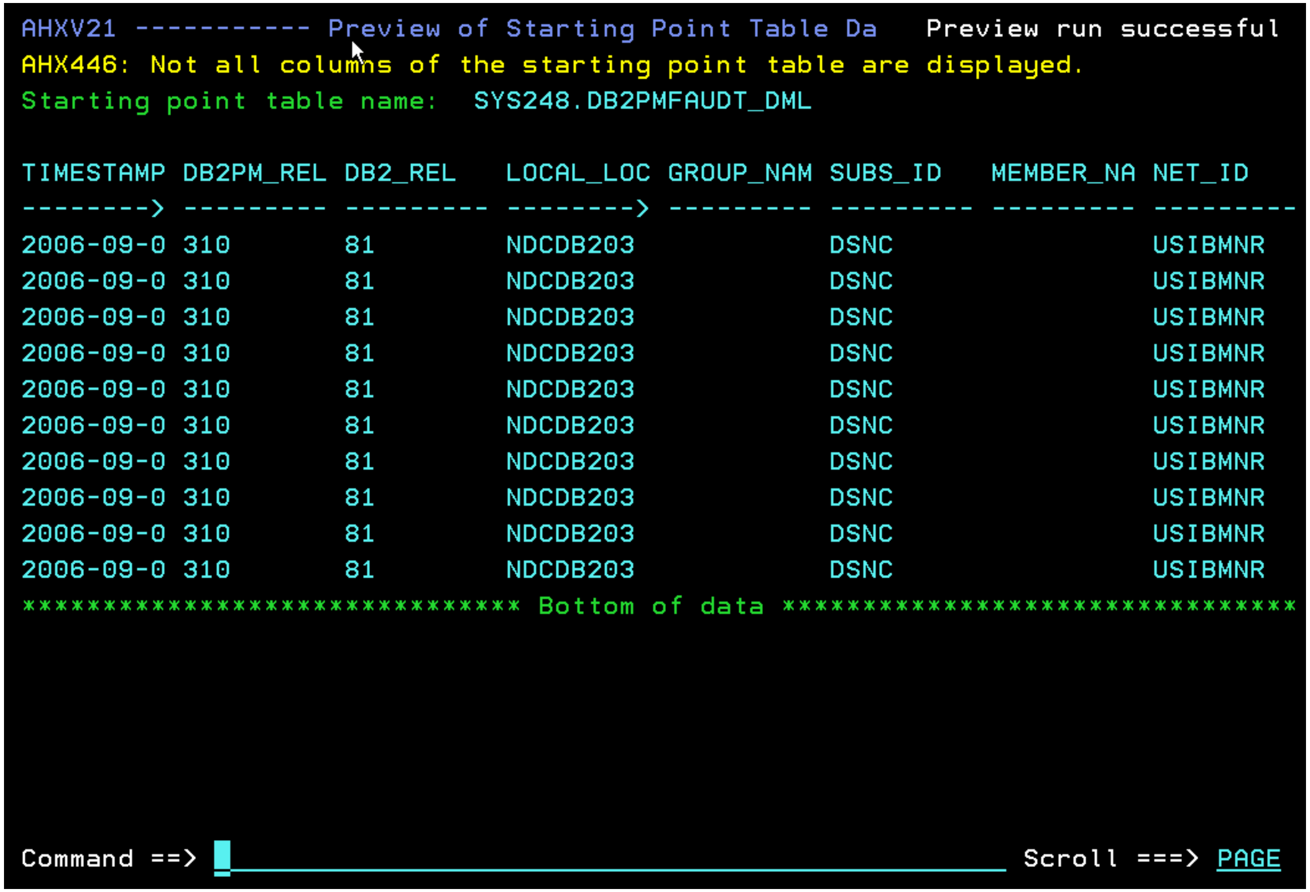


```
AHXV21 ---------------- Run Archive Specification -----------------------------
Command ==> _________________________________________________________________

Primary commands are:
 R - Run the archive specification
 P - Preview the starting point table data (to validate the row filter)
 B - Run the archive specification in a batch job

Confirm the row filter and run the archive specification.  Change the
row filter if desired, then run archive specification.

  Specification name: AUDIT Archive 1      DB2 system . . .  DSNB
  Creator  . . . . .  SYS248               User ID. . . . .  SYS248
  Description:

Complete archive run (delete source data during archive run)? ==> Y  (Yes/No)

Remote User Name ==> ____________________________________ (remote archive only)
Remote Password  ==>                                      (remote archive only)

Row filter ==> TIMESTAMP BETWEEN '2006-09-06-01.47.43.602771' AND '2006-09-06-0
1.49.38.838245'
_____________________________________________________________________ >
```

We can change completion

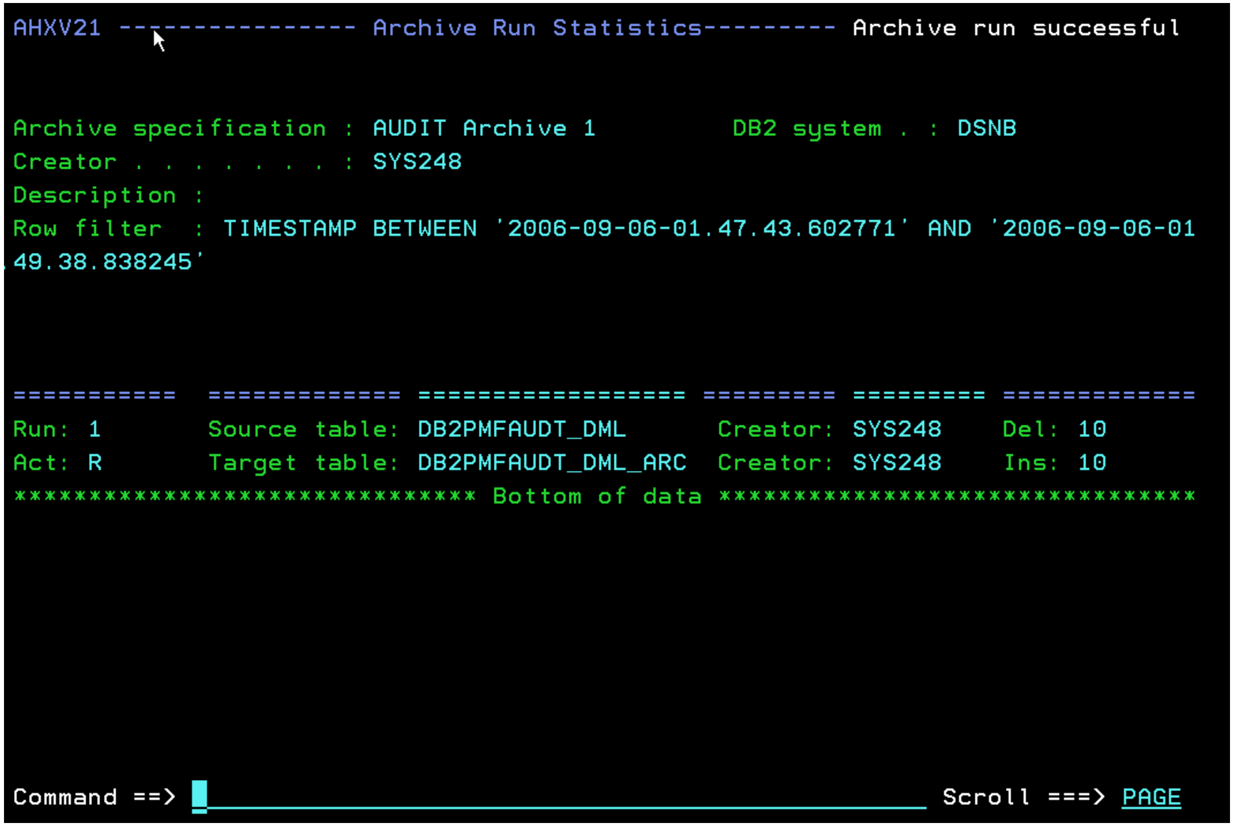
Filter modification allowed

Just a sampling, but we can verify that our row filter will affect the rows that we intended.



```
AHXV21 ----------- Preview of Starting Point Table Da   Preview run successful
AHX446: Not all columns of the starting point table are displayed.
Starting point table name:  SYS248.DB2PMFAUDT_DML

TIMESTAMP DB2PM_REL DB2_REL   LOCAL_LOC GROUP_NAM SUBS_ID   MEMBER_NA NET_ID
--------> --------- --------- --------> --------- --------- --------- ---------
2006-09-0 310       81        NDCDB203            DSNC                USIBMNR
2006-09-0 310       81        NDCDB203            DSNC                USIBMNR
2006-09-0 310       81        NDCDB203            DSNC                USIBMNR
2006-09-0 310       81        NDCDB203            DSNC                USIBMNR
2006-09-0 310       81        NDCDB203            DSNC                USIBMNR
2006-09-0 310       81        NDCDB203            DSNC                USIBMNR
2006-09-0 310       81        NDCDB203            DSNC                USIBMNR
2006-09-0 310       81        NDCDB203            DSNC                USIBMNR
2006-09-0 310       81        NDCDB203            DSNC                USIBMNR
2006-09-0 310       81        NDCDB203            DSNC                USIBMNR
******************************* Bottom of data ********************************




Command ==> ________________________________________________ Scroll ===> PAGE
```

Once the specification is run, the statistics are stored in the DAE metadata tables for reference.



```
AHXV21 ---------------- Archive Run Statistics--------- Archive run successful


Archive specification : AUDIT Archive 1          DB2 system . : DSNB
Creator . . . . . . . : SYS248
Description :
Row filter  : TIMESTAMP BETWEEN '2006-09-06-01.47.43.602771' AND '2006-09-06-01
.49.38.838245'




===========  ============= ================== ========= ========= =============
Run: 1       Source table: DB2PMFAUDT_DML      Creator: SYS248    Del: 10
Act: R       Target table: DB2PMFAUDT_DML_ARC  Creator: SYS248    Ins: 10
******************************* Bottom of data ********************************








Command ==> _________________________________________________ Scroll ===> PAGE
```

Additional Considerations

- **We chose to archive into an archive table. If we need to, we can now join the archive table with the active audit table if needed. We could have chosen to put the archive target on another DB2 and even archive to a UDB on AIX target.**
- **File archives work in a similar manner, the target is an UNLOAD file. In order to retrieve the data from a file archive, you need to restore (retrieve) into a retrieve target table, also managed by DAE.**

PCI – IBM Compliance Solution - Recap

- **Requirement 3: Protect Stored Data**
  - IBM Data Encryption Tool for DB2 and IMS Databases
- **Requirement 7: Restrict access to data by business “need to know”**
  - DB2 for z/OS V8 Multi-Level Security implemented via RACF
- **Requirement 10: Track and monitor all access to network resources and cardholder data**.
  - IBM Tivoli OMEGAMON XE for DB2 Performance Expert on z/OS
  - IBM Audit Management Expert
- **Requirement 10.7 Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulations.**
  - IBM Data Archive Expert