Data governance: Get in-depth DB2 auditing for more confident compliance

Ernie Mancill
Executive IT Specialist
DB2 for z/OS Tools

Information Management software

Disclaimer

The information contained in this presentation has not been submitted to any formal IBM review and is distributed on an "As Is" basis without any warranty either express or implied. The use of this information is a customer responsibility.

The measurement results presented here were run in a controlled laboratory environment using specific workloads. While the information here has been reviewed by IBM personnel for accuracy, there is no guarantee that the same or similar results will be obtained elsewhere. Performance results depend upon the workload and environment. Customers attempting to adapt this data to their own environments do so at their own risk.

In addition, the material in this presentation may be subject to enhancements or Programming Temporary Fixes (PTFs) subsequent to general availability of the code.

It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

Agenda

- Introduction
  - Regulatory Landscape
- System Z – Secure Platform for an insecure world
- DB2 on z/OS Security Support
  - DB2 on z/OS V8 Multi-Row Security
  - DB2 on z/OS V9 Trusted Context and Roles
- DB2 on z/OS Audit Trace
  - DB2 on z/OS V9 – Trace Improvements
  - DB2 on z/OS – Audit Trace Characteristics
- IBM Enterprise Data Governance Solutions
  - IBM Audit Management Expert for DB2
- IBM Enterprise Data Governance Software
- Q&A

Introduction: Regulatory Landscape

Information Management software

Why the Focus on Data Governance?

- **Tangible Costs to the enterprise**
  - Cost of notification campaign to affected customer base
  - Fines and financial penalties levied by regulators
  - Credit reporting costs
  - Reissuing credit instruments
  - Acquisition of technology and processes to redress breach
  - Gifts and concessions (compensation) to exposed customers
- **Intangible Costs**
  - Customer relationships terminated due lost confidence due to the breach
  - Target customer population who would have otherwise entered into a business relationship
  - Erosion of shareholder confidence
  - Diminished competitive standing in the marketplace
  - Legal redress by disenfranchised customer base
- **Bottom line**
  - Much more financially responsible to invest in compliance technology and processes before the breach occurs

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
    - VISA
    - Mastercard
    - AMEX
    - DISCOVER
  - Compliance is a mandated requirement
  - Severe penalties for non-compliance
  - Synchronicity with other compliance initiatives
  - Compliance viewed by many as competitive advantage

Different People have different “security” needs

- Chief Information Officer
  - Are my systems and data protected from inadvertent disclosure?
  - Are best practices deployed for security?
  - Should I build or buy security?
- Chief Financial Officer
  - Total cost of ownership – how much does “security” cost?
  - What return on investment does this spending deliver?
  - What risks/costs does it avoid?
- Chief Privacy Officer/Chief Information Security Officer
  - Can I meet Regulatory Compliance needs?
  - Are our processes auditable?
  - Are my IT Operations, Developers, End users/consumers educated on our security practices?
- Application Architects
  - Do we design “security” into the application architecture, add it after the fact or leave it up to the IT Operations staff?
- IT Operations
  - What products and technologies will best meet the needs/requirements of all the “executives” that have a security/compliance/audit focus in the business?

System Z – A Secure Platform for an Insecure World

z9 - a Security Overview

Information Management software

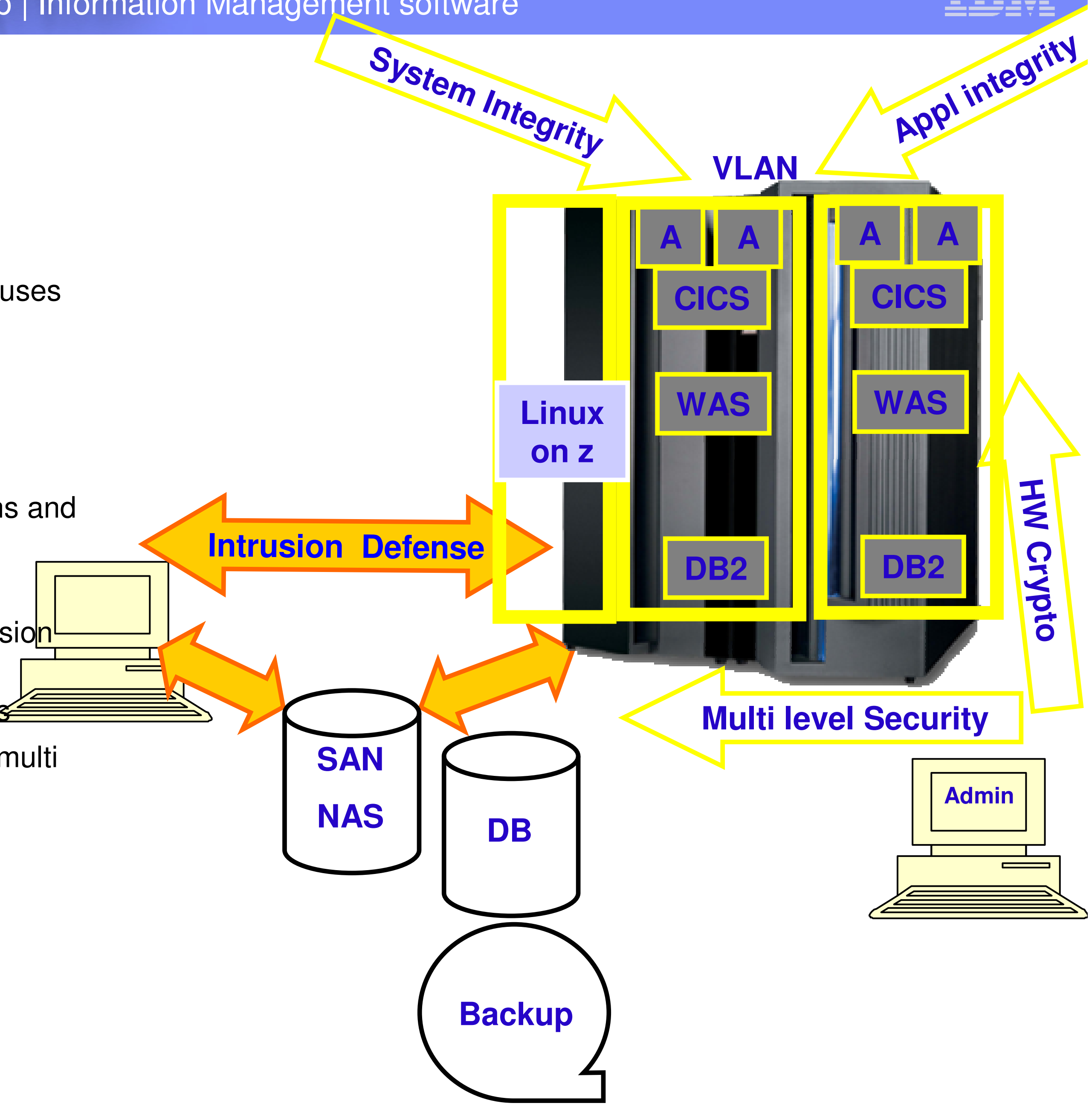
Protect sensitive information on line and off line

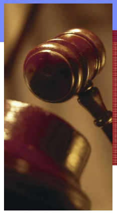
System z provides security without sacrificing responsiveness

- Protect the data
  - **End-to-end protection that helps keep data uncorrupted and uncompromised**
  - **Multiple Level Security for different levels of "need to know"**
- **Encrypt sensitive data**
- Prevent unauthorized access
  - **IBM Resource Access Control Facility – 25 years strong**
  - **Support for a variety of encryption algorithms**
  - **EAL5 and other security certifications**
- Secure and speed the transaction
  - **Specialized Cryptographic co-processor hardware**
- Monitor, manage, and control
  - **Centralized access and control helps lower security costs, meet compliance guidelines, and simplify audit trail.**
- Compliance with privacy/security legislation
  - **Auditability**
  - **Control**
  - **Recoverability**
- Solutions available
  - **DM tools from IBM**
  - **Tivoli Compliance InSight Manager**
  - **IBM Optim Solutions**

zSeries Architecture value

- System & Application Integrity
  - z/OS integrity statement
  - Inhibits trojan horses, worms & viruses via storage protection keys
  - Business Process Integration
  - Business Resilience
- Compartmentalization of work
  - Common Criteria certified partitions and guest isolation
  - Workload management
  - Virtual LANs reduce Security intrusion points
  - Middleware deployment processes
  - Row based security for DB2 and multi level security
- Data Confidentiality
  - Hardware encryption services
  - Encryption Key Management

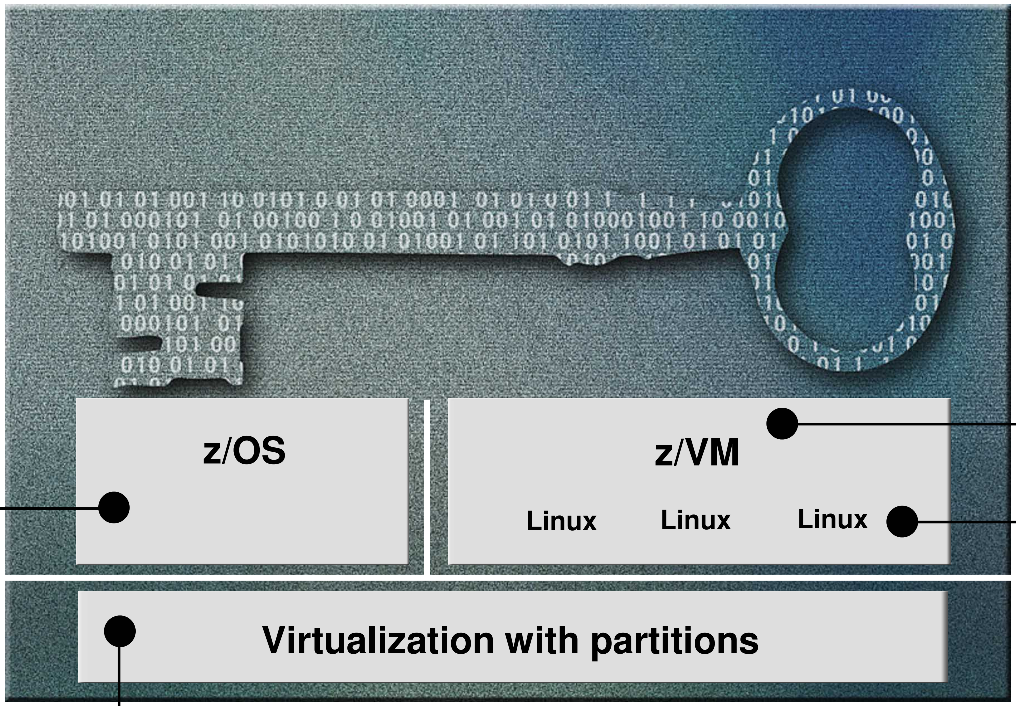




Certification of mainframe products and components

Certifications on System z

The Common Criteria program developed by NIST and NSA establishes an organizational and technical framework to evaluate the trustworthiness of IT Products and protection profiles



z/VM

- **Common Criteria** EAL3+ with CAPP and LSPP
  - **z/VM 5.1 + RACF**

Linux on System z

- **Common Criteria** EAL4+ with CAPP and LSPP
  - **SUSE LES9 certified**
- **Common Criteria** EAL3+ with CAPP and LSPP
  - **Red Hat EL3 certified at EAL3+**
  - **Red Hat EL4 EAL4+ in progress**

z/OS

- **Common Criteria** EAL4+ with CAPP and LSPP
  - z/OS 1.7 + RACF
- **IdenTrust™** certification for z/OS PKI Services

System z EC and other System z servers

- **Common Criteria** EAL5 with specific Target of Evaluation
  - **Logical partitions**
- FIPS 140-2 level 4
  - Crypto Express 2

See: www.**ibm.com**/security/standards/st_evaluations.shtml

DB2 V8 on z/OS : Multi-row Security
DB2 V9 on z/OS : Trusted Context and Roles

Access for “need to know” only

Information Management software

Multilevel Security

Provide access to data based on need to know

REQUIREMENT:

Data shared between people/organizations with different "need to know"

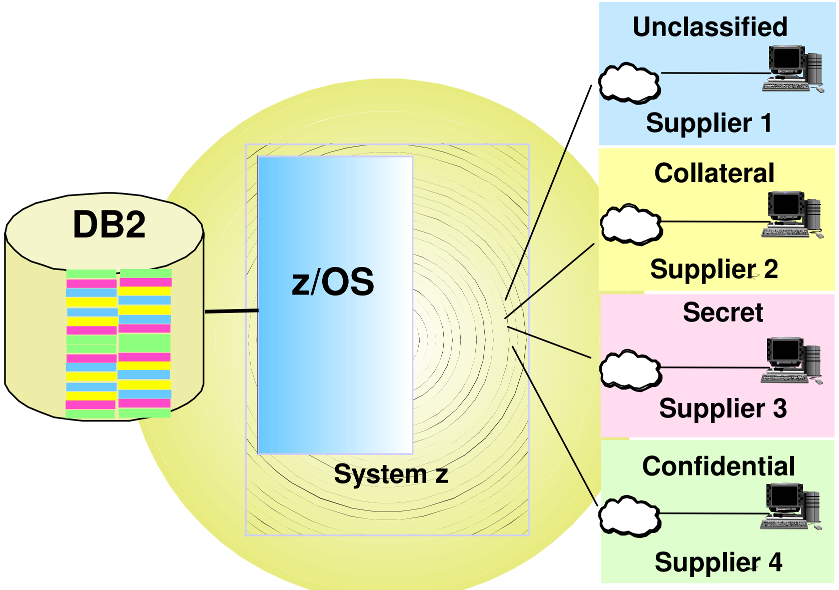
System z solution:

- **Highly secure access to DB2 databases**
- **Security labeling at the row-level of DB2**
- **With RACF as single security manager for both z/OS and DB2**

Public Sector: Hierarchical security

Commercial opportunities:

- Hosting similar applications
- Single database
  - **hosting subsidiaries**
  - **hosting partners**



MLS on System z

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’**
- **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 not seclabel assigned, then authorization failure and IFCID 140
  - 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 V1R7 and Security Server (RACF)**

Role and Trusted Context - Existing challenges

- **Single ID has all privileges (administrative + Business User). If stolen significant exposure**
- **As Business user authentication done by middleware, DB2 does not know who does what, e.g. “admin” vs. “end user”. Lack of accountability/auditability**
- **Trust all connection requests?**
  - Parm applies to all, means no authentication, not practical
  - Lack of already verified option inhibited migration from SNA to TCP/IP
- **Shared SYSADM ID or DBADM ID to avoid cascading effect when someone leaves unit**
  - **Create view for another but cannot alter it**
  - **Privileges granted can be exercised from anywhere**
  - **Full time DBA access to all prod data AND sensitive/private data**
  - **Privileges always available to DBA**
  - **Dual responsibilities (prod + dev) can lead to mistakes**

Trusted context functional overview

- **Requires RACF V1.8 and DB2 V9 NFM**
- Trusted context addresses the problem of establishing a trusted relationship between DB2 and an external entity, such as a middleware server.
- A series of trust attributes are evaluated at connect time to determine if a specific connection is to be trusted.
- The relationship between a connection and a trusted context is established when a connection to the server is first created
- Once established, a trusted connection provides the ability to:
  - Use the trusted connection for a different user without authentication.
  - Acquire special set of privileges by an authorization ID, that are not available to it outside the trusted context. This is accomplished by associating a role with the trusted context.
  - Allow a role to own objects, if objects are created in a trusted context with role defined as the owner.
- Trusted context provides:
  - User accountability
  - Improved Security and Manageability
  - Ability of DBADM to perform DDL on behalf of others via database role

Database role functional overview

- Can optionally be the owner of DB2 objects. A ROLE can be dropped if it owns no objects
- **Removing a person’s ROLE does not cause the objects to be cascade deleted**
- Role is independent of it’s creator. Allows a DBA to have privileges to create objects and manage them for a time, even though ownership is to be another id.
- Without roles, transferring ownership implies drop/recreate
- Implement on weekend, privileges no longer available on Monday morning
- Roles are a way to allow multiple DBA authids to have ownership of an object at the same time or at different times
- An example, how to secure privileged access via ROLE:
  - Grant DBA privileges to a ROLE
  - At the point where an application change needs to be implemented by DBA:
  - Assign DBA ROLE to DBA via trusted context
  - Via V9 audit trace filtering, start audit trace of the ROLE
  - DBA is performs necessary object change activity to support application change
  - Revoke Trusted Context assigned to DBA
  - Turn off audit trace and generate audit trace report
  - Review and store the audit trace report as necessary for compliance

DB2 V8 and V9 on z/OS : Trace improvements and Audit Trace characteristics

Who, What, When, and Where?

Information Management software

V9 Trace Extensions – START TRACE

- Qualifications by:
  - LOC
    - Location-Name
    - LUName
    - IPAddress
  - PLAN
  - PACKAGE
    - PKGLOC
    - PKGCOL
    - PKGPROG
  - Workstation Identifiers
    - USERID
    - APPLNAME
    - WRKSTN
  - Miscellaneous
    - CORRID
    - CONNID
    - ROLE

- Exclude by:
  - LOC
    - XLOC
  - PLAN
    - XPLAN
  - PACKAGE
    - XPKGLOC
    - XPKGCOL
    - XPKGPROG
  - Workstation Identifiers
    - XUSERID
    - XAPPLID
    - XWRKSTN
  - Miscellaneous
    - XCORRID
    - XCONNID
    - XROLE

V9 Trace Extensions - Wildcards

- Tracing threads using the * wildcard:
  - You can use the wildcard suffix, "*" to filter threads. For example, if you specify "-START TRACE PLAN (A,B,C*)", DB2 will trace, and then return A, B, CDE, CDEFG, CDEFGH, and so on. It will trace threads "A", "B" and all threads starting with "C".
- Tracing threads using the positional, (_) wildcard:
  - You can utilize the positional wildcard, which is represented by the, "_" character, to trace threads when you want the wildcard in the middle, or when you want to trace threads of a specific length. For example, if you specify "-START TRACE PLAN (A_C), all threads will be traced that are three characters that have "A" as the first character, and "C" as the third.
- Tracing multiple threads at once using wildcards:
  - You also have the option of tracing multiple threads based on multiple trace qualifications. For example, you can specify, "-START TRACE PLAN (A*, B*, C*) to simultaneously trace ALL threads for plan that start with "A", "B", and "C". The wildcard character, "*" will trace all threads.
  - You have the ability to filter multiple threads at the same time, setting specific criteria for the trace: For example, you can specify "-START TRACE PLAN (A) USERID (B). This will trace the threads where the plan thread is A, and the user ID is B.

V9 Trace Extensions – Some Restrictions

- When tracing threads, you can only specify more than one thread criteria for one filter per “-START TRACE” command.
  - For example, you can specify “-START TRACE PLAN (A,B) USERID (B) WRKSTN (E),” but you cannot specify “-START TRACE PLAN (A, B) USERID (A, B) WRKSTN (E).
- If you use one or no values for PLAN, AUTHID, or LOCATION, the START TRACE command starts a single trace. If you use multiple values for PLAN, AUTHID, or LOCATION, the command starts a trace for each plan, authorization ID, or location. There can be up to 32 traces going at one time.
- You must use a privilege set of the process that includes one of the following privileges or authorities:
  - TRACE privilege
  - SYSOPR authority
  - SYSCTRL authority
  - SYSADM authority

Audit class Events that are traced

1. Access attempts that DB2 denies because of inadequate authorization. This class is the default.
2. Explicit GRANT and REVOKE statements and their results. This class does not trace implicit grants and revokes.
3. CREATE, ALTER, and DROP statements that affect audited tables, and the results of these statements. This class traces the dropping of a table that is caused by DROP TABLESPACE or DROP DATABASE and the creation of a table with AUDIT CHANGES or AUDIT ALL. ALTER TABLE statements are audited only when they change the AUDIT option for the table.
4. Changes to audited tables. Only the first attempt to change a table, within a unit of recovery, is recorded. (If the agent or the transaction issues more than one COMMIT statement, the number of audit records increases accordingly.) The changed data is not recorded, only the attempt to make a change is recorded. If the change is not successful and is rolled back, the audit record remains; it is not deleted. This class includes access by the LOAD utility.

   Accesses to a dependent table that are caused by attempted deletions from a parent table are also audited. The audit record is written even if the delete rule is RESTRICT, which prevents the deletion from the parent table. The audit record is also written when the rule is CASCADE or SET NULL, which can result in deletions that cascade to the dependent table.
5. All read accesses to tables that are identified with the AUDIT ALL clause. As in class 4, only the first access within a DB2 unit of recovery is recorded. References to a parent table are also audited.
6. The bind of static and dynamic SQL statements of the following types:
   - INSERT, UPDATE, DELETE, CREATE VIEW, and LOCK TABLE statements for audited tables. Except for the values of host variables, the audit record contains the entire SQL statement.
   - SELECT statements on tables that are identified with the AUDIT ALL clause. Except for the values of host variables, the audit record contains the entire SQL statement.
7. Assignment or change of an authorization ID because of the following reasons:
   - Changes through an exit routine (default or user-written)
   - Changes through a SET CURRENT SQLID statement
   - An outbound or inbound authorization ID translation
   - An ID that is being mapped to a RACF ID from a Kerberos security ticket
8. The start of a utility job, and the end of each phase of the utility.
9. Various types of records that are written to IFCID 0146 by the IFI WRITE function.

Audit Trace Overhead *V8 admin*

- The performance impact of auditing is directly dependent on the amount of audit data produced. When the audit trace is active, the more tables that are audited and the more transactions that access them, the greater the performance impact. The overhead of audit trace is typically less than 5% but workload dependent.
- When estimating the performance impact of the audit trace, consider the frequency of certain events. For example, security violations are not as frequent as table accesses. The frequency of utility runs is likely to be measured in executions per day. Alternatively, authorization changes can be numerous in a transaction environment.
- Following is the summary of results of the DB2 V8 Audit trace measurements :

  The measurements were done with Audit trace class(*) on, similar to the tool.
  All the tables in the workload were enabled for 'Audit All'.

  For OLTP measurement with distributed IRWW SQL CLI workload with 9 Tables, 3 PI, 8 NPI and 7 transactions running at 493 transactions per second,
  the DB2 Class 2 CPU increase was +7.2%.

  For Utility measurements with LOAD, Rebuild Index, Reorg Table, Reorg Index utilities using 1 Table, 10 partitions, 1 PI and 5 NPI, there was no measurable CPU increase.
- Weigh auditing requirements against workload and anticipated impacts to application service levels and performance objectives carefully.

What to Audit

- **Closed Application Environment (*Probably not a candidate*)**
  - **Traditional Application controls well defined and comprehensive**
    - **CICS and IMS TM – Signon and Transaction Access secured via RACF**
    - **Production Batch – Controlled via program pathing / Job Scheduling**
- Data mining – no risk of update but access audit might be needed
- Adhoc environnent – QMF, SPUFI, etc. Constitutes exposure
  - SPUFI Plan can be restricted but ALL use should be audited
  - Privleged ID's (DBA) should be audited
  - SYSADMIN are difficult to audit
- Distributed Application Environment
  - Use of SQLESETI can provide granularity with credential population to IFI extensions
    - End User Workstation Name
    - End User Workstation Process
    - End User Workstation Userid
- "Offline" Utilities and certain tools are used outside of DB2
  - RACF dataset access defined controls
- Use of DSN1COPY should be restricted
- Data may not be as granular as you think
  - Depending on how you configured your connections into DB2 – CICS attach, SAP, or CICS users with unique id's, and distributed transactions. May get all audit data but may not be meaningful because of attach environments. Group versus AUTHID. SQLESETI implementation can help

What to Audit?- Continued

- Some items that should always be audited – low overhead
  - DB2 commands
  - DDL
  - Class 1 – attempts
  - Class 2
  - Class 3
  - Class 7 – set current SQL ID (exclude OMPE and authorized users)
  - Class 8 – utilities
  - Class 4 and 5 only run for SYSADM users
- Audit classes 1, 2, and 7 add no additional overhead. Because most transactions do not result in authorization failures or issue GRANTs, REVOKEs, or utilities, running these trace classes is cost-effective.

Limitations of the audit trace

- The audit trace does not record everything, as the following list of limitations indicates:
  - The auditing that is described in this information takes place only when the audit trace is on.
  - The trace does not record old data after it is changed because the log records old data.
  - If an agent or transaction accesses a table more than once in a single unit of recovery, the audit trace records only the first access.
  - The audit trace does not record accesses if you do not start the audit trace for the appropriate class of events.
  - The audit trace does not audit some utilities. The trace audits the first access of a table with the LOAD utility, but it does not audit access by the COPY, RECOVER, and REPAIR utilities. The audit trace does not audit access by stand-alone utilities, such as DSN1CHKR and DSN1PRNT. (And most 3rd party utilities)
  - The trace audits only the tables that you specifically choose to audit.
  - You cannot audit access to auxiliary tables.
  - You cannot audit the catalog tables because you cannot create or alter catalog tables.
- This auditing coverage is consistent with the goal of providing a moderate volume of audit data with a low impact on performance. However, when you choose classes of events to audit, consider that you might ask for more data than you are willing to process.

IBM Audit Management Expert for DB2 V2 : Technology Introduction

Who, What, When, and Where?

Information Management software

Audit Management Expert Overview

- Auditors will be able to Access:
  - SELECT, INSERT, UPDATE, and DELETE activity by user or by object
  - **SQL Text and Host Variable value for each statement**
    - **Row count that SQL statement affects**
  - CREATE, ALTER, and DROP operations against an audited object
  - Explicit GRANT and REVOKE operations
  - Utility access to an audited object
  - DB2 commands entered
  - Assignment or modification of an authorization ID
  - Authorization failures
- **Provides auditors with flexible options for examining the data in the audit repository**
  - Audit Trace Data, **Audit SQL Collector (ASC),** Log Analysis data
    - V2.1 no longer needs to alter objects to ‘AUDIT ALL’ for read/update
    - DB2 Catalog Objects can now be audited for SQL read/update

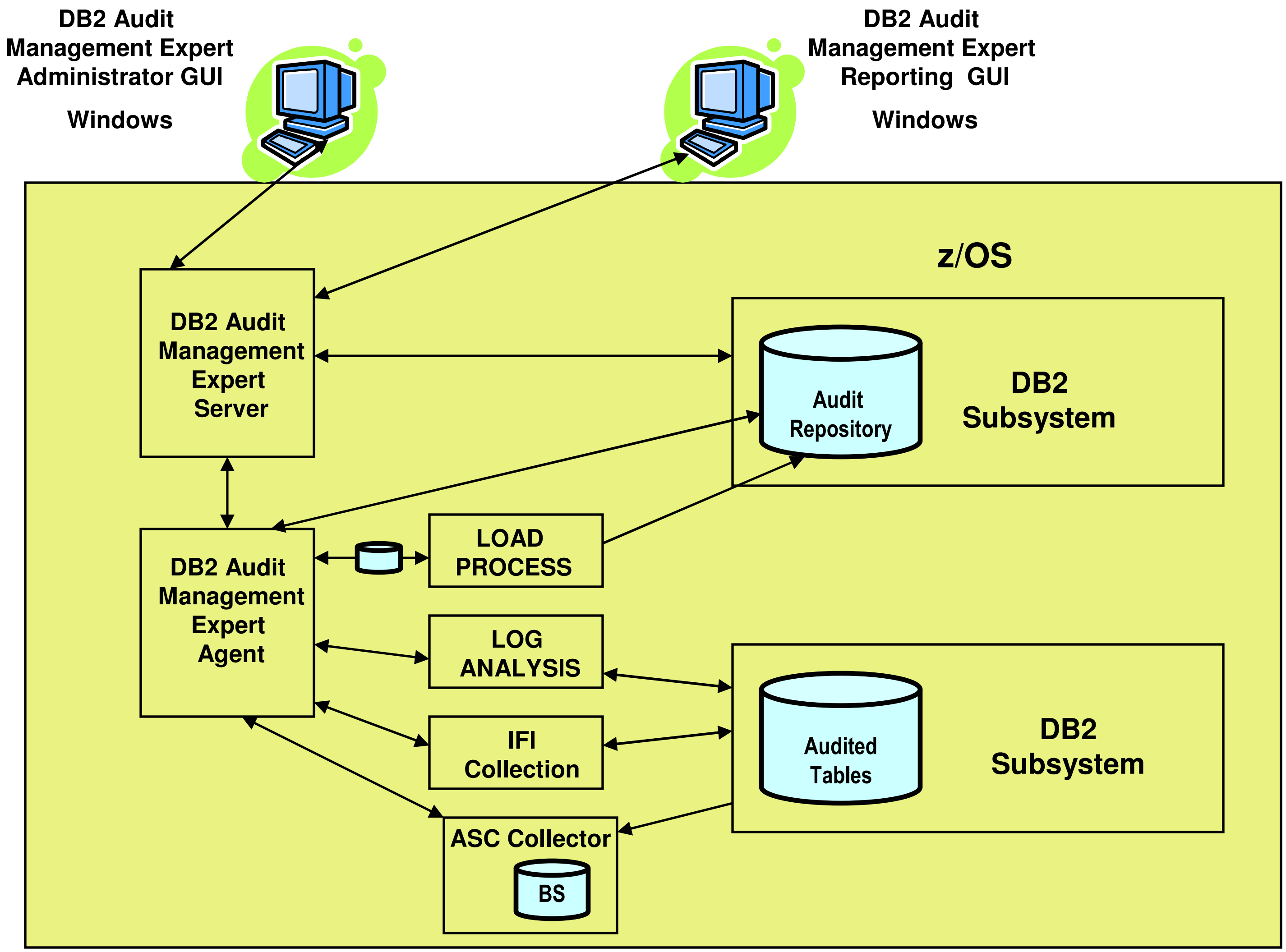
Security and separation of roles

- Supporting internal and external auditors in collection and reporting of DB2 audit data
- Does not require auditors to be DB2 defined users within the monitored DB2 system(s)
- Does not require the auditors to log on to the operating system where the monitored system is running
- Does not require extensive interaction between the auditor and the system support personnel (DBA/Sys admin)
- Auditor will not be able to directly manipulate any DB2 resources
- Provide complete visibility of all auditable objects to an administrator level user
- Provide controls for limiting visibility to auditors of auditable objects
- Removes DBA from audit data collection process. With V2.1 removes the "ALTER for AUDIT" requirement

DB2 Audit Management Expert Components

- Audit server
  - Started task or batch job
  - central control point for an Audit Management Expert network
  - single audit server can support data collection from multiple agents on multiple z/OS systems
- Agent
  - Started Task or batch job
  - responsible for communications in an Audit Management Expert environment
  - acts as a ″container″ to run the various collectors
  - One per DB2 to Audit
- CLIENT User interfaces
  - Audit Management Expert Reporter
  - Audit Management Expert Administration
  - Windows

DB2 Audit Management Expert Architecture


DB2 Audit Management Expert Administrator GUI
Windows
DB2 Audit Management Expert Reporting GUI
Windows
z/OS
DB2 Audit Management Expert Server
Audit Repository
DB2 Subsystem
DB2 Audit Management Expert Agent
LOAD PROCESS
LOG ANALYSIS
IFI Collection
ASC Collector
BS
Audited Tables
DB2 Subsystem

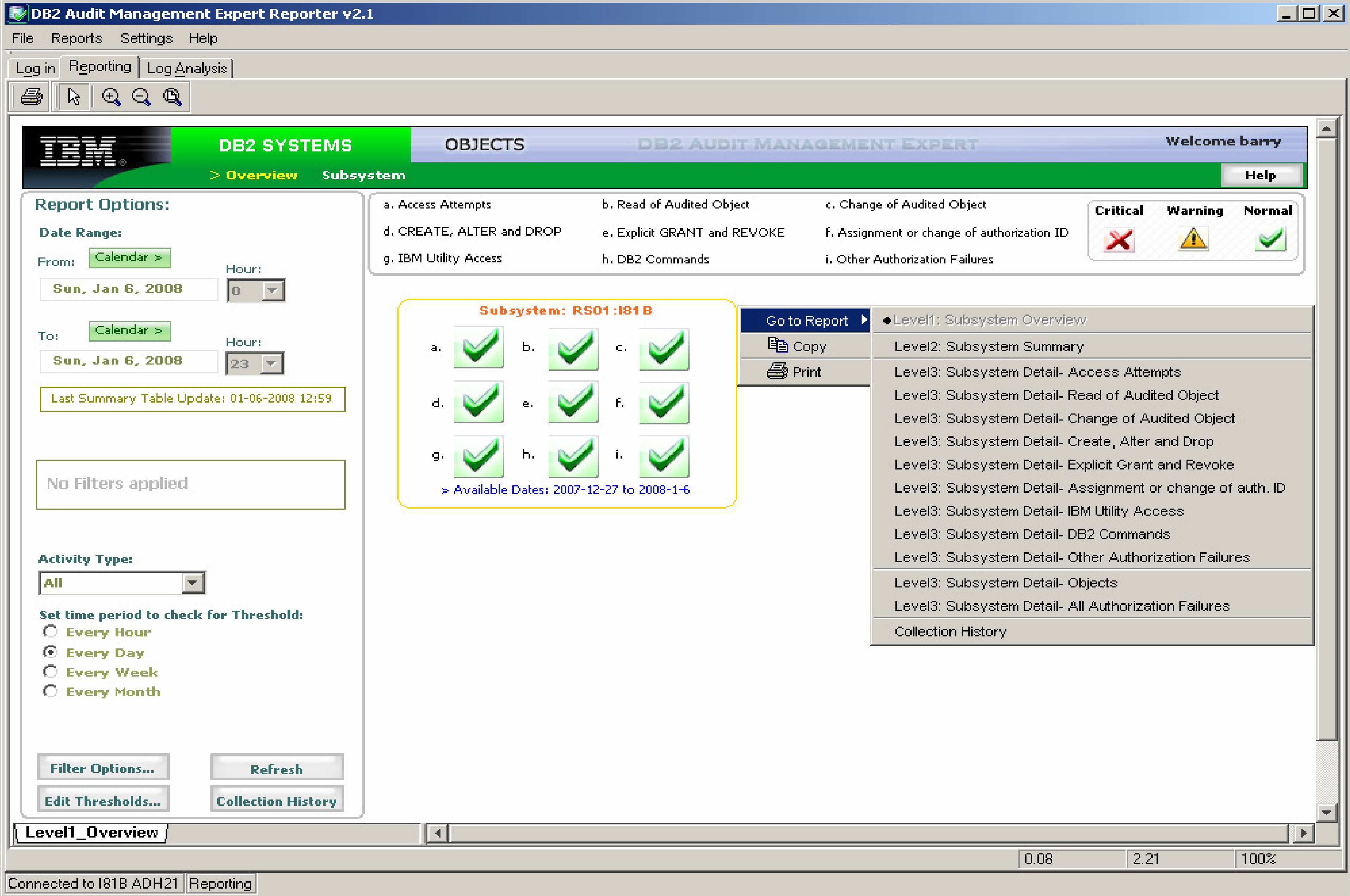
ASC- Audit SQL Collector

DB2 Audit Management Expert Profiles

- Profiles are created/maintained via **Administration UI**
  - Collection Profile
    - records the details for what audit data is stored to the Audit Management Expert repository
  - Agent Profile
    - Select ASC collection method
    - Configure General settings
      - Retention count, interval length
    - DB2 Load utility parameters
    - Define Job cards for load and log analysis
  - User Profile
    - contain information specific to an individual Audit Management Expert user such as: the user type, configurable privileges, and associated user groups

Reporting Facilities

- UI Reporting options enable auditors to view and report on data in a variety of ways
  - Overview – Level 1
    - View all of the subsystems currently being monitored
    - based on summary tables
    - available filters are AUTHID and PLANS
  - Subsystem – Level 2
    - View activity for a selected subsystem
    - based on summary tables
    - available filters are AUTHID and PLANS
  - Detail - Level 3
    - View details for a particular type of activity for a selected subsystem
    - not based on the summary tables
    - 20 possible filters to choose from
  - Graphical or Tabular
- AME 2.1 provides extensive report filtering
- Batch reporting



DB2 Audit Management Expert Reporter v2.1

Report Options:

Date Range:

From: Calendar > Sun, Jan 6, 2008 Hour: 0

To: Calendar > Sun, Jan 6, 2008 Hour: 23

Last Summary Table Update: 01-06-2008 12:59

No Filters applied

Activity Type: All

Set time period to check for Threshold:

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

a. Access Attempts	b. Read of Audited Object	c. Change of Audited Object
d. CREATE, ALTER and DROP	e. Explicit 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: RS01 :I81B

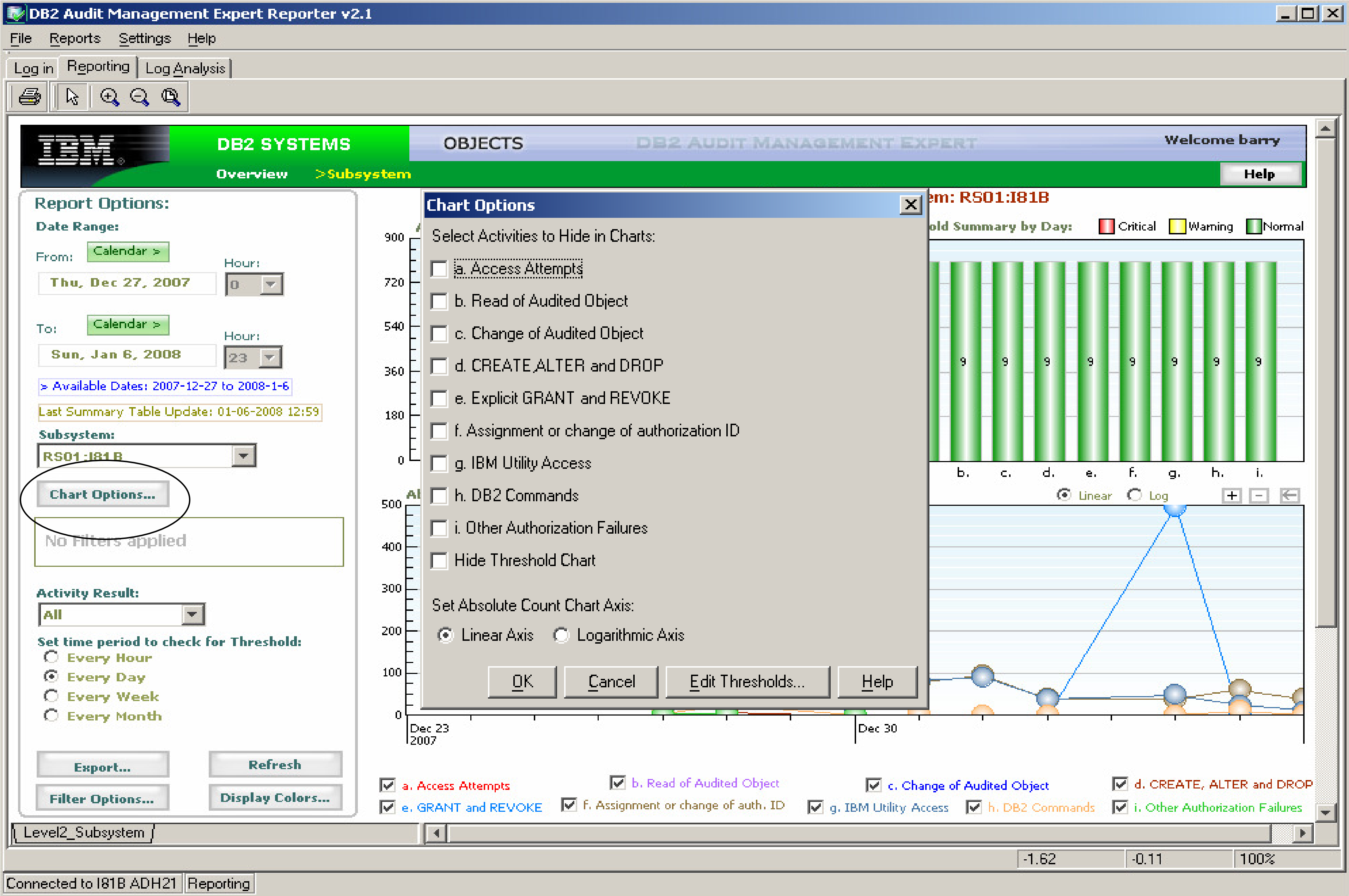
a. ✓	b. ✓	c. ✓
d. ✓	e. ✓	f. ✓
g. ✓	h. ✓	i. ✓

> Available Dates: 2007-12-27 to 2008-1-6

Go to Report
Copy
Print
Level1: Subsystem Overview
Level2: Subsystem Summary
Level3: Subsystem Detail- Access Attempts
Level3: Subsystem Detail- Read of Audited Object
Level3: Subsystem Detail- Change of Audited Object
Level3: Subsystem Detail- Create, Alter and Drop
Level3: Subsystem Detail- Explicit Grant and Revoke
Level3: Subsystem Detail- Assignment or change of auth. ID
Level3: Subsystem Detail- IBM Utility Access
Level3: Subsystem Detail- DB2 Commands
Level3: Subsystem Detail- Other Authorization Failures
Level3: Subsystem Detail- Objects
Level3: Subsystem Detail- All Authorization Failures
Collection History
Level1_Overview

0.08 2.21 100%

Connected to I81B ADH21 Reporting



DB2 Audit Management Expert Reporter v2.1

Report Options:

Date Range:

From: Calendar > — Thu, Dec 27, 2007 — Hour: 0

To: Calendar > — Sun, Jan 6, 2008 — Hour: 23

> Available Dates: 2007-12-27 to 2008-1-6

Last Summary Table Update: 01-06-2008 12:59

Subsystem: RS01:I81B

Chart Options...

No Filters applied

Activity Result: All

Set time period to check for Threshold:

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

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

Chart Options

Select Activities to Hide in Charts:

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

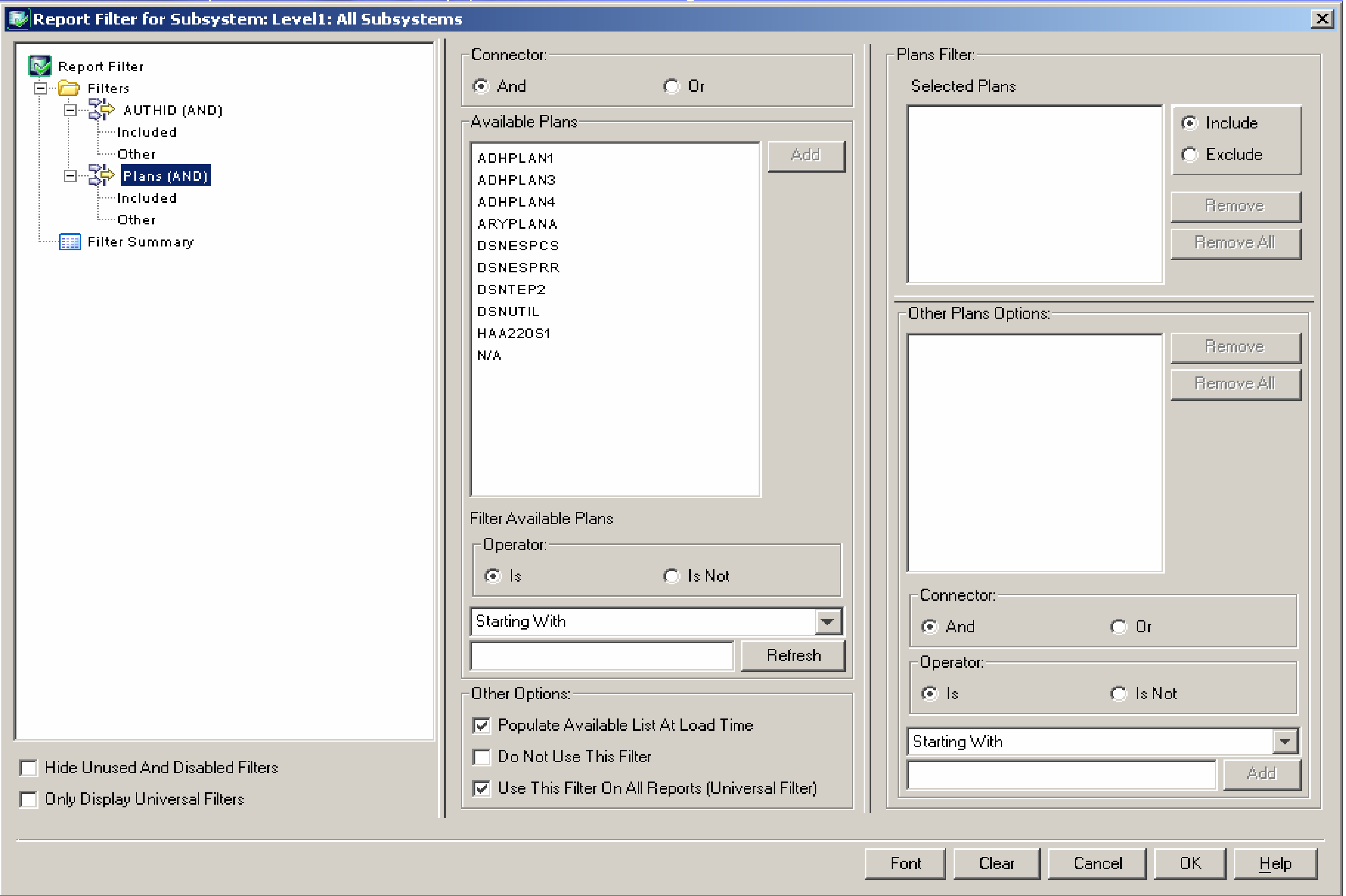
Set Absolute Count Chart Axis:

● Linear Axis ○ Logarithmic Axis

OK Cancel Edit Thresholds... Help

☑ a. Access Attempts ☑ b. Read of Audited Object ☑ c. 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

Connected to I81B ADH21 Reporting



Report Filter for Subsystem: Level1: All Subsystems

- Report Filter
  - Filters
    - AUTHID (AND)
      - Included
      - Other
    - Plans (AND)
      - Included
      - Other
  - Filter Summary

□ Hide Unused And Disabled Filters

□ Only Display Universal Filters

Connector: ● And ○ Or

Available Plans

- ADHPLAN1
- ADHPLAN3
- ADHPLAN4
- ARYPLANA
- DSNESPCS
- DSNESPRR
- DSNTEP2
- DSNUTIL
- HAA220S1
- N/A

Add

Filter Available Plans

Operator: ● Is ○ Is Not

Starting With

Refresh

Other Options:

☑ Populate Available List At Load Time

□ Do Not Use This Filter

☑ Use This Filter On All Reports (Universal Filter)

Plans Filter:

Selected Plans

● Include

○ Exclude

Remove

Remove All

Other Plans Options:

Remove

Remove All

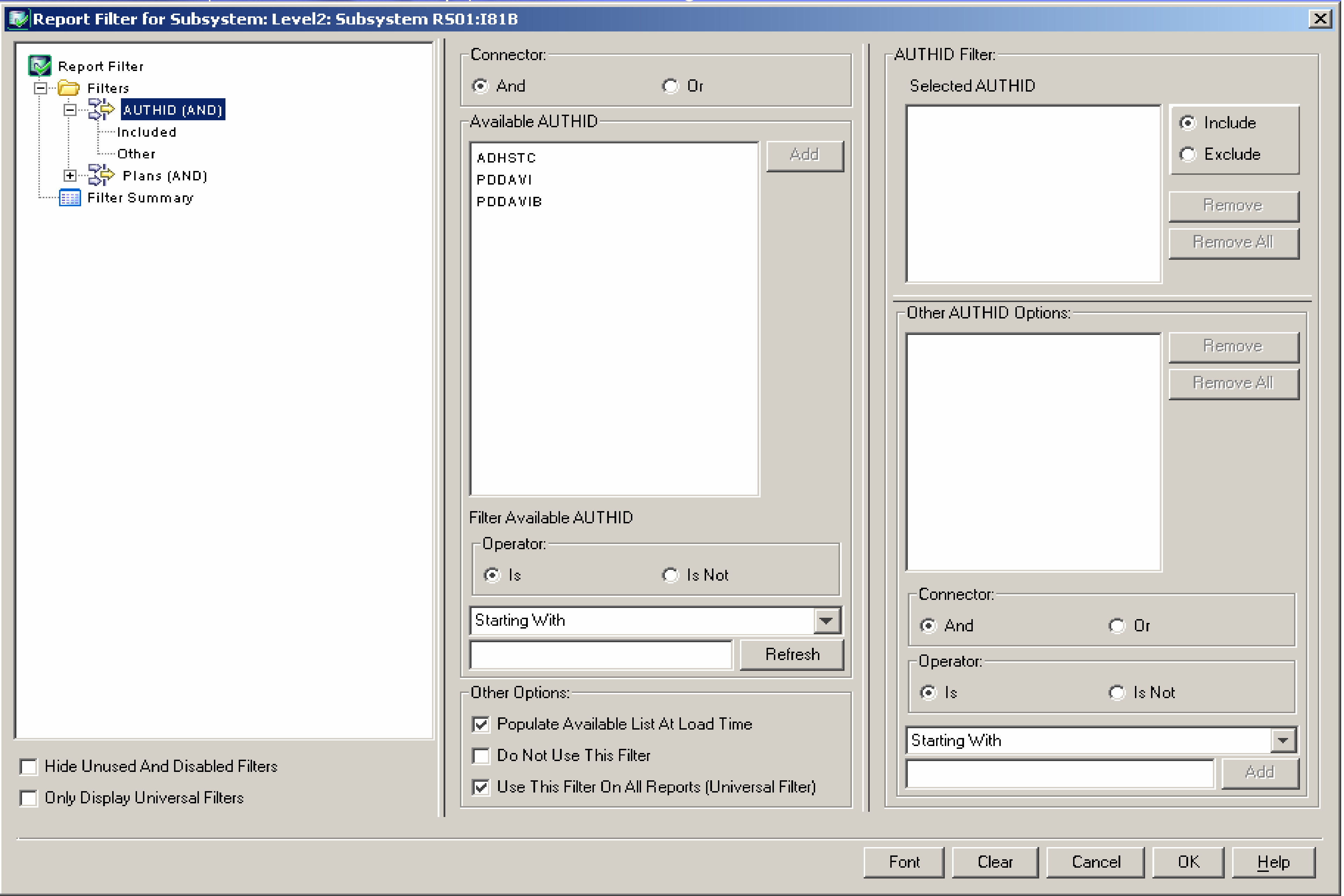
Connector: ● And ○ Or

Operator: ● Is ○ Is Not

Starting With

Add

Font | Clear | Cancel | OK | Help



Report Filter for Subsystem: Level2: Subsystem RS01:I81B

- Report Filter
  - Filters
    - AUTHID (AND)
      - Included
      - Other
    - Plans (AND)
  - Filter Summary

□ Hide Unused And Disabled Filters

□ Only Display Universal Filters

Connector: ● And ○ Or

Available AUTHID:

ADHSTC
PDDAVI
PDDAVIB

Filter Available AUTHID

Operator: ● Is ○ Is Not

Starting With

Other Options:

☑ Populate Available List At Load Time

□ Do Not Use This Filter

☑ Use This Filter On All Reports (Universal Filter)

AUTHID Filter:

Selected AUTHID

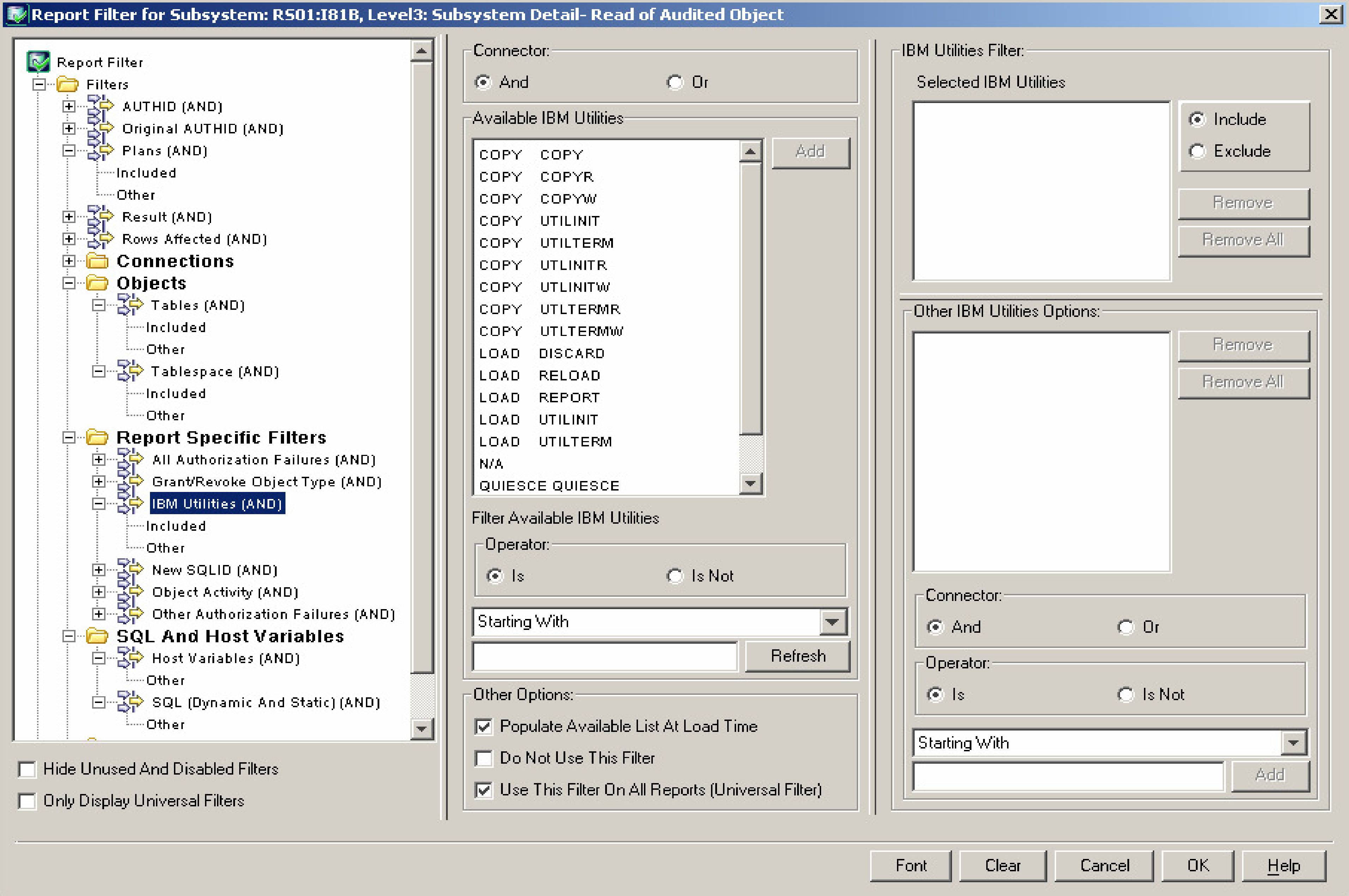
● Include ○ Exclude

Other AUTHID Options:

Connector: ● And ○ Or

Operator: ● Is ○ Is Not

Starting With



Report Filter for Subsystem: RS01:I81B, Level3: Subsystem Detail- Read of Audited Object

- Report Filter
  - Filters
    - AUTHID (AND)
    - Original AUTHID (AND)
    - Plans (AND)
      - Included
      - Other
    - Result (AND)
    - Rows Affected (AND)
    - Connections
    - Objects
      - Tables (AND)
        - Included
        - Other
      - Tablespace (AND)
        - Included
        - Other
    - Report Specific Filters
      - All Authorization Failures (AND)
      - Grant/Revoke Object Type (AND)
      - IBM Utilities (AND)
        - Included
        - Other
      - New SQLID (AND)
      - Object Activity (AND)
      - Other Authorization Failures (AND)
    - SQL And Host Variables
      - Host Variables (AND)
        - Other
      - SQL (Dynamic And Static) (AND)
        - Other

□ Hide Unused And Disabled Filters

□ Only Display Universal Filters

Connector: ● And ○ Or

Available IBM Utilities

```
COPY    COPY
COPY    COPYR
COPY    COPYW
COPY    UTILINIT
COPY    UTILTERM
COPY    UTLINITR
COPY    UTLINITW
COPY    UTLTERMR
COPY    UTLTERMW
LOAD    DISCARD
LOAD    RELOAD
LOAD    REPORT
LOAD    UTILINIT
LOAD    UTILTERM
N/A
QUIESCE QUIESCE
```

Filter Available IBM Utilities

Operator: ● Is ○ Is Not

Starting With

Other Options:

☑ Populate Available List At Load Time

□ Do Not Use This Filter

☑ Use This Filter On All Reports (Universal Filter)

IBM Utilities Filter:

Selected IBM Utilities

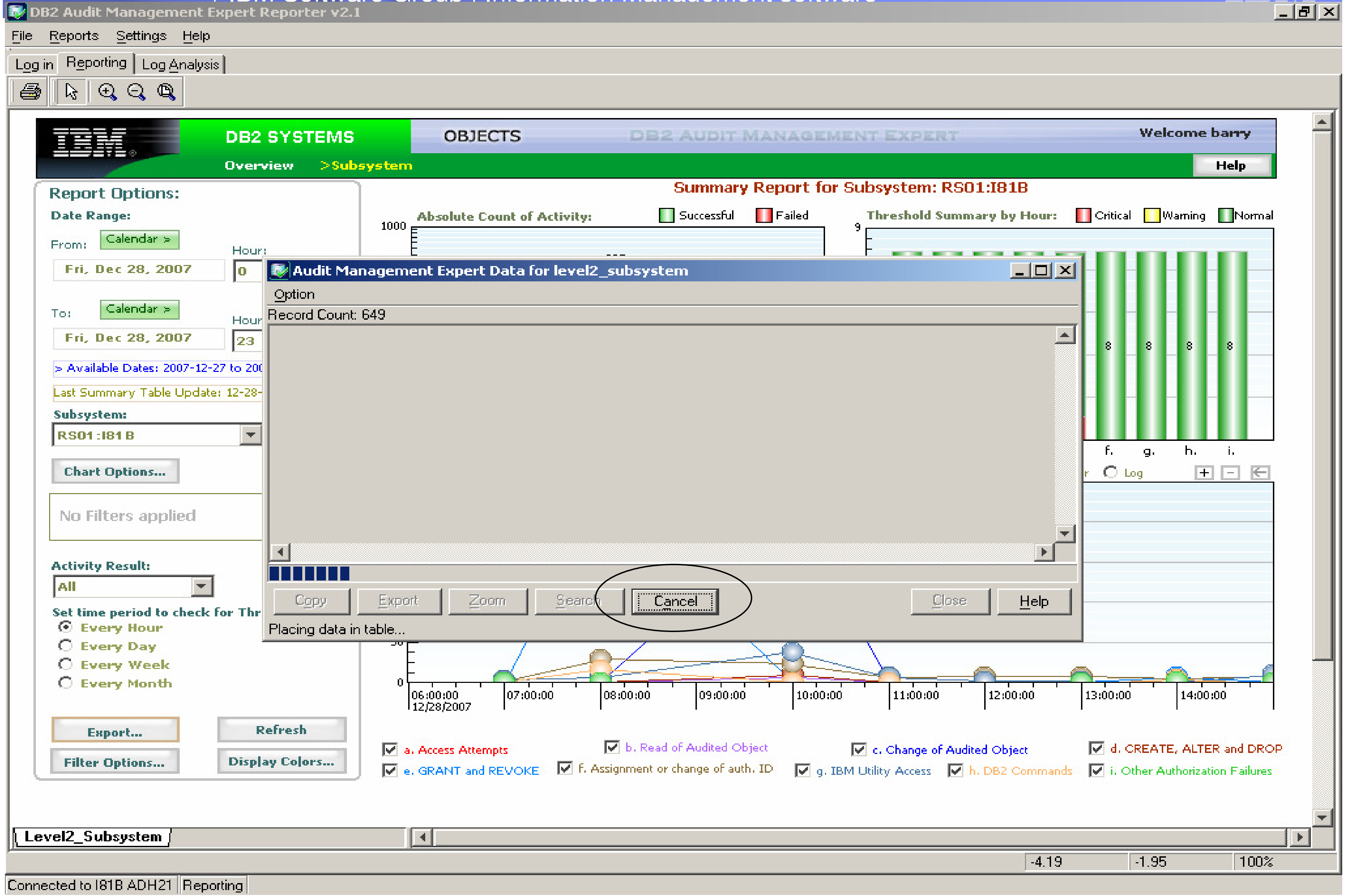
● Include ○ Exclude

Other IBM Utilities Options:

Connector: ● And ○ Or

Operator: ● Is ○ Is Not

Starting With



Summary Report for Subsystem: RS01:I81B

Report Options:

Date Range:

From: Fri, Dec 28, 2007 Hour: 0

To: Fri, Dec 28, 2007 Hour: 23

> Available Dates: 2007-12-27 to 200

Last Summary Table Update: 12-28-

Subsystem: RS01 :I81 B

No Filters applied

Activity Result: All

Set time period to check for Thr

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

Absolute Count of Activity: 🟩 Successful 🟥 Failed

Threshold Summary by Hour: 🟥 Critical 🟨 Warning 🟩 Normal

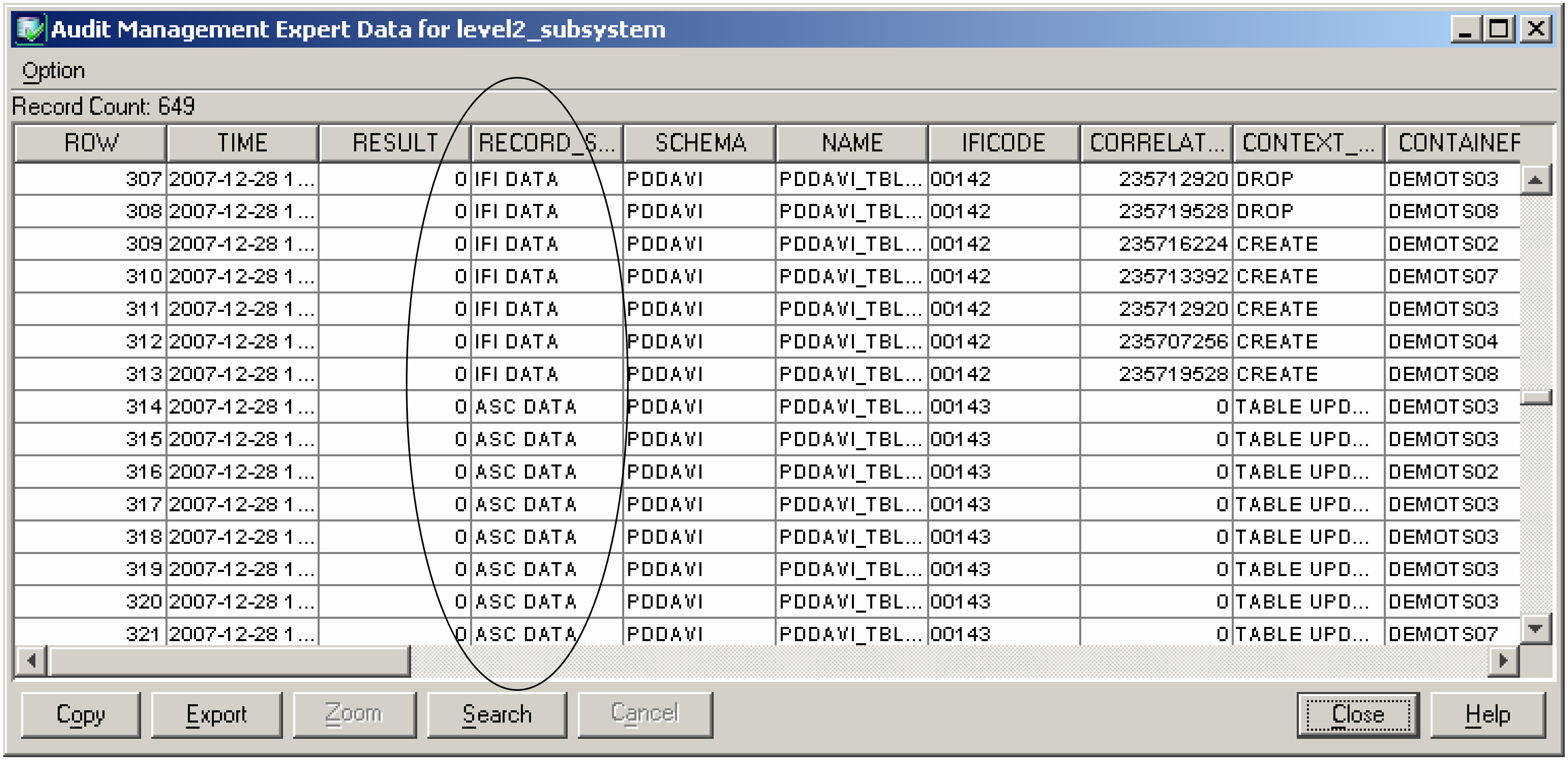
Record Count: 649

Placing data in table...

☑ a. Access Attempts ☑ b. Read of Audited Object ☑ c. 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

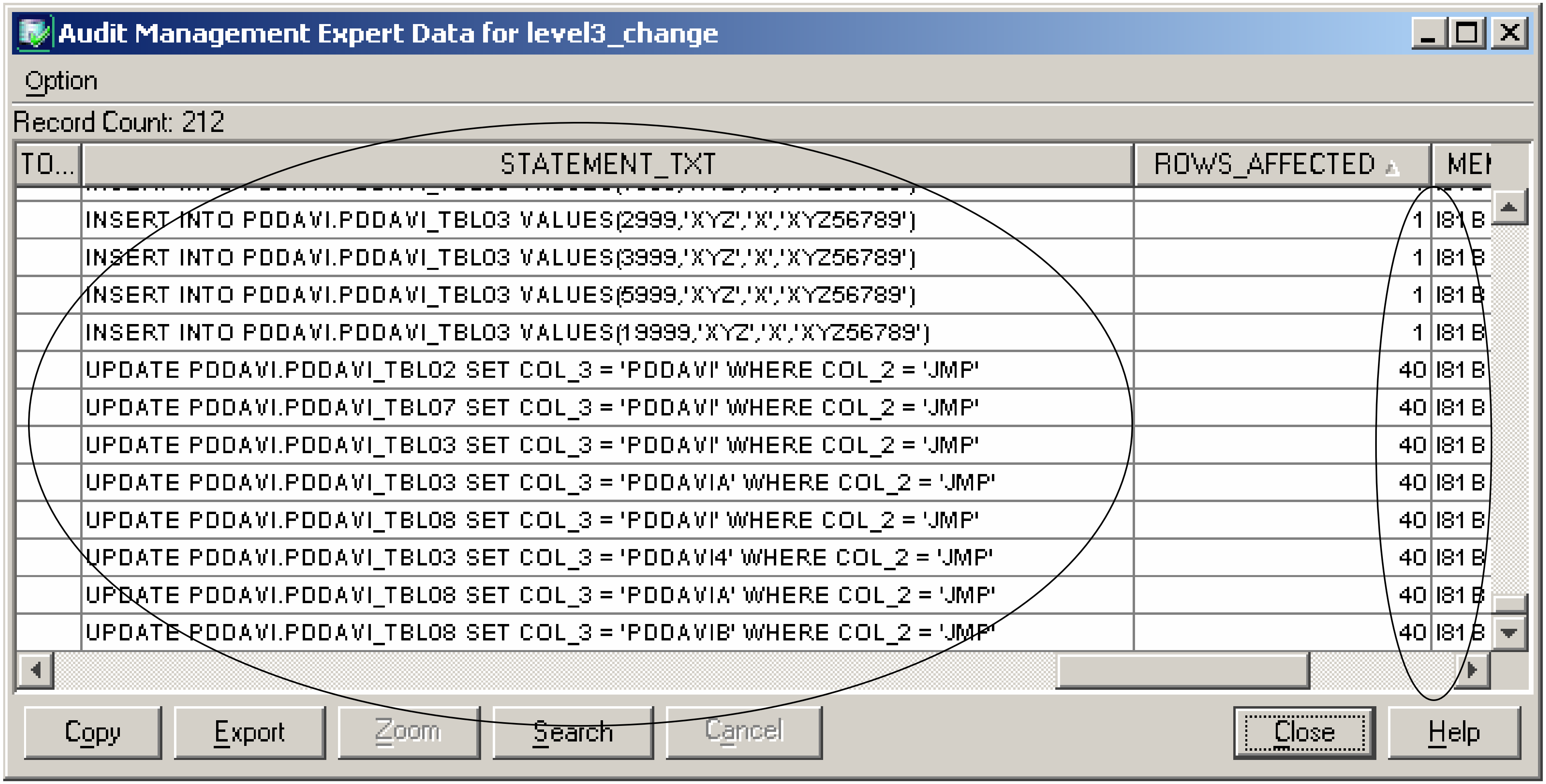
Connected to I81B ADH21 | Reporting



Audit Management Expert Data for level2_subsystem

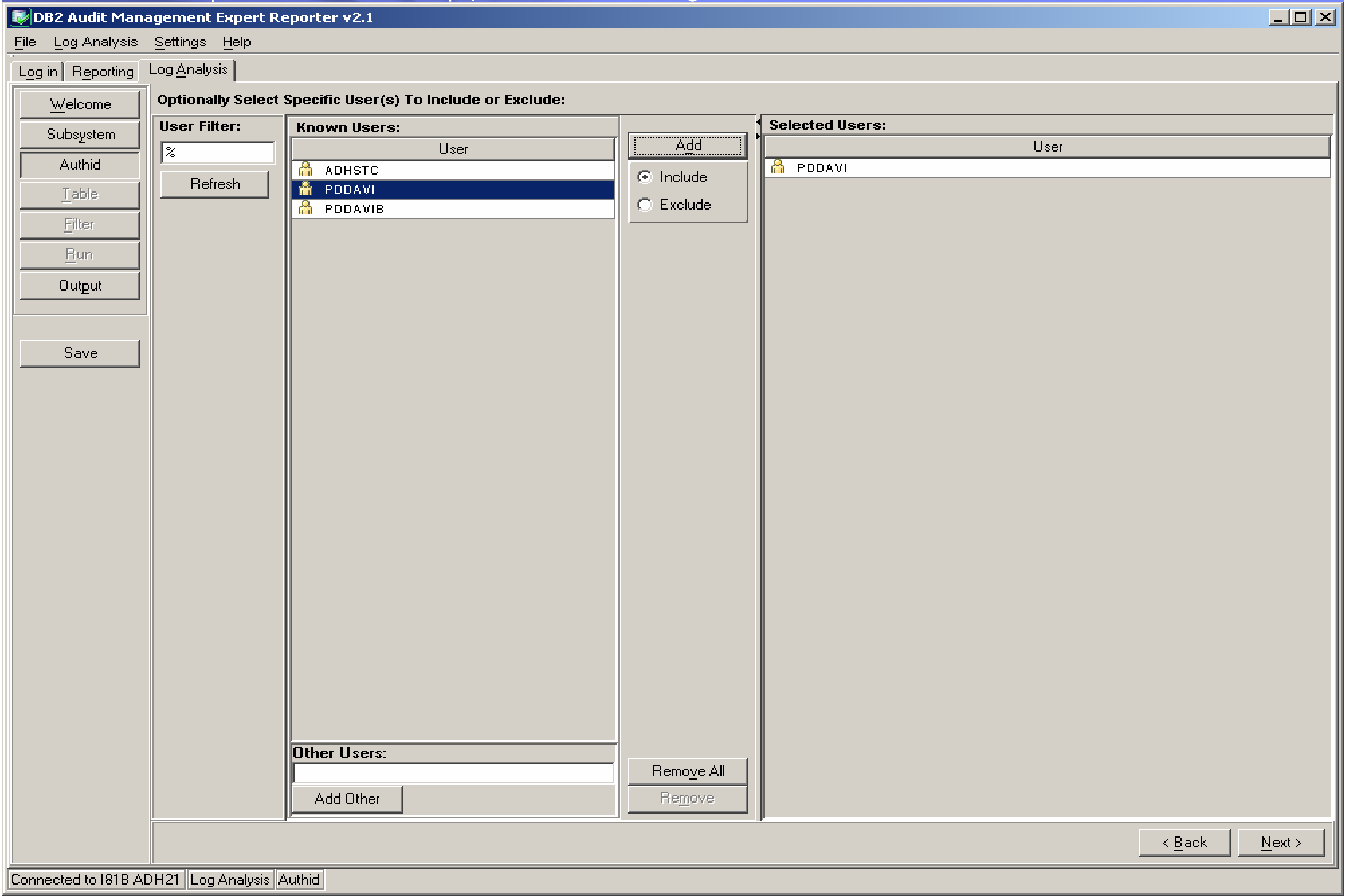
Record Count: 649

ROW	TIME	RESULT	RECORD_S...	SCHEMA	NAME	IFICODE	CORRELAT...	CONTEXT_...	CONTAINEF
307	2007-12-28 1 ...	0	IFI DATA	PDDAVI	PDDAVI_TBL...	00142	235712920	DROP	DEMOTS03
308	2007-12-28 1 ...	0	IFI DATA	PDDAVI	PDDAVI_TBL...	00142	235719528	DROP	DEMOTS08
309	2007-12-28 1 ...	0	IFI DATA	PDDAVI	PDDAVI_TBL...	00142	235716224	CREATE	DEMOTS02
310	2007-12-28 1 ...	0	IFI DATA	PDDAVI	PDDAVI_TBL...	00142	235713392	CREATE	DEMOTS07
311	2007-12-28 1 ...	0	IFI DATA	PDDAVI	PDDAVI_TBL...	00142	235712920	CREATE	DEMOTS03
312	2007-12-28 1 ...	0	IFI DATA	PDDAVI	PDDAVI_TBL...	00142	235707256	CREATE	DEMOTS04
313	2007-12-28 1 ...	0	IFI DATA	PDDAVI	PDDAVI_TBL...	00142	235719528	CREATE	DEMOTS08
314	2007-12-28 1 ...	0	ASC DATA	PDDAVI	PDDAVI_TBL...	00143	0	TABLE UPD...	DEMOTS03
315	2007-12-28 1 ...	0	ASC DATA	PDDAVI	PDDAVI_TBL...	00143	0	TABLE UPD...	DEMOTS03
316	2007-12-28 1 ...	0	ASC DATA	PDDAVI	PDDAVI_TBL...	00143	0	TABLE UPD...	DEMOTS02
317	2007-12-28 1 ...	0	ASC DATA	PDDAVI	PDDAVI_TBL...	00143	0	TABLE UPD...	DEMOTS03
318	2007-12-28 1 ...	0	ASC DATA	PDDAVI	PDDAVI_TBL...	00143	0	TABLE UPD...	DEMOTS03
319	2007-12-28 1 ...	0	ASC DATA	PDDAVI	PDDAVI_TBL...	00143	0	TABLE UPD...	DEMOTS03
320	2007-12-28 1 ...	0	ASC DATA	PDDAVI	PDDAVI_TBL...	00143	0	TABLE UPD...	DEMOTS03
321	2007-12-28 1 ...	0	ASC DATA	PDDAVI	PDDAVI_TBL...	00143	0	TABLE UPD...	DEMOTS07



Record Count: 212

TO...	STATEMENT_TXT	ROWS_AFFECTED	MEI
	INSERT INTO PDDAVI.PDDAVI_TBL03 VALUES(2999,'XYZ','X','XYZ56789')	1	I81 B
	INSERT INTO PDDAVI.PDDAVI_TBL03 VALUES(3999,'XYZ','X','XYZ56789')	1	I81 B
	INSERT INTO PDDAVI.PDDAVI_TBL03 VALUES(5999,'XYZ','X','XYZ56789')	1	I81 B
	INSERT INTO PDDAVI.PDDAVI_TBL03 VALUES(19999,'XYZ','X','XYZ56789')	1	I81 B
	UPDATE PDDAVI.PDDAVI_TBL02 SET COL_3 = 'PDDAVI' WHERE COL_2 = 'JMP'	40	I81 B
	UPDATE PDDAVI.PDDAVI_TBL07 SET COL_3 = 'PDDAVI' WHERE COL_2 = 'JMP'	40	I81 B
	UPDATE PDDAVI.PDDAVI_TBL03 SET COL_3 = 'PDDAVI' WHERE COL_2 = 'JMP'	40	I81 B
	UPDATE PDDAVI.PDDAVI_TBL03 SET COL_3 = 'PDDAVIA' WHERE COL_2 = 'JMP'	40	I81 B
	UPDATE PDDAVI.PDDAVI_TBL08 SET COL_3 = 'PDDAVI' WHERE COL_2 = 'JMP'	40	I81 B
	UPDATE PDDAVI.PDDAVI_TBL03 SET COL_3 = 'PDDAVI4' WHERE COL_2 = 'JMP'	40	I81 B
	UPDATE PDDAVI.PDDAVI_TBL08 SET COL_3 = 'PDDAVIA' WHERE COL_2 = 'JMP'	40	I81 B
	UPDATE PDDAVI.PDDAVI_TBL08 SET COL_3 = 'PDDAVIB' WHERE COL_2 = 'JMP'	40	I81 B



DB2 Audit Management Expert Reporter v2.1

Optionally Select Specific User(s) To Include or Exclude:

User Filter: %

Known Users:

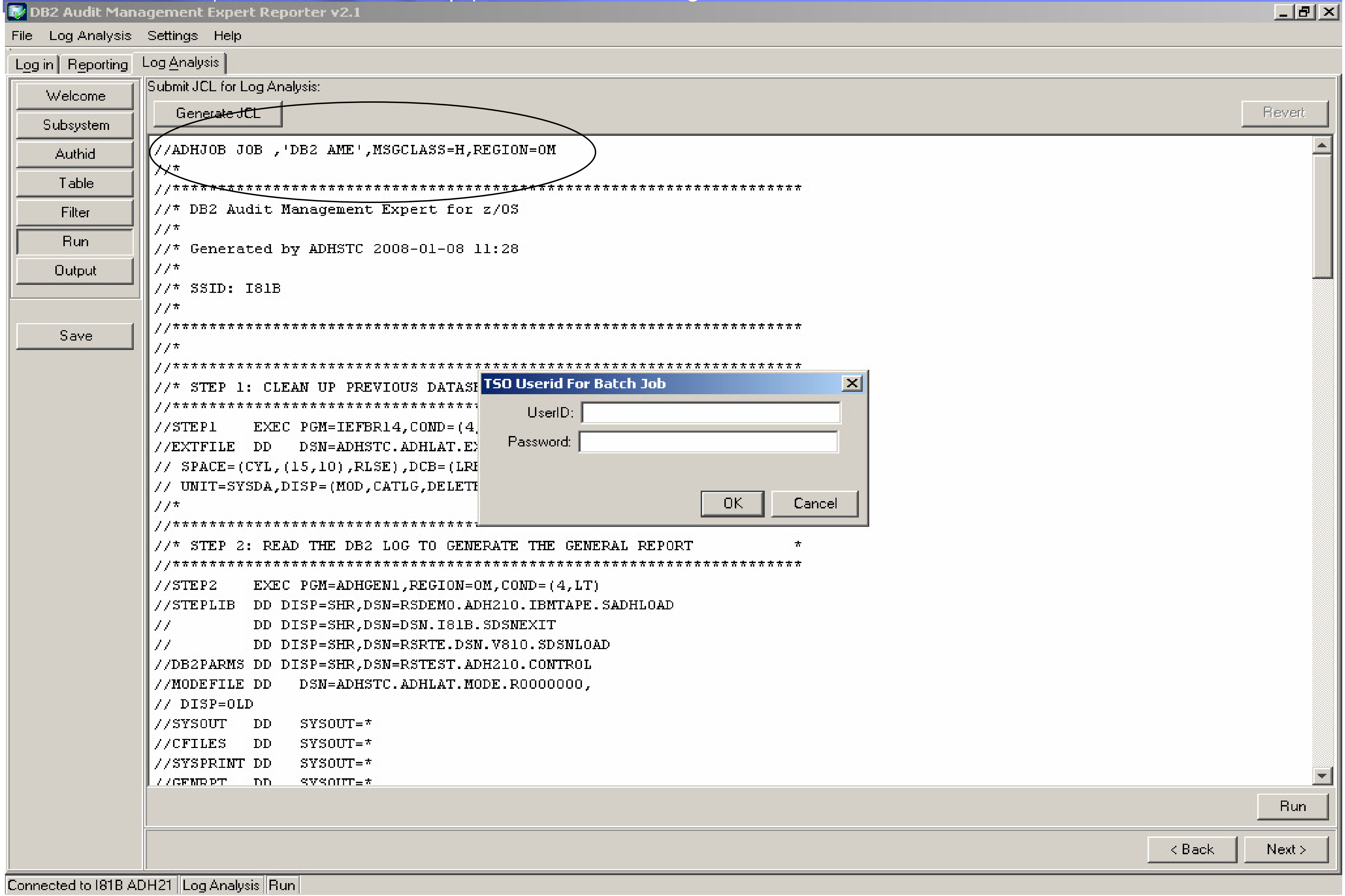
User
ADHSTC
PDDAVI
PDDAVIB

● Include
○ Exclude

Selected Users:

User
PDDAVI

Connected to I81B ADH21 | Log Analysis | Authid



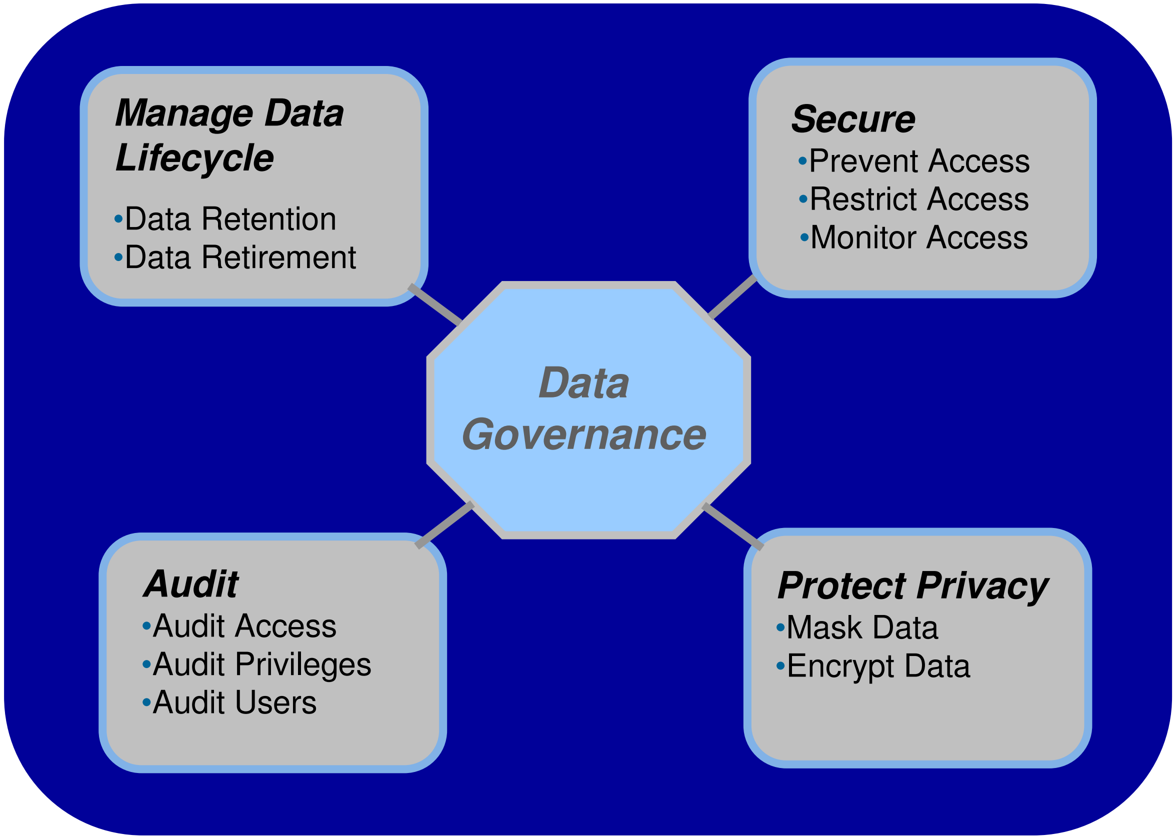
```
//ADHJOB JOB ,'DB2 AME',MSGCLASS=H,REGION=0M
//*
//*********************************************************************
//* DB2 Audit Management Expert for z/OS
//*
//* Generated by ADHSTC 2008-01-08 11:28
//*
//* SSID: I81B
//*
//*********************************************************************
//*
//*********************************************************************
//* STEP 1: CLEAN UP PREVIOUS DATASE
//*********************************
//STEP1    EXEC PGM=IEFBR14,COND=(4,
//EXTFILE  DD   DSN=ADHSTC.ADHLAT.EX
// SPACE=(CYL,(15,10),RLSE),DCB=(LRE
// UNIT=SYSDA,DISP=(MOD,CATLG,DELETE
//*
//*********************************
//* STEP 2: READ THE DB2 LOG TO GENERATE THE GENERAL REPORT           *
//*********************************************************************
//STEP2    EXEC PGM=ADHGEN1,REGION=0M,COND=(4,LT)
//STEPLIB  DD DISP=SHR,DSN=RSDEMO.ADH210.IBMTAPE.SADHLOAD
//         DD DISP=SHR,DSN=DSN.I81B.SDSNEXIT
//         DD DISP=SHR,DSN=RSRTE.DSN.V810.SDSNLOAD
//DB2PARMS DD DISP=SHR,DSN=RSTEST.ADH210.CONTROL
//MODEFILE DD   DSN=ADHSTC.ADHLAT.MODE.R0000000,
// DISP=OLD
//SYSOUT   DD   SYSOUT=*
//CFILES   DD   SYSOUT=*
//SYSPRINT DD   SYSOUT=*
//GENRPT   DD   SYSOUT=*
```

IBM Enterprise Data Governance Solutions

- *Design Create and Test*
- *Secure and Protect*
- *Retain and Decommission*
- *Monitor and Audit*

Information Management software

Data Governance for System z



Data Governance

Manage Data Lifecycle

- Data Retention
- Data Retirement

Secure

- Prevent Access
- Restrict Access
- Monitor Access

Audit

- Audit Access
- Audit Privileges
- Audit Users

Protect Privacy

- Mask Data
- Encrypt Data

Enterprise Data Governance Solutions

- Retain, Retire, Discover, Test
  - Cost-effectively manage data growth
  - Ensure inactive data is not effecting performance of the active data
  - Design requires classifying, modeling and assigning stewardship
  - Testing requires cost-effective methods to obtain realistic test data

Manage Data Lifecycle

- Optim Data Growth Solution
- Rational Data Architect
- Optim Test Data Management

- Optim Data Growth Solution
  - Lower storage costs and improve performance by separating inactive from active data in heterogeneous databases and/or packaged application environments
- Rational Data Architect
  - Enables discovery, modeling and visualization of data assets
- Optim Test Data Management
  - Produce accurate testing results using the realistic test business objects for heterogeneous databases and/or packaged application environments

Enterprise Data Governance Solutions

- Protect, Restrict, Monitor
  - Protect and secure your data and information assets
  - Apply consistent security to enable collaboration while mitigating risk

Secure

- Tivoli z/Secure Suite
- DB2/RACF Security

- Tivoli z/Secure Suite
  - Enable compliance requirements with more efficient and effective RACF administration, using significantly less resources

- DB2/ RACF Security
  - Resource level security
  - Trusted Context and Roles
  - MLS

Enterprise Data Governance Solutions

- Audit
  - Prevent unauthorized access by monitoring database activity to identify any ‘out of policy’ situations
  - Support ongoing compliance procedures or special investigations by providing audit reports

Audit
• Tivoli Compliance Insight Manager
• DB2 / IMS Audit Management Expert

- Tivoli Compliance Insight Manager
  - Enable compliance requirements with comprehensive auditing across the enterprise

- DB2 / IMS Audit Management Expert
  - Enable compliance requirements with detailed database auditing for DB2 and IMS database activity on z/Series

Enterprise Data Governance Solutions

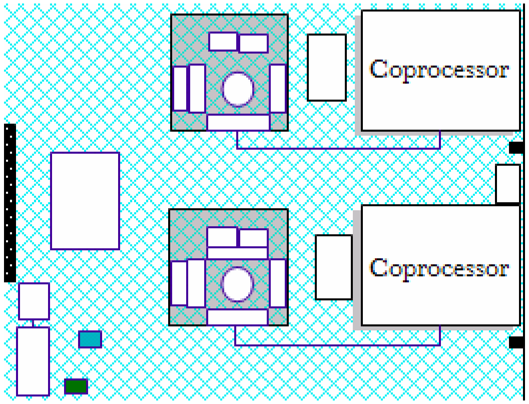
- Protect Privacy
  - Preventing unauthorized access is critical to Enterprise Data Governance
  - Privacy protection ensures confidential and sensitive data is protected regardless of how the data is obtained

Protect Privacy

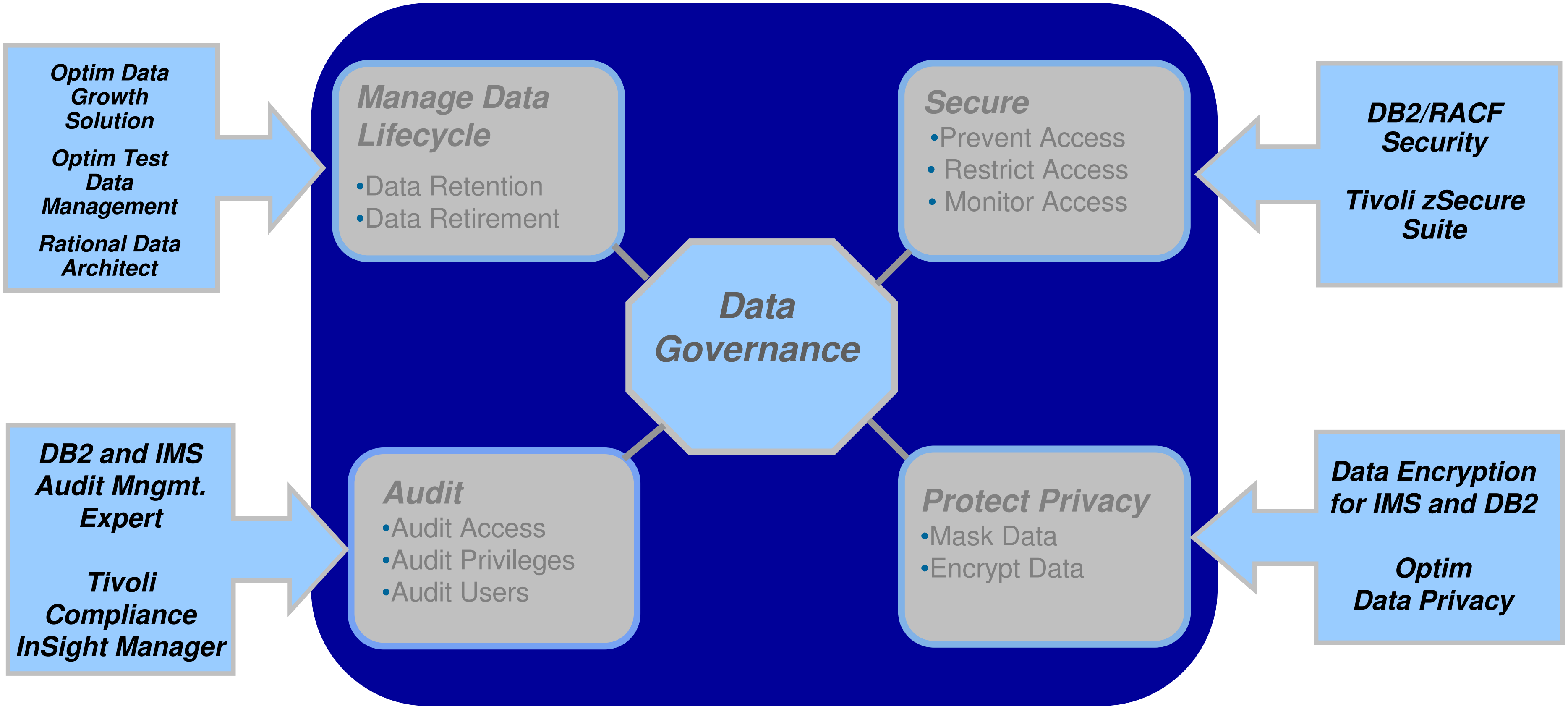
• Optim Data Privacy Solution

• IBM Encryption Tool for DB2 and IMS Databases

- Optim Data Privacy Solution
  - Reduce the liability risk of exposing sensitive or confidential test data across heterogeneous databases and/or packaged application environments
  - Masking and transformation of sensitive fields or column values with application and relationship awareness
- IBM Encryption Tool for DB2 and IMS Databases
  - Prevents theft of confidential or sensitive DB2 data
  - High performance solution leveraging latest cryptographic hardware
  - Non intrusive implementation (no application changes)



Data Governance for System z



For More Information……

Enterprise Data Management Solutions

- **Optim Data Growth Solution**
  - http://www.princetonsoftech.com/Solutions/DataGrowth.asp
- **Optim Data Privacy Solution**
  - http://www.princetonsoftech.com/Solutions/DataPrivacy.asp

DB2 Offerings

- **DB2 Audit Management Expert**
  - http://www.ibm.com/software/data/db2imstools/db2tools/db2ame/
- **IBM Data Encryption for DB2 and IMS Databases**
  - http://www.ibm.com/software/data/db2imstools/db2tools/ibmencrypt.html

Tivoli Offerings

- http://www-306.ibm.com/software/tivoli/products/zsecure/

Thank You for Joining Us today!

Go to **www.ibm.com/software/systemz** to:

- Replay this teleconference
- Replay previously broadcast teleconferences
- Register for upcoming events