



Data Auditing using DB2 Audit Management Expert for z/OS

Document version 2.0

Kelly Smith: kelly.smith@rocketsoftware.com

Barry Davis: bdavis@rocketsoftware.com

Jeremy Weatherall: jweatherall@rocketsoftware.com

Rajesh Nandwani: rnandwani@rocketsoftware.com

Susan Livingston: slivingston@rocketsoftware.com

Chris Born: cborn@rocketsoftware.com

Thomas Hubbard: thubbard@rocketsoftware.com

Mary Petras: marypetr@us.ibm.com

Thomas A. Kisielewicz: takisiel@us.ibm.com

Rita Vuong: rvuong@us.ibm.com

CONTENTS

List of Tables	v
Revision History	vi
1 Executive Summary.....	1
1.1 Auditing Today.....	2
1.2 Why Audit	3
1.3 Company Perspective.....	4
1.4 Auditor’s Perspective	5
1.5 The DBA Perspective	7
1.6 Traditional Auditing	7
1.7 Achieving Integrity through Segregation of Duties.....	8
2 DB2 Audit Management Expert for z/OS.....	8
2.1 Expertise.....	8
2.2 Centralization.....	8
2.3 Simplification.....	9
2.4 Segregation of Duties	9

2.5	Internal Security.....	9
3	Best Practices.....	10
3.1	Planning for Installation	10
3.1.1	Architecture.....	10
3.1.2	Port and host information.....	10
3.1.3	SMP/E.....	12
3.1.4	APF Library Authorization.....	12
3.1.5	Started Tasks.....	12
3.1.6	User IDs.....	12
3.1.7	Repository Database	13
3.1.8	Product Data Sets.....	14
3.2	Repository.....	15
3.3	Availability of audit data	15
3.4	Server Configuration Tips	16
3.4.1	Local Environment Settings.....	16
3.4.2	Server Collection Settings	17
3.5	Agent Configuration Tips	17
3.5.1	Local Environment Settings.....	17
3.5.2	Agent Collection Settings.....	17
3.6	Stand-Alone Utilities	18
3.7	Securing and Monitoring the Audit Data	18
3.8	Data Collection Considerations	18
3.8.1	How Audit data is Collected.....	18
3.8.2	What Data to Collect.....	19
3.8.3	Controlling Data Collection	19
3.9	DB2 Load Facility.....	20

3.10	Reporting	21
3.10.1	Filtering in the Reporting User Interface.....	21
3.10.2	Batch Reports	21
4	Administration User Interface	23
4.1	Logging in to the Administration User Interface.....	23
4.2	Add Users and Groups	24
4.3	Agents.....	24
4.3.1	Check Agent Status	25
4.4	Create a Collection Profile	26
4.4.1	Adding Rules to the Collection Profile	28
4.4.2	Determine the Collection Profile Schedule	29
4.4.3	General Audits	30
4.4.4	Select Targets.....	31
4.4.5	Events	34
4.4.6	Include or Exclude by Identity.....	34
4.4.7	Include or Exclude by Plan	36
4.4.8	Collection Profile Summary	36
4.5	Authorizations Tab.....	39
4.6	Repository Tab	39
5	Reporting User Interface	41
5.1	Logging in to the Reporting User Interface.....	41
5.2	DB2 Systems Level 1 - Overview	41
5.2.1	Add a Level 1 Filter.....	45
5.2.2	DB2 Systems Level 2 – Subsystem.....	47
5.2.3	Add a Level 3 Filter.....	49
5.2.4	LOG ANALYSIS.....	59

LIST OF TABLES

Table 1:	Government regulations that require auditing	3
Table 2:	Information required during installation	11

REVISION HISTORY

Date	Version	Revised By	Comments
6/2008	2	Kelly Smith	Updated for current release of DB2 Audit Management Expert for z/OS 2.1.

1 Executive Summary

No company wants to end up in the media with unwanted publicity about any event that can affect company integrity, resulting in the loss of stockholder or customer confidence. One way this can be avoided is through a better understanding of corporate data auditing procedures, as well as the associated fraud exposures and auditing costs.

Auditing is important, not only because it is the law, but because the integrity of your company is important. Auditing helps ensure the integrity of company data. Auditing does not generate revenue, so companies want to audit with the least expense possible while remaining in compliance. The problems with using traditional methods of auditing are many: Lack of segregation of duties between the auditors and those they may need to monitor, no centralization of the audit data from the many systems and sources a company may have; and no (or little) automation of auditing processes. These problems can result in fraud exposure and unnecessary costs.

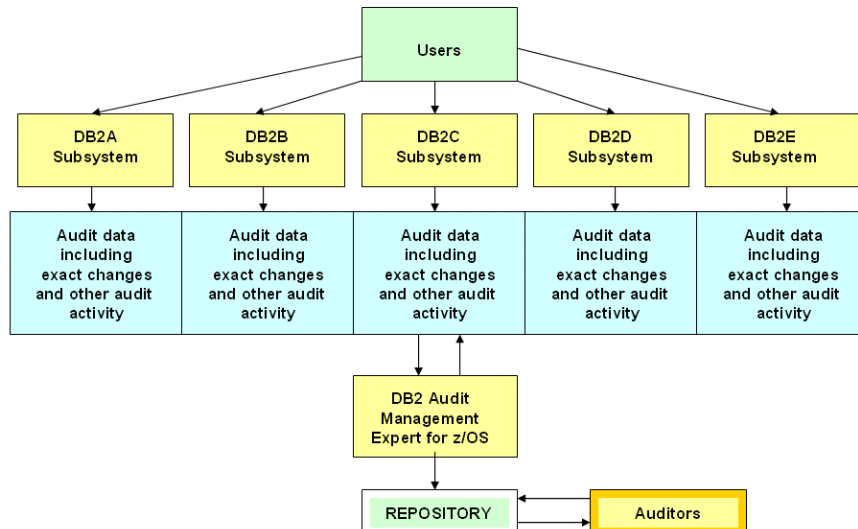
Auditors lose their independence because they need to go to other, highly technical people to get the data they require – those they may need to audit – in order to acquire the necessary information. An auditor's reliance on others not only increases costs by using these highly paid people, but also increases fraud exposure. Without a segregation of duties in this area, there is a greater possibility that the data may be manipulated before reaching the auditor.

The auditing process can be complicated by the sheer size of the data center, causing critical exposures to be overlooked. When audit data is collected from many systems and sources, the data must be combined, correlated and displayed in a clear format, providing auditors with factual and easy-to-read material.

Little or no automation results in great amounts of time spent on the auditing process, which becomes error-prone, and costly. Programs can be written to automate the collection and correlation of the audited data, but those programs need to be maintained on a regular basis. Additionally, those types of programs are specific to accessing data required at that point in time, and often conflict with the required segregation of duties between auditors and database administrators, or DB2 programmers in the case where programs are written by the same people the auditors will monitor.

Without segregation of duties, fraud is always a possibility. Without centralization and automation, a more comprehensive audit results in a higher labor cost, and a less comprehensive audit runs the risk of a company being out of compliance. The right software can greatly improve the likelihood of a successful audit and give auditors the necessary insight to answer questions about accessed data: who, what, when, where and how.

IBM's DB2 Audit Management Expert for z/OS pulls together disparate data sources from different systems into a central repository (as shown below) with a simple-to-use interface, giving auditors a complete view of the business activity collected without reliance on the technical personnel they need to monitor. Collecting data with an auditing software product enables the product repository to also be audited to provide integrity and prevent audit data tampering.



DB2 Audit Management Expert for z/OS is a comprehensive auditing solution that provides the three keys to auditing success: segregation of duties to ensure integrity; centralization of the data to be audited in order to eliminate the complexities of collecting data from many systems; and automation, to achieve more thorough audits, reduce the cost of auditing and reduce the risk of being out of compliance.

Auditors now have an automated, simple method to gain the information required to determine compliance. The easy-to-use interface gives them the tools they need to audit the data they want from one central location, filter it based on their requirements, and display data of interest using standard or custom reports.

1.1 Auditing Today

Several challenges affect auditing today. It is important to accurately collect and correlate data into useful report representations that auditors can easily use. The data must adhere to regulatory compliance regardless of the size of a company's IT department. Also, many auditors depend on developers or database administrators (DBAs) to set up or gather the information they require, despite the fact that these personnel may also need to be monitored.

These challenges raise several significant questions. How do auditors ensure that the person providing the information has not updated sensitive data or excluded it from the reports? How can auditors do a thorough job without being dependent on database personnel when there are a large number of systems to monitor? How can a company ensure the external auditor has precise, accurate information to determine if they meet all applicable regulatory compliance?

This white paper focuses specifically on data auditing, which is just one aspect of regulatory compliance. There are three levels of data auditing: ensuring business controls are in place, internal audits, and external audits. This white paper is targeted to the first two levels.

1.2 Why Audit

Your data is valuable. It has always been a good practice to perform audits as a method of maintaining checks and balances. Not only does this include auditing the quality of the data, but more importantly, who has access to the data. This was thought to ensure that no one person has the ability to maintain and manipulate information that could be considered highly sensitive and negatively impact the company's bottom line.

In recent years, there have been many publicized incidents where fraud has occurred, and in most cases, these incidents have had major financial ramifications. With the possibility of such occurrences, the government has had to intervene in an attempt to prevent repeated incidents by establishing several regulations that permeate many industries throughout corporate America. Not only is auditing a good practice, but now, in most industries, it's the law. Many countries have similar regulations, such as those regulations shown in the table below.

Some penalty examples include:

- Up to \$1 million in fines and up to ten years imprisonment for a CEO or CFO who submits a wrong certification.
- Up to \$5 million in fines and up to twenty years imprisonment for willful submission of a wrong certification.
- Removal from the exchange and lack of investor confidence

Table 1: Government regulations that require auditing

Regulation	Threat
Sarbanes-Oxley Act of 2002	<ul style="list-style-type: none"> • Act passed to prevent corporate and accounting scandals • CEO and CFO certifications of annual and quarterly SEC reports • Evaluates the effectiveness of internal controls • Requires rapid disclosure of material changes in financial conditions or operations • Set up automatic controls repository to identify deficiencies • Public Company Accounting Oversight Board is an agency that regulates auditors in public companies
Gramm-Leach-Bliley Act	<ul style="list-style-type: none"> • Act passed to legalize mergers between banking and insurance companies • Financial institutions are required to have a policy to protect information from security threats and protect data integrity • Financial Privacy Rule: requires a privacy notice from financial institutions to their customers every year • Safeguards Rule: financial institutions should have a security plan to protect their consumer's non-public personal information • Pretexting Protection: financial institutions have to protect their consumer's non-public information by preventing someone without authority from accessing the information
Health Insurance Portability and Accountability Act (HIPAA)	<ul style="list-style-type: none"> • Act passed to restrict access to patient treatment and payment information to approved personnel • Protect people when they lose their jobs or change occupation
Basel II (primarily banking)	<ul style="list-style-type: none"> • Capital requirement should be more risk-sensitive • Market discipline: people who deposit money into banks can influence the way bank managers are involved in risky activities

	<ul style="list-style-type: none"> • Help financial system in the bank become more stable
Solvency II (insurance)	<ul style="list-style-type: none"> • Help protect policyholders against the risk of a company failing • Used in insurance industry to ensure a more efficient capital allocation • Provide financial stability
Japanese Financial Instruments and Exchange Law (FIEL)	<ul style="list-style-type: none"> • Intended to protect investors • Criminal penalties increased to the maximum for market frauds • Disclosure rules applies to any investment fund that invests in securities • Corporate reorganization will require securities to be registered • Companies required to have a quarterly report • Statements in annual and quarterly report are required to be certified
Japanese Protecting personal freedom act	<ul style="list-style-type: none"> • Act passed to protect personal information, or any information that can identify an individual (name, date of birth) • A person's consent is needed before someone can access his/her personal information
Financial Services and Markets Act (FISMA)	<ul style="list-style-type: none"> • Act passed is intended to reduce financial crime • Ensures consumers are protected • Insurance, banking, or investment business need to be authorized before they can conduct regulated activities
Payment Card Industry (PCI)	<ul style="list-style-type: none"> • Regulation passed to protect someone in the event their credit card is stolen • Protect against unauthorized charges on a stolen credit card • Protects cardholder's information • Access to cardholder's information will be restricted on a business need-to-know • All access to cardholder's information and network resources will be tracked and monitored • Required to maintain information security
Patriot Act	<ul style="list-style-type: none"> • Act passed mandating publicly and privately held companies to assist law enforcement agencies in surveilling terror suspects • Provide private information on-demand, such as email and telephone communications, financial or medical records • Act passed after the USA World Trade Center attacks of 9/11/01
Various anti-money laundering (AML)	<ul style="list-style-type: none"> • Requires financial institutions to monitor, investigate and report any suspicious transactions related to money laundering or currency crimes

Within each company there are several views of auditing: the corporate view, the auditor view, and the DBA view. The essential issue, however, is how companies can achieve compliance and maintain stockholder and customer confidence in the corporation, while simultaneously ensuring that as data grows, auditing costs (which do not generate revenue) are managed appropriately, and that the auditing method ensures accurate data.

1.3 Company Perspective

Such government regulations are pressuring companies to audit the viewing and updating of data. Since auditing does not generate revenue, this is now considered part of the cost of doing business. Companies try to accomplish this with as little funding and resources as possible while remaining in compliance. This adds another layer of complexity to the overall business model.

Auditing is a key component of the overall security, compliance and risk management of any company. Audit policies need to complement the plans and policies of other business areas to reduce the risk of problems, as well as to ensure that any errors are caught as soon as possible.

A company needs to assess its organization and decide how to approach and implement the audit process. This can be done by bringing in an outside company or organizing an internal audit department to oversee the process. They will maintain control of the - *who*, *what*, *where*, *when*, and *how* of the audit controls.

The audit team needs to know who is involved in the processing of data and at what point a breakdown can occur. Most companies have these tasks covered, as specific employees are granted access to sensitive data in order to perform their job duties. The challenge arises when privileged users are involved (usually those who ultimately control the data: the systems teams, or system administrators with a high level of authority to access data) or when access controls are not well-monitored.

The data or process that will be audited will vary depending on the industry and the regulations to which it is subject. Overall, it is standard practice to have audits on any data considered personal or sensitive.

The auditing process raises many questions from a company perspective:

- What data will be audited?
- At what point in the process must checks be established?
- When will they audit? (How often is too much or too little? How much will this cost to accomplish?)
- How will they audit? Will it be done manually or in some type of automated fashion? Are there tools to help with the audit? (This is another difficult subject to address. Part of the answer lies in the industry and the regulations that pertain to that industry.)

As you can see, there is a lot to consider when it comes to auditing, an area that is sometimes overlooked since it does not generate revenue. It is nonetheless a crucial area, since thorough audits can help to prevent fraud.

1.4 Auditor's Perspective

Auditors want to know *who*, *what*, *when*, *where* and *how*. It can be difficult pulling together all the information required in an audit due to an auditor's dependence on developers or database administrators (DBAs). This dependency has drawbacks:

- Collection: Existing developer and DBA tools are not audit-oriented, nor are they designed to collect all the relevant audit information from the source.
- Reporting: Existing developer and DBA tools are not audit-oriented, nor are they designed to present information in a useful way for an audit.
- Integrity: DBAs are part of the audited population, and should therefore not be relied upon to provide key audit information. Furthermore, DBA user identifications (user IDs) have more system-level privileges than typical business users, giving them more opportunity to circumvent normal business controls.

Alternatively, auditors could collect and correlate the information themselves, but this direct approach has drawbacks:

- Privileges: Auditors generally are not granted the system privileges needed to collect the required information themselves.
- I.T. Skills: Even if auditors were given these privileges, they need substantial knowledge of information technology to collect and correlate data at an application level. Developing such skill is costly, time-consuming, and tangential to the auditor's primary role.
- Complexity: Because data can be proliferated across the enterprise, it is increasingly difficult to pull information together from "all" systems.
- Cost: A more comprehensive audit results in a higher labor cost.
- Repercussion: A less comprehensive audit runs the risk of missing important events and could allow a company to operate out of compliance.

1.5 The DBA Perspective

It is important to know the business process as well as the audit process. When audits are performed, it is also important to have the right people involved. When any audit process discusses data, there will ultimately be a discussion about the database administrators (DBAs).

The amount of DBA involvement in the auditing process varies widely. Because different industries are held to different security standards, some audit requirements can result in a substantially greater workload for both the DBA and the audit team. The workload can also be affected by the auditing process itself. For obvious reasons, the less work that is required by the DBA for the auditing process, the better for both the DBA and the auditor. However, while assisting the auditor, the DBA is aware that they too are within the scope of the audit.

Most employees in a company have pre-defined data access privileges associated with their job role. Prior to the enhanced auditing regulations, it was an accepted practice to allow DBAs and system administrator's access privileges to all data. Today, access to sensitive data is split among the DBA and system administrators. While each still has access to sensitive data, they do not have access to data that isn't within their business scope. That is, their access to sensitive data is mostly compartmentalized and each only has the appropriate access to perform their job duties. Despite how a DBA's access to sensitive data has changed with the implementation of each regulation, a DBA's role in the audit process is still required and important.

1.6 Traditional Auditing

Using traditional auditing methods, auditors require a multitude of resources: a system user ID for each system they need to collect data from; database access on each of these systems; tools to collect the data; tools to put the pieces of data together in a meaningful way, help from database administrators and DB2 system programmers, and so on. The larger the environment, the more difficult it is to coordinate these resources.

From a high-level perspective, the response is usually surprise and dismay at the cost of obtaining data during an audit, which in turn creates the motivation to reduce the cost. A company may wonder if it is necessary to spend money in order to train auditors to be nearly as experienced as database administrators when the auditor will still require the DBAs help to get the data. It all boils down to a conflict of duties between the auditor and the database administrator.

Certain concerns arise from the company's perspective. Not only are the efforts mostly manual, but how thorough can the audit be using these methods? Was something critical missed? If so, you could end up in reactive mode. The audit data is gathered after the event and could be difficult to find or unavailable.

It is understood that applications to audit data are sometimes written in-house, but that can create an exposure. It raises additional questions: Who wrote the code? Is the code maintained or even secured? Using that program, can someone manipulate audit data, and would anyone know?

Since auditing doesn't bring in revenue, companies will try to accomplish it with as little funding and resources as possible to adhere to regulations. The question is whether companies are really saving as much as they can while ensuring the integrity of the audit.

1.7 Achieving Integrity through Segregation of Duties

The key to gathering data with integrity, meaningful representations of the data, and maintaining a separation of the roles of auditor and DBA, is to automate the process with auditing software. Auditing software gives the auditors independence so they can adhere to published industry standards without relying on personnel who are also being monitored. The right software can help organizations audit more successfully, and less expensively, by providing an easy-to-use tool to access the required data.

2 DB2 Audit Management Expert for z/OS

DB2 Audit Management Expert for z/OS is a comprehensive auditing solution that centralizes auditing information, greatly simplifies access for auditors, and provides data integrity through segregation of duties on DB2, z/OS so auditors can easily find out who, what, where, when, and how. The key advantages DB2 Audit Management Expert for z/OS provides are described in the following sections.

2.1 Expertise

Auditors often must consult multiple sources because no one person has the security authorizations to access, nor knowledge about, all of the necessary data. DB2 Audit Management Expert for z/OS pulls together data from all of the disparate sources and collects it into a central repository with a simple-to-use graphical user interface, so auditors can analyze the data without relying on a DB2 systems programmer, DBA, or developer. From the auditor's perspective, it is like working with an expert DBA or a combination of a systems programmer and a DBA. If an auditor wants activity for a specific table from specific plans or users, DB2 Audit Management Expert for z/OS collects what is needed.

2.2 Centralization

DB2 Audit Management Expert for z/OS tracks, correlates, and analyzes DB2 activities using several methods and deposits audit information into a single repository to produce a complete view of this business activity for auditors.

A centralized repository creates consistency of views; a single source for reporting which is available both online and in batch; institutional controls, summarization of the data; high level trending of audit anomalies, drill-down capability -- a layer at a time; a robust level of reporting events with minimal overhead -- controlled by the auditor without DBA involvement.

As data proliferates across the enterprise, centralization is integral to reducing auditing costs and increasing productivity, creating easier and more thorough audits, thereby reducing the risk of being out of compliance.

2.3 Simplification

DB2 Audit Management Expert for z/OS reduces manual auditing and empowers non-technical users to easily audit the data without requiring logins to each system.

In a traditional environment, auditors require logins to all the systems and require authorization to access each of the DB2 subsystems. In large sites, setting up and keeping track of all of these logins can be an administrative nightmare.

Auditors using DB2 Audit Management Expert for z/OS do not need to go to a large number of sources to access data and they do not need user IDs for DB2 or the operating system. They log into one place, DB2 Audit Management Expert for z/OS, to gain complete visibility of all auditable objects. An auditor can display collected data for all DB2 subsystems, or just the images and DB2 subsystems of interest, all from the central repository. The administration user interface, usually managed by the lead auditor, provides the ability to assign auditor's access to the tool which in turn allows them access to the repository data. For these reasons, DB2 Audit Management Expert for z/OS makes auditing data much more manageable.

2.4 Segregation of Duties

Segregation of duties has always been a challenge to the auditing process. In general, auditors usually depend on developers or database administrators (DBAs) to collect and report information. As described in the Auditors Perspective section, the most critical drawback with this approach pertains to the integrity of the data provided to the auditor.

DB2 Audit Management Expert for z/OS maintains the segregation of duties, resulting in assurance of data integrity, which results in more accurate reports. This frees up DBAs to perform their own duties and allows auditors to run audit reports independently of the DBAs, resulting in easier, more accurate audits. Auditors now have the ability to adhere to published industry standards and external auditing without relying on the personnel being monitored.

The DB2 Audit Management Expert for z/OS administrator can specify how much visibility each auditor has to the auditable objects.

2.5 Internal Security

DB2 Audit Management Expert for z/OS is well-suited to enforce controls that govern DBAs, as well as to report on their activity. DBAs are trusted with sensitive data in order to do their jobs. They need to be able to maintain, copy, and recover sensitive data, as well as load and reorganize it, to name a few of their responsibilities. The continuous, automated auditing provided by DB2 Audit Management Expert for z/OS removes the opportunity to alter or even omit important data from the audit reports. Thus, an independent audit mechanism in place of personnel involvement provides assurance that reported data has not been modified. Consequently, the accuracy of data and reports is more reliable.

3 Best Practices

DB2 Audit Management Expert for z/OS 2.1 is a comprehensive auditing solution. Audit Management Expert enables companies to easily segregate duties while providing essential centralization of data and automation of the auditing processes in order to reduce fraud exposures as well as the costs associated with manual auditing methods.

The following sections focus on best practices for ease of use and utmost value.

3.1 Planning for Installation

The installation process will proceed quickly and smoothly if you have all the necessary information at hand before you begin.

3.1.1 Architecture

The audit server is a started task or batch job and the central control point for a DB2 Audit Management Expert for z/OS network. A single audit server can support data collection from multiple agents on multiple z/OS systems.

The agent is a started task or batch job and is responsible for communications in a DB2 Audit Management Expert for z/OS environment. It acts as a container to run the various collectors. One agent is required for every DB2 subsystem you wish to audit.

The Audit SQL collector (ASC) collector is a started task that is started and stopped by the agent. The ASC collector is used for collecting all reads and changes of audited objects.

Audit Management Expert provides two user interfaces:

- The administration user interface: used to set up administration items such as userids, authorizations, agent settings, repository information, collection specifications and more.
- The reporting user interface: used to display the audit data that was captured. Batch jobs are also available.

The audit repository is a DB2 database and is used to store the audit data collected by Audit Management Expert in DB2.

3.1.2 Port and Host Information

Three ports are required:

1. A port for the server to listen for the agent
2. A port for the server to listen to the clients
3. A port for the DB2 subsystem where the Audit Management Expert repository will reside

Check with your TCP/IP Administrator to help you determine which ports are available.

Table 2 can be used as a worksheet for gathering the information you will need.

Table 2: Information required during installation

	Item	Purpose	Default	My Value
For Server				
	agent-listener-port in member ADHCFGS	Same as server-port in member ADHCFGA	52521	
	client-listener-port in member ADHCFGS	Same as Admin Client's Settings: Server port	52522	
For Agent				
	Server-address in member ADHCFGA	Server host name or IP Address	none	
	server-port in member ADHCFGA	Same as agent-listener-port in member ADHCFGS	52521	
For Reporting User Interface				
	Settings: Server host	Same as server-host in member ADHCFGA	none	
	Settings: Server port	Same as client-listener-port in member ADHCFGS	52522	
For Admin User Interface				
	Settings: Server host	Same as server-host in member ADHCFGA	none	
	Settings: Server port	Same as client-listener-port in member ADHCFGS	52522	
	Repository tab: Host Name	Network address of repository's DB2 subsystem	IPADDR in DISPLAY DDF	
	Repository tab: Location	Location of repository's DB2 subsystem	Run ADHDDLL	
	Repository tab: Port	DB2 port for reporting-to-repository communication via JDBC	TCPPORT in DISPLAY DDF	

3.1.3 SMP/E

There are two FMIDs to install into the same zone:

- H35A210 DB2 Audit Management Expert for z/OS
- H25F132 FEC (acronym for IBM common code)

3.1.4 APF Library Authorization

DB2 Audit Management Expert for z/OS requires that the product LOAD and FEC LOAD Library is APF authorized and every data set is allocated to the STEPLIB.

- SADHLOAD - product LOAD library
- SFECLOAD – FEC LOAD library

3.1.5 Started Tasks

The following started tasks need to be configured:

The server is the central control point for a DB2 Audit Management Expert for z/OS network. A single audit server can support data collection from multiple agents on multiple z/OS systems.

The agent is responsible for communications in a DB2 Audit Management Expert for z/OS environment. The recommended name includes the DB2 subsystem ID (ssid). DB2 Audit Management Expert for the z/OS requires one agent per DB2 subsystem to audit.

The ASC Collector is used to collect all reads and changes and is started and stopped by the agent.

- The naming standard is ADHCssid, where ssid is the identifier of the DB2 subsystem to be monitored. The ssid also corresponds to the *agent-monitor* parameter of the agent configuration file.
- The ASC started task must contain ADHPARMS DD that points to the DB2 Audit Management Expert ASC configuration file.
- Can also be stopped by issuing the following command:

```
/P ADHCssid
```

where ssid is the identifier of the DB2 subsystem being monitored.

- ADHMSTR (the Master Address Space)
 - Starts during the initial start-up of the ASC Collector
 - Runs from IPL to IPL
 - Can be shut down for maintenance via the ADHMSTR shutdown procedure

3.1.6 User IDs

Configuration of the user IDs and authorities follow:

- The person installing the product requires SYSADM authority.
- The Server user ID requires:
 - Unix System Services access by the product User Administrator Procedures (UAP) which can be used to either create or reset the product password
 - OMVS segment in its RACF profile
 - SELECT/INSERT/UPDATE access to the repository tables
 - SYSCTRL as the primary auth ID with remote login privilege
- The Agent user ID can be the same as the Server user ID
 - Unix System Services access required by the UAP
 - OMVS segment in its RACF profile
 - BPX.SERVER access (the BPX.SERVER FACILITY class profile is not always defined)
 - SYSCTRL as the primary auth ID with remote login privilege
 - Package and plan access
 - Authority to use the dynamic LPA facility CSVDYLPA
 - Authority to submit batch jobs and run DB2 utilities
 - Authority to create DB2 Audit Management Expert for z/OS data sets and user data sets
- Reporting/JDBC user ID
 - Requires authority to SELECT, UPDATE, INSERT and DELETE
- Log Analysis
 - The user must have authority to view a table (SELECT * access) for the targeted tables
 - Authority to submit batch jobs
 - The Job card can be used in two ways:
 - Use job card specified in the agent (optional)
 - Prompt for the TSO user ID
 - The user must have one of the following authorizations to produce a Log Analysis report:
 - RECOVERDB privilege for the database
 - DBADM or DBCTRL authority for the database
 - SYSCTRL or SYSADM authority

3.1.7 Repository Database

Create the DB2 Audit Management Expert for z/OS repository database

- The DDL to create the Audit Management Expert DB2 objects is shipped to install into the IBM DB2 Tools SYSTOOLS database. An object creator schema name of SYSTOOLS is used. This is the default but can be changed.
 - If changed, the new name must be specified in the Agent and Server XML configuration file

Create objects

- Tablespace, tables, indexes and, primary key
- The default buffer pool is BP0 with no compression

Views

- The install of the repository creates views on most of the repository objects and some on the DB2 Catalog objects

ALIAS

- Create DB2 Audit Management Expert for z/OS repository ALIASes for each authid that runs the Agent, Server, or is used for the Reporting User Interface JDBC.
- Have at hand the DB2 Audit Management Expert for z/OS repository database name.
- Have at hand any USERID that submits the Agent or Server.

Run RUNSTATS after some data is collected

3.1.8 Product Data Sets

Several data sets are created for DB2 Audit Management Expert for z/OS as follows:

- The control file: a VSAM data set
 - IBM DB2 Audit Management Expert configuration information is stored in a VSAM data set referred to as the product control file. This control file is created using sample JCL shipped with Audit Management Expert.
 - If you have a single DB2 subsystem, both the agent and server can use the same control file.
 - If you have two DB2 subsystems, both subsystems can be defined in the same control file and both the server and agent can use the same control file. Alternatively, they can use separate control files (depending on whether or not you want to manage your subsystems from one control file, or have separate control files for each subsystem).
 - If the agent is located in an LPAR that does not have access to the control file that the server uses, then you must create a control file on the subsystem where the agent resides.
 - **Important:** If the IBM DB2 Log Analysis Tool is in use at your installation, you must use a separate VSAM control file for IBM DB2 Audit Management Expert for z/OS. (The product control file created for use by DB2 Audit Management Expert for z/OS cannot be shared by the Log Analysis Tool.)
- ASC collection – VSAM data sets
 - The Audit SQL Collector (ASC) collector writes data to VSAM backstore data sets that are tied together with a unique timestamp. New interval VSAM data sets are allocated on an interval basis. The interval is defined in the Administration UI.
 - The VSAM data sets are created and deleted by the ASC collector
 - Each subsystem requires the creation of its own unique set of supporting data sets
- DB2 Load Datasets – Physical Sequential data sets
 - The DB2 Audit Management Expert for z/OS Agent reads the VSAM backstore data sets created by the ASC collector, and creates physical sequential data sets that are used by the DB2 Load utility to load the audit data into the product repository.
 - The DB2 load data sets are created, used and deleted by Agent
 - The DB2 load data sets are defined and named via the Administration UI, Agents tab.
 - The DB2 subsystem ID (SSID) is appended to the high level qualifier automatically

3.2 Repository

The repository should be located in a production DB2 subsystem. Ideally, it should be separate from the monitored production subsystems and connected by fast network links. For recommendations, see section 3.7, Securing and Monitoring the Audit Data.

The repository table spaces should have regular runstats, reorgs, and backups run like any production data.

The default DDL to create the repository puts tables and indexes in Buffer Pool 0 (BP0) and should be reviewed for what is best in your environment.

Repository data can grow quickly, especially if extraneous data is captured. For this reason, it is important to establish a plan for archiving the data to be kept in order to satisfy regulatory compliance rules.

The fast-growing tables are ADHEVENT, ADHEVENT_HOSTVS and ADH_SUMMARYUPDATE. Consider using compression on these tables.

3.3 Availability of Audit Data

In general, audit data does not need to be available in real time. DB2 Audit Management Expert for z/OS populates the repository in 'near real-time' as the actions occur and are being captured. It is not possible to capture the data and populate the repository during an off-peak shift. Depending on how often you want to view the audit data, DB2 Audit Management Expert for z/OS parameters can be used to define how often to update the DB2 Audit Management Expert for z/OS repository.

The raw DB2 audit data is loaded into data sets and memory where events will accumulate before being loaded into the DB2 Audit Management Expert for z/OS repository. These events are periodically loaded into the normalized audit data repository tables using DB2 LOAD. The frequency with which the events are loaded into the audit repository is controlled by Agent settings shown below. The following agent settings can be found in the Administration User Interface; Agents Tab under General Settings.

- Event Count – available in the 'Memory' section. Represents the number of audit events that will be accumulated before they are loaded into the repository tables. The value of the Event count can vary from 10 seconds to 10000 seconds (166.7 minutes) with a default value of 2507 (42 minutes). Values of 20 seconds or lower should only be used for diagnostic purposes. Recommended setting for use during product evaluations are shown in the Agent Configuration Tips section of this white paper.
- ASC Data Manager Interval – available in the 'Time' section. Represents the time between reads of the ASC data files, when newly accumulated events are loaded into the agent. The value can vary from 300 seconds (5 minutes) to a maximum value of 1800 seconds (30 minutes) with a default value of 675 seconds (11.25 minutes). Recommended setting for use during product evaluations are shown in the Agent Configuration Tips section of this white paper.
- Static SQL collection interval – available in the 'Time' section. Represents the time (in seconds) between collections of static SQL from the DB2 catalog. The ASC collector returns the package and section number, used by the agent to retrieve the static SQL text from the DB2 catalog. Audit events will be loaded into the Audit

Data Repository. The static SQL text will be loaded by the next run of the Static SQL collector, which can vary from 600 seconds (10 minutes) to a maximum value of 1800 seconds (30 minutes) with a default value of 900 seconds (15 minutes).

- Event Timeout - The maximum amount of time (in seconds) that an event is expected to take being processed by the agent. The total time from an event taking place in the monitored database until it appears in the audit repository is slightly greater than the sum of the ASC Data manager Interval and the Event Timeout. This time can vary from 60 seconds (1 minute) to a maximum value of 3600 seconds (60 minutes) with a default value of 945 seconds (15.75 minutes).

For more information, see the (Configuring the Agent section of the DB2 Audit Management Expert for z/OS user's guide.)

At periodic intervals, the server configuration parameter, `summarizer-refresh-interval`, is used by the server to read selected audit data from the repository. It condenses the audit data into a summary table, which is stored in the audit repository. This enables the reporting user interface to display high-level statistics without having to read the entire set of audit data. Some metrics are commonly reported, so putting those metrics into the summary table makes them available without the user having to explicitly request them.

The summary table includes Access Attempts, Reads, Changes, Create, Alter and Drop, Explicit Grant and Revoke, and Assignment or change of authorization ID, IBM utility access, DB2 commands, and other authorization failures.

This data is grouped by hour, day, week, month, successes, failures, AUTHIDs, or plans. For product evaluations, summary data may need to be available sooner. Recommended settings for product evaluations are shown in "Server Configuration Tips", section 3.4 of this white paper.

3.4 Server Configuration Tips

This section contains recommendations for the server configuration settings. These settings primarily define the z/OS DB2 subsystem, TCPIP ports, and how often data is summarized. These thresholds can be set much lower during product evaluations to allow the data to propagate to the reporting user interface much faster.

3.4.1 Local Environment Settings

The server configuration file needs to be updated to reflect the machine's environment. The agent- and client-listener ports may need to be changed to use available TCPIP port numbers. The repository location is the DB2 subsystem.

```
<client-listener-port>52522</client-listener-port>  
<agent-listener-port>52521</agent-listener-port>  
<server-repository>Q91J</server-repository>
```

3.4.2 Server Collection Settings

By default, the summary table will be populated every 30 minutes (1800 seconds). If you are evaluating the product and want to see the data sooner, the time interval for refreshing the summary table should be decreased to 300 seconds (5 minutes) to allow data to display in the reporting user interface much faster.

```
<summarizer-refresh-interval>300</summarizer-refresh-interval>
```

3.5 Agent Configuration Tips

This section contains recommendations for the Agent configuration settings. These settings primarily apply to how often data is written to the repository. If you are evaluating the product and want to see the data sooner, these settings need to be set much lower to allow the data to propagate to the reporting user interface faster.

3.5.1 Local Environment Settings

The agent configuration file needs to be updated to reflect the machine's environment.

- The server-port in the agent configuration file needs to match the port number specified by the parameter 'agent-listener-port' in the server configuration file, as shown below. The parameter 'server-address' is the system name or IP address for the machine where the server is located.

The server configuration file:

```
<client-listener-port>52522</client-listener-port>  
<agent-listener-port>52521</agent-listener-port>  
<server-repository>Q91J</server-repository>
```

The agent configuration file:

```
<server-address>rs25.companyname.com</server-address>  
<server-port>52521</server-port>  
<agent-monitor>Q91J</agent-monitor>  
<server-repository>Q91J</server-repository>
```

- The parameter 'agent-monitor' specifies the name of the monitored subsystem.

3.5.2 Agent Collection Settings

The default settings for the agent and server assume a "real" workload, and it may take over 30 minutes for collected data to show up in the repository. If you are evaluating the product and want the data to show up sooner, the agent Event Count, ASC Data Manager Interval, and Static SQL collection interval should be decreased to a low number to allow data to display in the reporting user interface much faster.

Decrease the Event Count to 20, ASC Data Manager Interval to 300 (seconds), and the Static SQL collection interval to 600 (seconds) during the evaluation to decrease the latency before the audit data displays.

3.6 Stand-Alone Utilities

The DB2 audit trace does not provide detailed information on utilities. In general, utilities just show the type of utility and who ran it, not what it was against. Utilities should be restricted and subject to well-defined controls.

To track vendor utilities, add the vendor utility table to the list of tables being audited.

3.7 Securing and Monitoring the Audit Data

The auditor must have confidence that the audit data in the repository accurately reflects the audited subsystems and has not been tampered with.

Ideally, the DB2 subsystem containing the repository should only contain the AME repository to tightly control access by privileged users. This method helps ensure that the AME repository that holds the collected audit data has not been tampered with and provides segregation of duties. The installer should have initial access to set up AME and that authority should be revoked thereafter and only granted when access is needed.

In addition, the DB2 Audit Management Expert repository should be audited to ensure no one with authority has manipulated any audit data. Create a collection profile that monitors repository table activity by any user ID other than server and agent. **Caution:** monitoring sever and agent User IDs is recursive and will cause the repository to grow without limit.

The server, agents, and JDBC need different authorities. Use a separate user ID for each. Give as little authority as possible to each necessary user ID.

- Server: See SAMPLIB members ADHGRTS (repository tables), ADHGRTPS (packages) and ADHGRTQS (plans)
- Agents: See SAMPLIB members ADHGRTA (repository tables) and ADHGRTQA (plans)
- Reporting user interface (JDBC): See SAMPLIB member ADHGRTR (repository tables)

Do not give these user IDs additional authorities.

3.8 Data Collection Considerations

3.8.1 How Audit Data is Collected

DB2 Audit Management Expert for z/OS collects audit data using a proprietary SQL collector, the DB2 Instrumental Facility Interface (IFI), and a log analysis facility.

- The proprietary Audit SQL collector (ASC) captures all SELECTS (reads) and all changes (UPDATE, INSERT, DELETE), dynamic and static SQL text and host variables for each statement, and row count that SQL affects for DB2 tables.
- The IFI collector captures DDL: CREATE, ALTER(DB2 V9), DROP (audit flag is required), authorization failures, grants and revokes, AUTHID changes, as well as command and utility executions in DB2 systems for DB2 tables.
- The log analysis facility captures before and after images for updates, after images for inserts, and before images for deletes to rows in an audited table (on demand).

The proprietary Audit SQL collector uses a collector developed in IBM's DB2 Query Monitor for z/OS. It is not necessary to have Query Monitor, but if you do, Query Monitor and the ASC component of DB2 Audit Management Expert for z/OS will use a shared master address space (shared collector) so that when both are running, the data is only collected once. If Query Monitor is not running, the DB2 Audit Management Expert ASC component starts the master address space. If the DB2 Audit Management Expert ASC component finds the master address space, it uses the master address space started by Query Monitor instead. If using both products, the overhead is significantly reduced by using the shared address space.

3.8.2 What Data to Collect

A DB2 subsystem can process a huge amount of data. If DB2 Audit Management Expert for z/OS were configured to capture all of that activity, it would incur unnecessary overhead, require a huge repository, and most likely, not all of the captured activity would be useful.

It is essential to audit only data of interest, such as any data that is sensitive in nature and requires auditing. These are the activities that are truly useful to an auditor.

Audit data collection enables you to audit table access for everything listed below. (Flexibility options allow you to collect all, or focus on one area, such as change of authorization or updates.)

- All SELECTS (reads)
- All changes (UPDATE, INSERT, DELETE)
- CREATE, ALTER, DROP (first in UOW)
- Explicit GRANT and REVOKE operations
- IBM utility access
- Vendor utilities when the utility table is added to the list of tables being audited
- DB2 commands entered
- Before and After images of changes (UPDATE), after images of INSERT, and before images of DELETE) to tables
- Dynamic and Static SQL text for each statement and row count that SQL statement affects
- Host variable value for each statement and row count that SQL statement affects
- Assignment or modification of an authorization ID
- Authorization failures

Audit Management Expert gives auditors a centralized repository with the information they require about who performed what activity, as well as where, when, and how it was performed. Auditors can find out who read sensitive databases, who updated sensitive databases, and even see the before and after images so they know what was changed.

3.8.3 Controlling Data Collection

Filtering capability is available on both the collection side (before the data has been written to the repository), and on the reporting side (after the data has been collected and stored in the repository). It is wise to filter on the collection side instead of the reporting side to ensure that unnecessary data is not written to the repository.

Collection filters to reduce the audit data to a useful subset

The DB2 Audit Management Expert for z/OS administrator controls the amount of data collected and stored in its audit repository using a collection profile. With this collection profile you can collect a subset of the audit activity by filtering for any of the following:

- Time
- General Audits – All failed authorizations, successful and failed authid changes, grants and revokes, IBM DB2 utilities, DB2 commands
- Reads
- Changes
- AUTHIDs
- Tables
- Plans
- WorkstationName
- WorkstationTrans

Use of Includes and/or Excludes

A major performance advantage of DB2 Audit Management Expert for z/OS is its ability to include and exclude data in a collection profile. For example, if we are sure that package A accesses table B securely, we may want to exclude that plan from the collection profile. The input/output (I/O) to the repository will be correspondingly reduced, and the overall performance of DB2 AME for z/OS improved. Consider when there are a million accesses and a large number of includes and/or excludes – in this case, saving the I/O to the repository is highly beneficial.

Including and excluding will increase CPU usage slightly, but from initial performance tests, the CPU usage of the DB2 AME agent was a small percentage of the total processing. Ultimately, it is more efficient to use CPU filtering to exclude an unwanted event instead of inserting it into the repository.

3.9 DB2 Load Facility

DB2 Audit Management Expert for z/OS reads the VSAM backstore data sets created by the ASC collector, and creates physical sequential data sets that are used by the DB2 Load utility to load the audit data into the product repository. The DB2 load data sets are created, used, and deleted by the Agent. In the event of a DB2 Load failure, the agent attempts to resubmit the job up to the retry count. If the retry count is reached and the job has still not completed, the agent terminates and operator intervention is required.

To reduce DB2 Load failures:

- Double check the DB2 Load job card found in the Administration User Interface within the Agent Editor, JCL panel for accuracy.
- Ensure the repository has enough space available to load the audit data
- Ensure the DB2 system is configured correctly

The DB2 Load facility can be set by using the Agent Editor within the Administration User Interface. The Agent Editor provides the ability to set several parameters for the DB2 Load facility, such as:

- **LS retention count** – set the number of generations of files from the DB2LOAD process to keep on disk
- **Dataset HLQ** - set the DB2LOAD data set high-level qualifier(HLQ).**Note:** It is recommended that the installation's security software product (i.e. RACF or

equivalent) be configured so that all data sets created using this HLQ are protected against unauthorized access.

- **Space allocation parameters and SMS class settings** – ensure these are set correctly.
- **Job Retry Count** - set the maximum number of times to submit a DB2LOAD job that has failed.
- **Job Retry Wait**—set the amount of time to wait (in seconds) before retrying a DB2LOAD job that has failed.
- **DB2LOAD JCL JOB Card** - specify the JOB Card for the DB2LOAD submitted jobs.

3.10 Reporting

3.10.1 Filtering in the Reporting User Interface

Data that has been collected and stored in the repository can be filtered using the Reporting User Interface. The auditor can view a subset of the collected data by filtering on any of the following:

- Time
- Authid
- PLANS
- Objects: Table/tablespace
- Event type (Authorizations/AuthidChanges/Grants/Revokes/Utilities/DB2 Commands)
- Object (reads/changes)
- Subsystem
- Connections
 - Type: Batch, TSO, DB2, Server, Utility, etc.
 - Network IP
 - Requester location
- WorkstationName
- WorkstationTrans

3.10.2 Batch Reports

There are six batch reports that can be used to display data of interest. Reports can be run for a specific day or date range. This enables a report to be produced weekly, for example, by either running the batch report manually, or automating the process through the system scheduler. The following reports are available:

- TABLES - Objects Referenced by User
- UTILITIES - Utilities Used By User
- TABUTILS - Utilities and Objects Referenced By User
- AUTHATTEMPT - Authorization / Changes By User
- AUTHFAIL - Authorization Failures By User
- AUTHALL - All Authorization Attempts By User

This white paper will show the example of monitoring two SYSADM users, CSKELL and CSREGG and their activity against sensitive tables, CREDIT_AUTH_SYS.CSCART and PRDA01.CSAUD1. For this specific batch report, the auditor is attempting to find out what actions the user “CSKELL” is taking against sensitive table “PRDA01.CSAUD1”.

The batch report produced is 134 bytes wide.

```
//RUN          EXEC PGM=ADH@REP ,
// PARM='Q91J'
//STEPLIB DD DISP=SHR,DSN=RSQA.ADH210.IBMTAPE.SADHLOAD
//          DD DISP=SHR,DSN=DSN.V910.SDSNLOAD
//ADHPARMS DD DISP=SHR,DSN=RSQA.ADH210.RS25Q91J.CONTROL
//ADHREPRT DD   SYSOUT=*
//ADHPRINT DD   SYSOUT=*
//SYSUDUMP DD   SYSOUT=*
//ADHCFG DD     *
STARTDATE "2008-05-01"
ENDDATE "2008-05-01"
REPORT TABLES
USERID CSKELL
OWNERNAME PRDA01
OBJECTNAME CSAUD1
```

Only a partial report is shown below. This report shows that an update was made by SYSADM user CSKELL for schema/table PRDA01.CSAUD1, and updated in batch. To find out more information, run the log analysis feature of DB2 Audit Management Expert for z/OS to find out what specifically was changed. This will allow you to view before and after images of the table. An example of a log analysis report is provided in section 5.2.4 of this white paper, under the Reporting user interface.

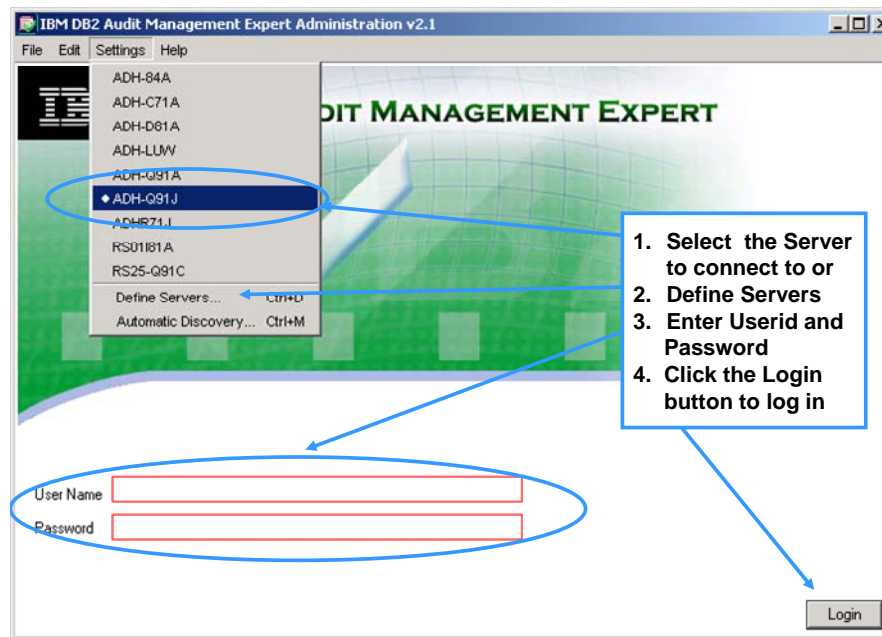
DB2 Audit Management Expert
Objects Referenced By User

Event Type	Context Type	Event Timestamp	Correlation Id					
00143	TABLE UPDATE	2008-05-01	-13.45.00.539091 0					
User Id	Original Op Id	End User Id	End User Trans Name	End User Workstation Name				
CSKELL	CSKELL	N/A	N/A	N/A				
Container	Schema Name	Object Name	Object Type	Database Id				
CSAUD1##	PRDA01	CSAUD1	TABLE/VIEW	CSKELLD				
Source Database	Application Id	Application Nm	Subsystem	Connection	CorrelationId	Server Name		
N/A	N/A	N/A	Q91J	BATCH	CSKELLUP	N/A	N/A	CSKELL
Schema	Name	Plan						
PDBATE	DSN@EP2L	DSNTEP9						

4 Administration User Interface

There are many tasks that can be accomplished with the DB2 Audit Management Expert Administration for z/OS User Interface. This section walks you through a scenario that monitors the activities of two SYSADM users, CSREGG, and CSKELL, against sensitive tables, PRDA01.CSAUD1 and CREDIT_AUTH_SYS.CSCART.

4.1 Logging in to the Administration User Interface



4.2 Add Users and Groups

DB2 Audit Management Expert for z/OS Administration user interface provides the ability to create users, assign permissions to users, edit users, clone (copy) users, and delete users. Users and groups are created in and used by DB2 Audit Management Expert for z/OS and are different from TSO user IDs (e.g. CSREGG and CSKELL). The process of adding Users and Groups is not demonstrated in this white paper; see the DB2 Audit Management Expert for z/OS User's Guide for more information.

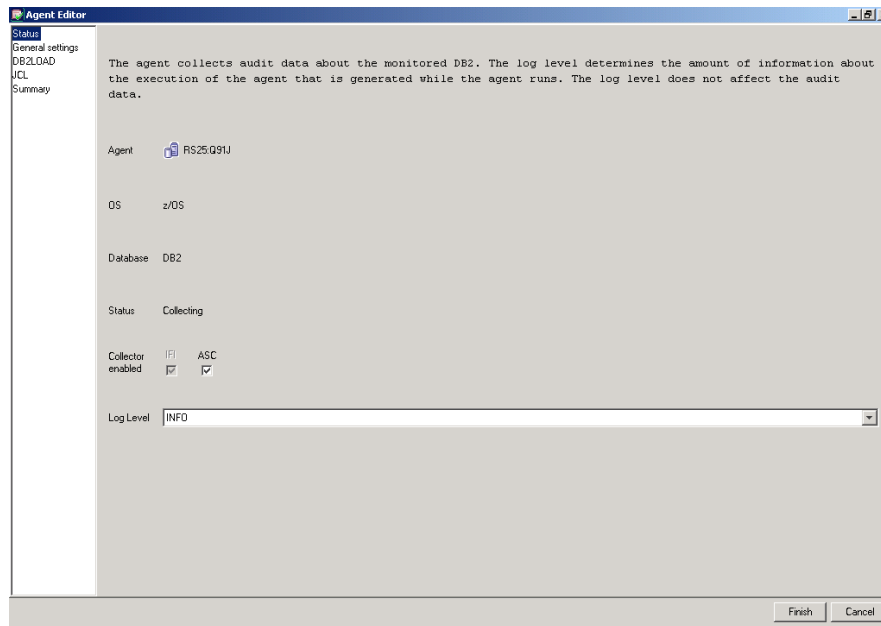
4.3 Agents

The Agents tab is critical to the collection and success of DB2 Audit Management Expert for z/OS. On the left hand side of the screen, it contains tabs for agent **Status**, as well as the following tab options:

The **General settings** tab controls both memory (how much memory is used by the agent) and latency (how often data is written to the AME repository). See sections 3.3 Availability of Audit Data, and 3.5 Agent Collection Settings for more information.

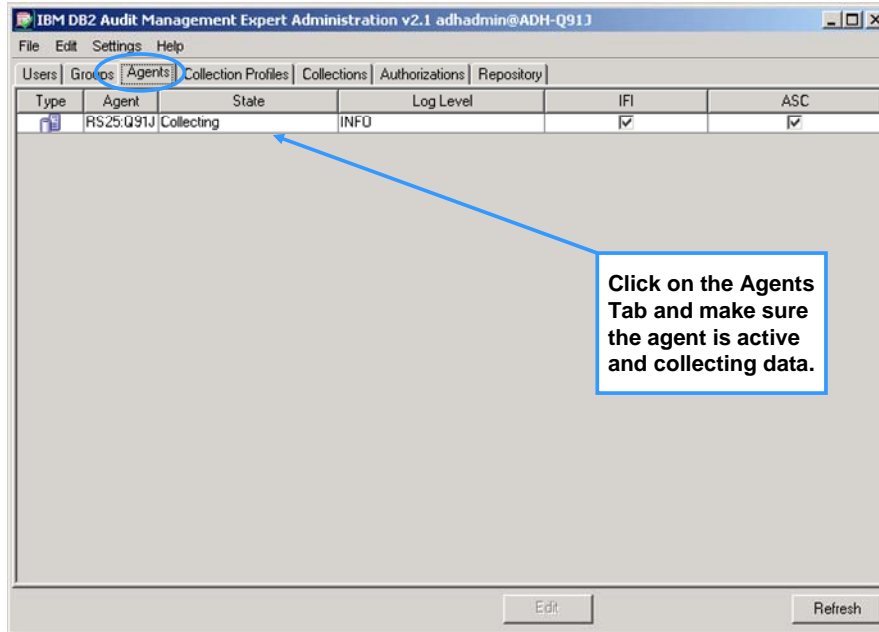
The **DB2LOAD** tab allows the high level qualifier of the DB2 Load files to be entered, and contains the space allocation parameters and SMS class settings, as well as other setting options. See section 3.9 DB2 Load Facility for more information.

The **JCL** tab allows job cards to be entered, for use with Log Analysis (optional), and DB2 Load (required).



4.3.1 Check Agent Status

Check the agent status by selecting the 'Agents' tab. If the agent status is not in the collecting state, make sure that the agent configuration file is properly set up and that the agent has been started. Also, check the agent log file to make sure that no errors have occurred after startup. For more information on properly configuring the agent configuration file and diagnosing the agent log file, please refer to the DB2 Audit Management Expert for z/OS User's Guide.



4.4 Create a Collection Profile

The collection profile in this example monitors the activities of two SYSADM users, CSREGG and CSKELL, against sensitive tables PRDA01.CSAUD1 and CREDIT_AUTH_SYS.CSCART. In the Administration UI, click on the 'Collection Profiles' tab (captured below) and click, Add.

IBM DB2 Audit Management Expert Administration v2.1 adhadmin@ADH-Q91J

File Edit Settings Help

Users Groups Agents **Collection Profiles** Collections Authorizations Repository

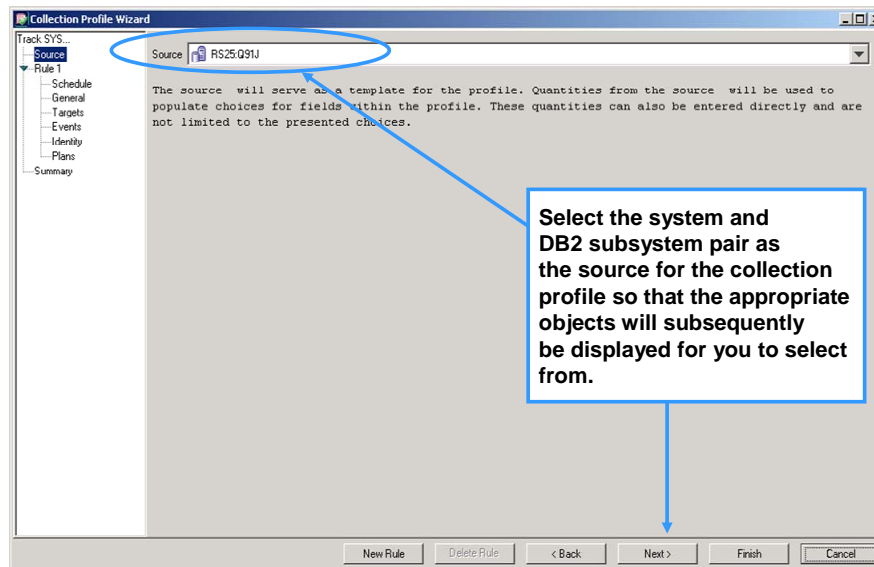
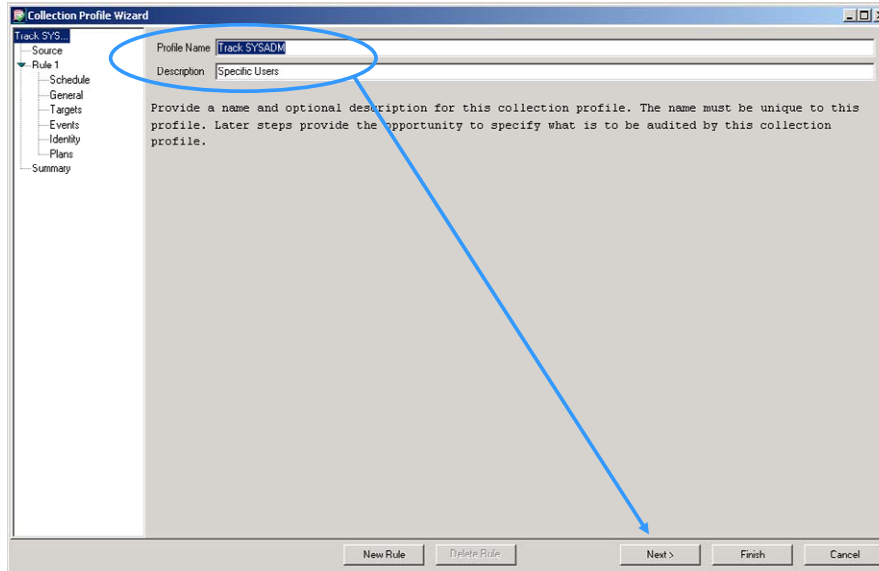
Profile Name	Description	Last Modified	Rules	Active Collections
DB2Stress1000	for stress testing	2008-04-18 07:46:22	1	0
GainTest		2008-04-21 02:45:04	1	0
ProfZTest01		2008-04-18 03:00:33	1	0
ProfZTest02		2008-04-18 03:01:13	1	0
ProfZTest03		2008-04-18 03:01:53	1	0
ProfZTest04		2008-04-18 03:02:36	1	0
ProfZTest05		2008-04-18 03:03:31	2	0
ProfZTest06		2008-04-18 03:04:25	2	0
ProfZTest07		2008-04-18 03:05:58	1	0
ProfZTest08		2008-04-18 03:08:42	2	0
ProfZTest09		2008-04-18 03:11:25	2	0
ProfZTest10		2008-04-18 03:12:35	1	0
ProfZTest11		2008-04-18 03:14:33	2	0
ProfZTest12		2008-04-18 03:16:32	2	0
ProfZTest13		2008-04-18 03:18:07	1	0
ProfZTest14		2008-04-18 03:20:58	2	0
ProfZTest15		2008-04-18 03:22:55	1	0
ProfZTest16		2008-04-18 03:25:47	2	0
ProfZTest17		2008-04-18 03:27:46	1	0
ProfZTest18		2008-04-18 03:30:14	2	0
ProfZTest19		2008-04-18 03:31:27	1	0
Q91J_Profile1	test BK64319	2008-04-17 17:05:38	2	0
SLStress1	for stress testing	2008-04-18 17:25:02	1	0

1. Add a collection profile by selecting the Collection Profiles tab

2. Click the Add button

Add Edit Clone Delete Refresh

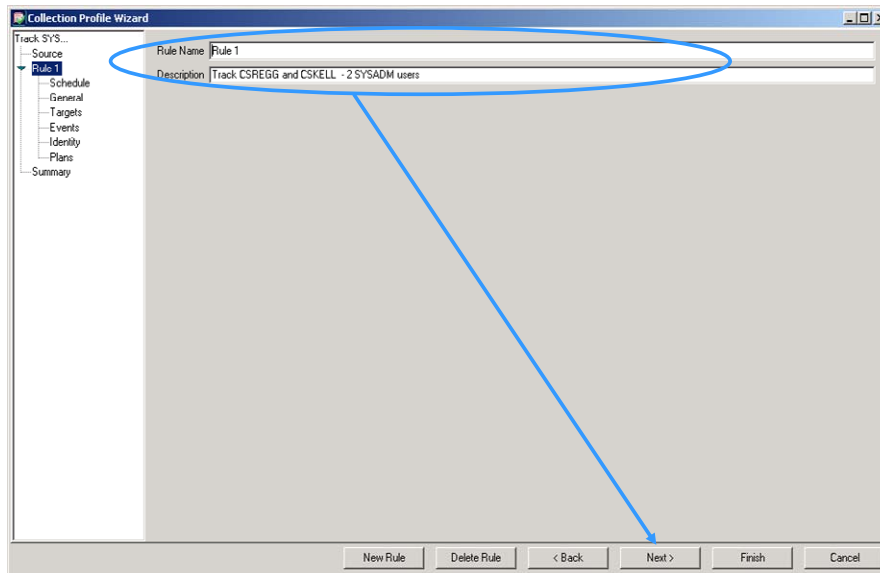
Specify a profile name and add a meaningful description, as shown below. In this example, a profile name of "Track SYSADM" has been specified. The 'Next>' button takes you through each screen.



4.4.1 Adding Rules to the Collection Profile

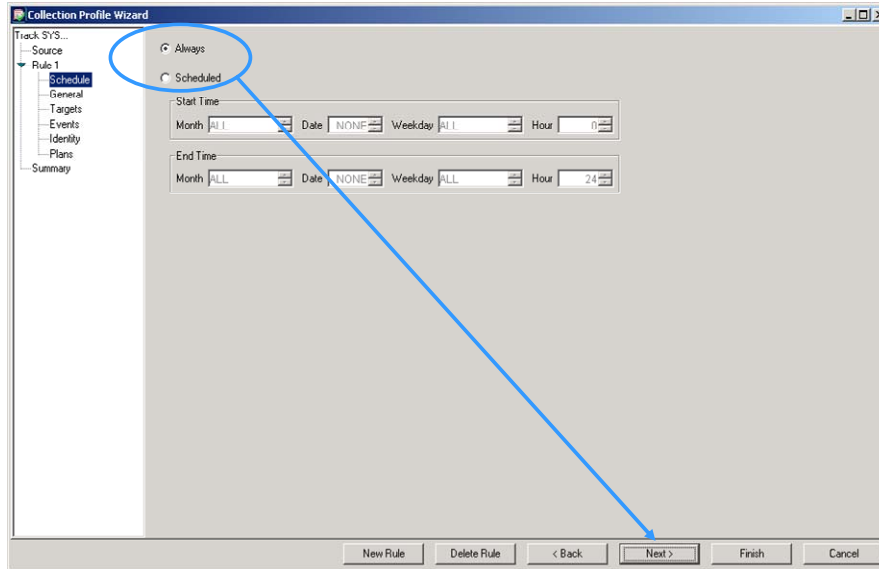
The rules determine how DB2 Audit Management Expert for z/OS performs auditing. Rules are simply criteria on which the DB2 data will be collected. One or more rules comprise a collection profile. Only one collection profile can be active at a time, so you may have one collection profile with many rules.

The sub-classifications under Rule1 (in the tree view on the left hand side of the screen capture below) represent subsequent panels containing parameters that need to be defined. The 'Next>' button takes you through each screen. Adding another rule is described in section 4.4.8. Enter a rule name, provide a description, and then click next.



4.4.2 Determine the Collection Profile Schedule

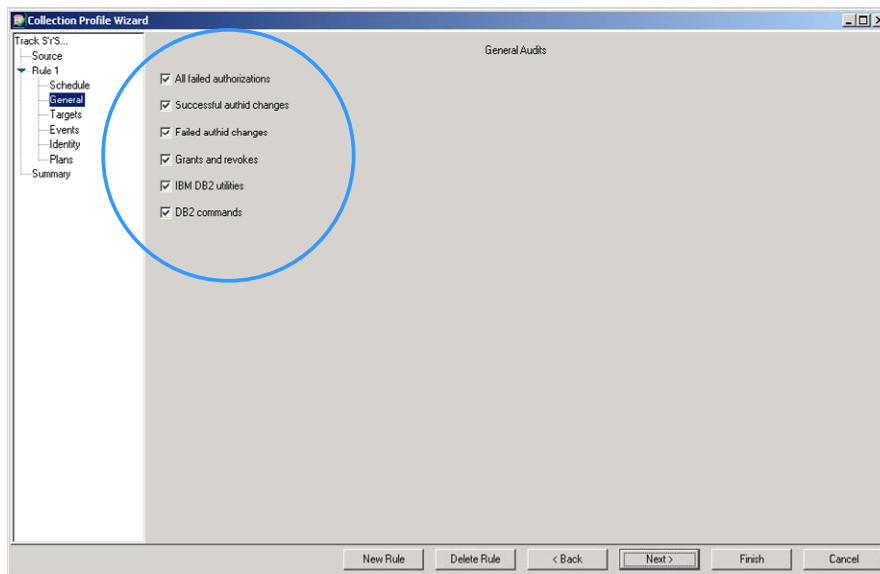
A schedule within a collection profile is a time-frame within which audit data should be collected for the monitored DB2 activity. Determine the collection profile schedule and click Next.



4.4.3 General Audits

The General Audits screen contains items that can potentially be audited, for example, you may want to collect data for all users across the entire subsystem for actions such as Authorization Failures, Connect Failures, etc. When you select an item in General Audits, it will be collected for all users.

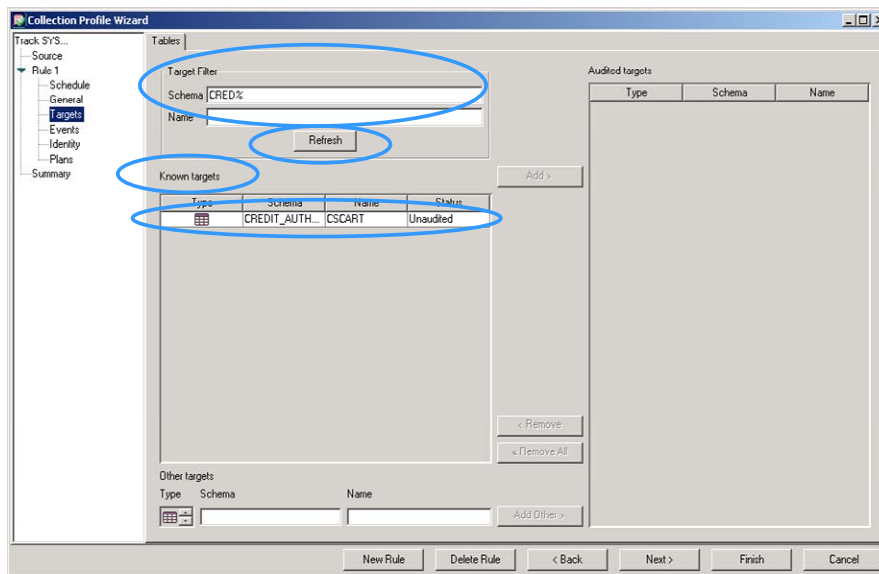
This example shows collection of data for users CSREGG and CSKELL. If the General Audits items are not selected, they will not be collected for users CSREGG and CSKELL either. Further ahead on the Identity screen (see section 4.4.6), we will be given the opportunity to refine the current audit rule to filter audited events based on selected users, in our case CSREGG and CSKELL.. After filling out the General Audits panel, click 'Next>'.



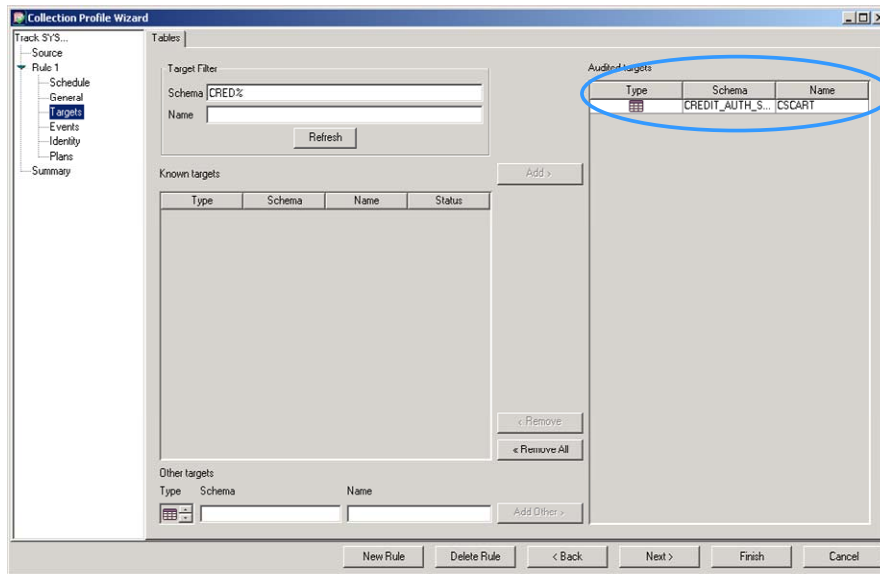
4.4.4 Select Targets

DB2 Audit Management Expert for z/OS allows you to select audited targets from a list of available tables within the source DB2 subsystem. Targets are simply the individual tables within the databases in the specified subsystem you wish to audit. Targets from multiple schemas can be added to a rule by selecting a table(s), adding the table(s) to the list of Audited Targets, and repeating the process for another schema.

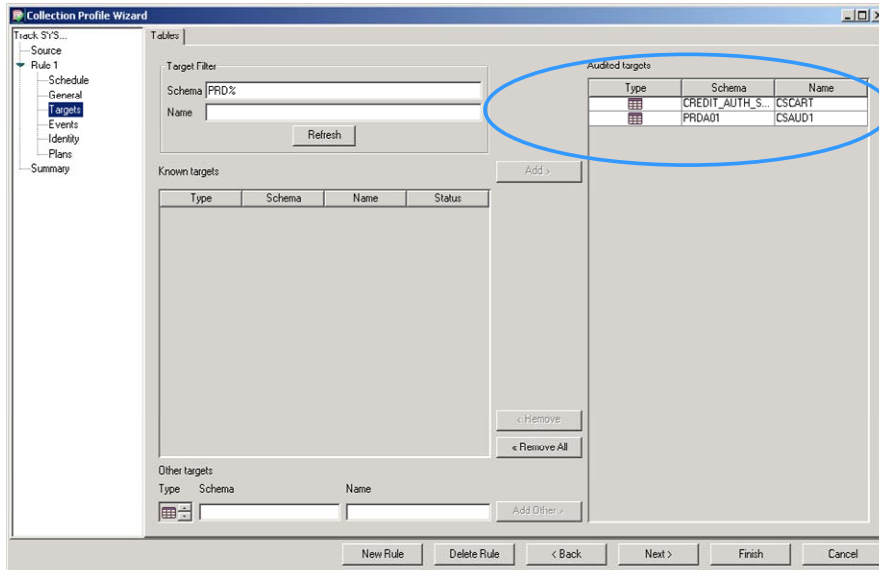
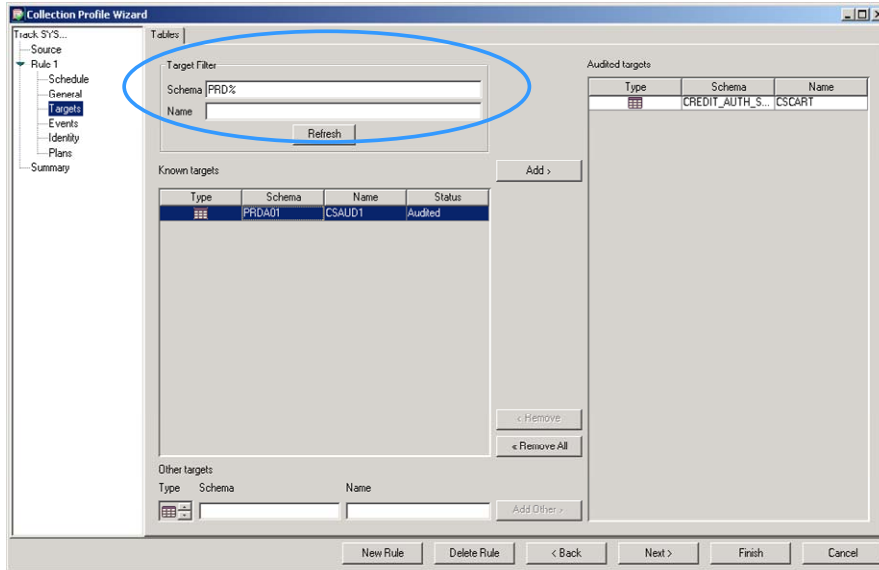
In the example below, a partial schema name of CRED% is entered followed by the % to indicate a mask. Click 'Refresh' to display the matching schemas. The 'Name' field (below the 'Schema' name) represents a table name. To monitor all tables for a particular schema, leave the 'Name' field blank. Highlight the row with the desired schema / table name and click the 'Add' button in the middle of the screen. It is grayed out in this example because the line with the schema / table name has not yet been selected.



The selected table within the specified schema has been added to the Audited Targets list.

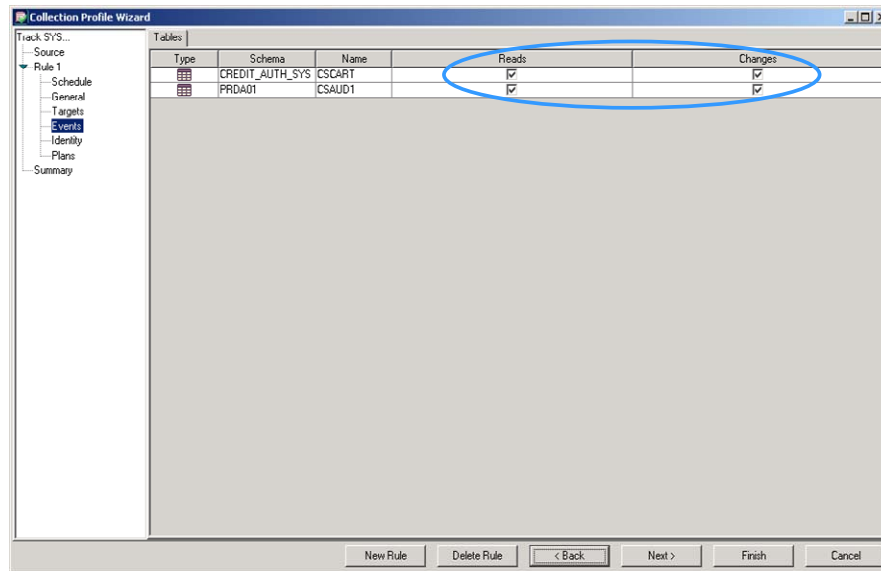


If you have another target that you want to add to this rule, type in the schema or table name and click 'Refresh'. Then highlight the desired row within the 'Known Targets' list, and click the 'Add' button.



4.4.5 Events

Below you will see that both sensitive tables described earlier have been added. To track reads and changes for the specified SYSADM users, check both boxes. Reads and Changes are captured using the ASC Collector. If these boxes are checked, and the audit trace (IFI) has been enabled, then CREATE, ALTER, and DROPS are also captured if the ALTER AUDIT ALL has been issued for the audited tables (one exception, ALTERS are only collected for DB2 V9). If Reads and Changes are captured through the ASC Collector, they will not be collected by the IFI. If reads and changes are not checked, CREATE, ALTER, and DROPS are not captured either.



4.4.6 Include or Exclude by Identity

A collection profile can be set up to include (monitor) or exclude events for specific user (AuthIDs), by a specific workstation user ID (WSNAME), or those associated with a specific workstation transaction (WSTran).

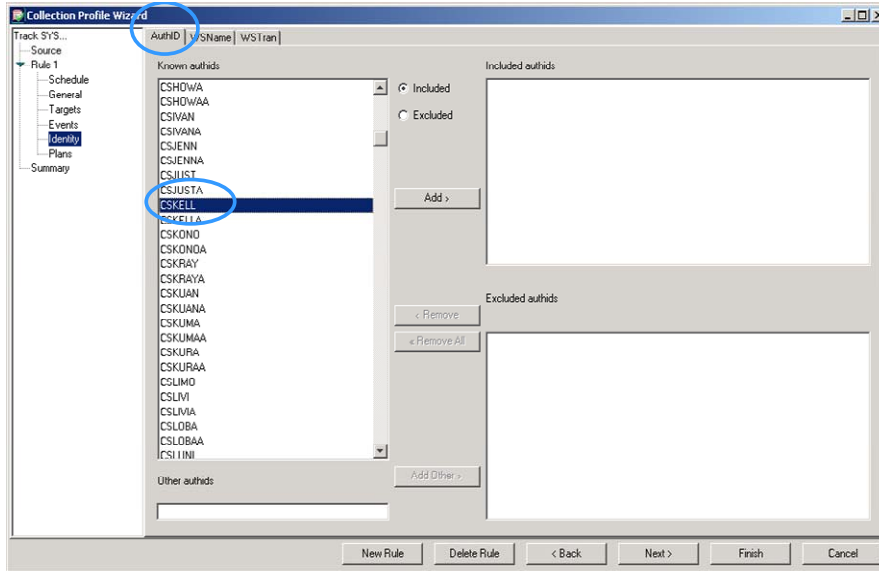
If you do not select any events to be included or excluded, the default is to collect for all AuthIDs, workstations, and workstation transactions. However, it should be noted that if, for example, you include one specific AuthID, then only data for that AuthID is collected and any others are implicitly excluded.

Warning: If you audit the repository tables, you should not monitor transactions for the user IDs running the agent and server. Monitoring sever and agent User IDs is recursive and will cause the repository to grow without limit.

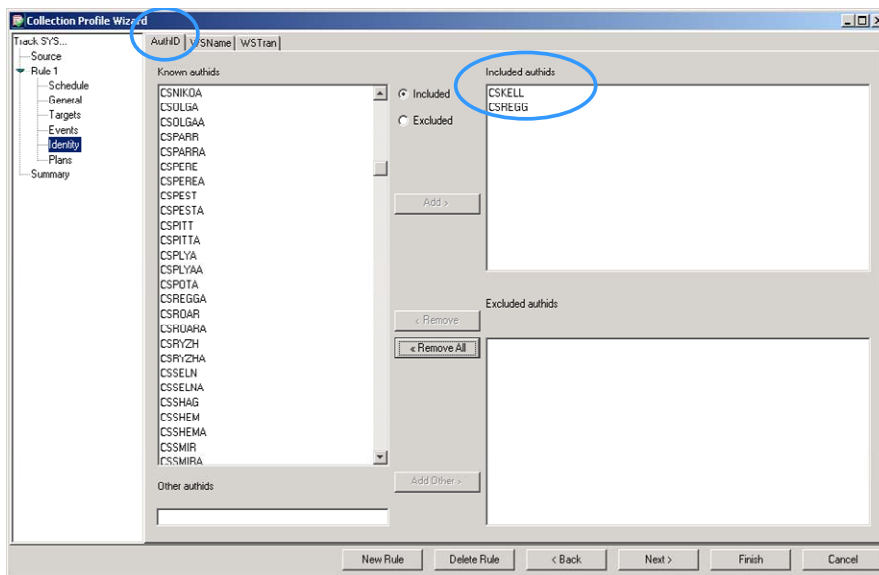
The data used to populate the lists of AuthIDs is retrieved from the SYSIBM.SYSUSERAUTH table and includes all users. The data used to populate the lists of workstations, and workstation transactions comes from audit data already collected by DB2 Audit Management Expert for z/OS. The first time you create a collection profile there

will be no data in the repository, so these lists will be empty. If you wish to include or exclude a specific name, type it in the 'other' text field at the bottom of the screen and click 'Add Other'.

The following screen shot shows all known Authid's for DB2 subsystem Q19. This example demonstrates a request to audit privileged (SYSADM) users, CSKELL and CSREGG. To audit these specific users, highlight the user and click 'Add' shown in the middle column of the screen to the right of the highlighted CSKELL.



These users are now shown in the 'Included authids' list. Click 'Finish'.

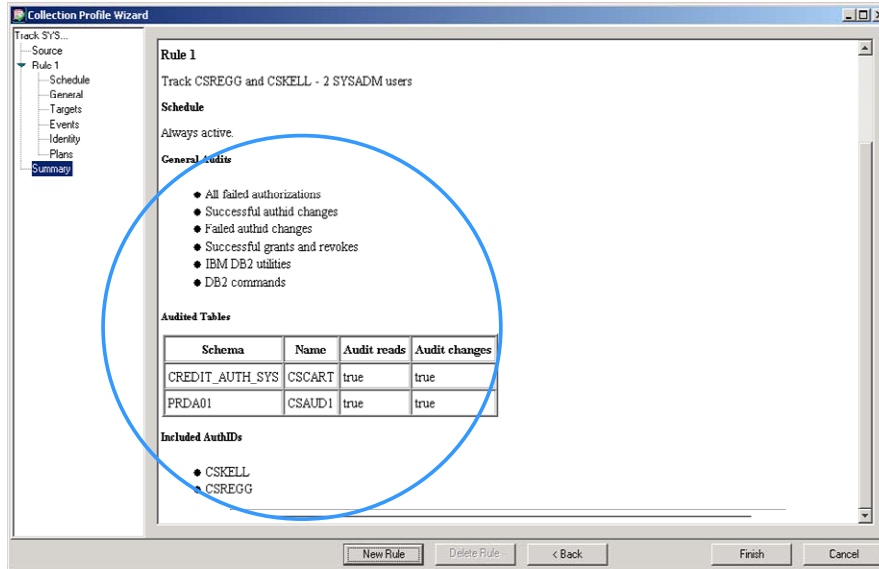


4.4.7 Include or Exclude by Plan

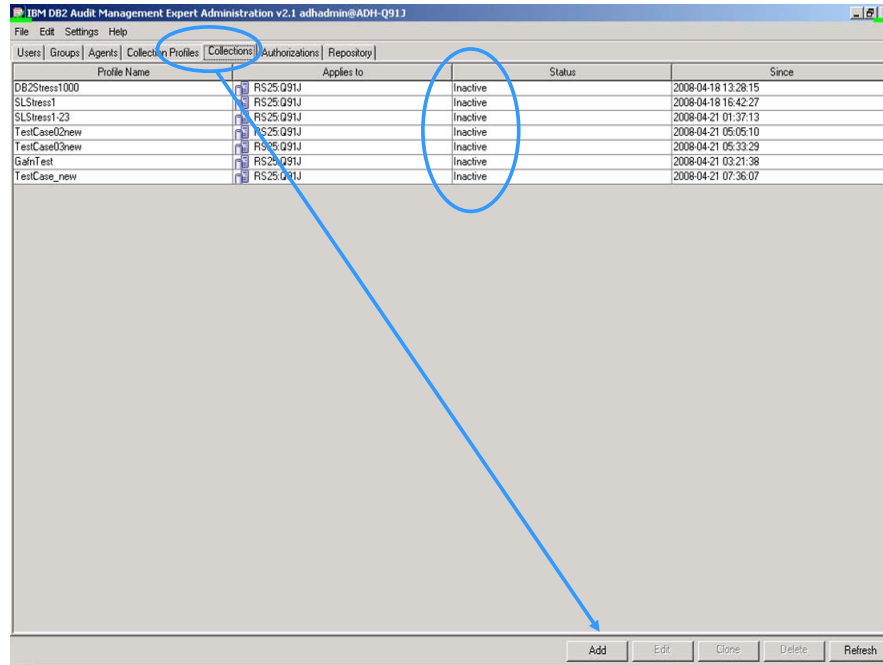
The Plans page of the collection profile enables you to include or exclude specific plans from the rule.

4.4.8 Collection Profile Summary

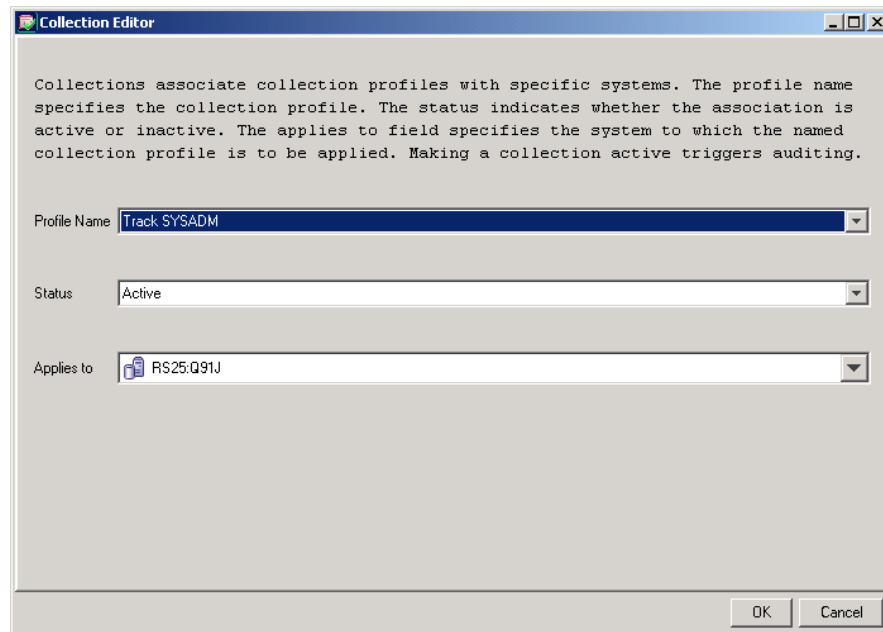
The final page of the collection profile enables you to view a summary of the collection profile.

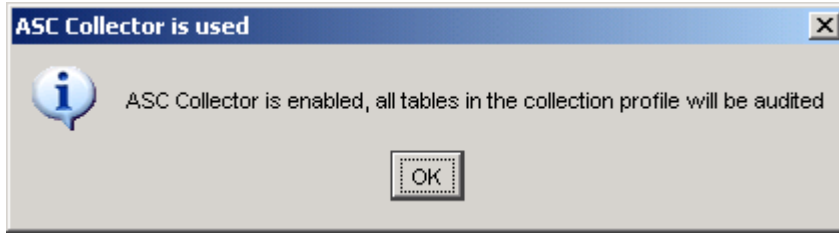


Now that the collection profile has been created, go to the 'Collections' tab and click 'Add' to add a new active collection with the newly created collection profile.



Select the profile name from the drop down list, as shown below, and press 'OK'.





In the following screen shot, note that the collection profile, "Track SYSADM", is now active, and audit data is being collected for that collection profile

IBM DB2 Audit Management Expert Administration v2.1 adhadmin@ADH-Q91J

File Edit Settings Help

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

Profile Name	Applies to	Status	Since
DB2Stress1000	RS25-Q91J	Inactive	2008-04-18 13:28:15
SLStress1	RS25-Q91J	Inactive	2008-04-18 16:42:27
SLStress1-23	RS25-Q91J	Inactive	2008-04-21 01:37:13
TestCase02new	RS25-Q91J	Inactive	2008-04-21 05:05:10
TestCase03new	RS25-Q91J	Inactive	2008-04-21 05:33:29
GainTest	RS25-Q91J	Inactive	2008-04-21 03:21:38
TestCase_new	RS25-Q91J	Inactive	2008-04-21 07:36:07
Track SYSADM	RS25-Q91J	Active	2008-04-22 16:30:02

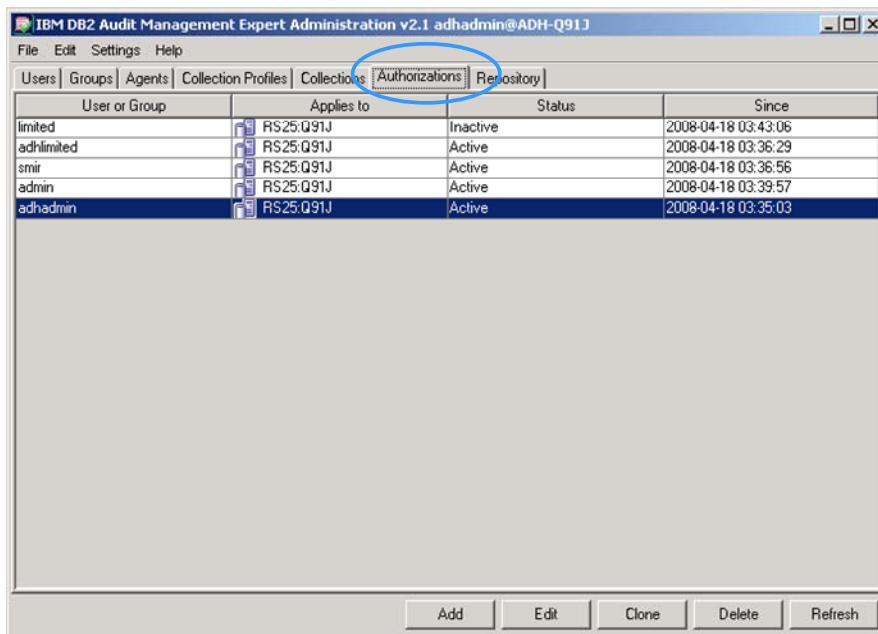
Add Edit Clone Delete Refresh

4.5 Authorizations Tab

Authorizations describe which audit data, once collected, can be viewed by associated users or groups. From the administration interface 'Authorizations' tab, administrators can create authorizations, edit authorizations, clone authorizations, delete authorizations, and view which users have active (or inactive) authorizations for a particular database.

For each authorization, the 'Authorizations' tab displays the user (or group) that has authorization, the database to which the authorization is applied, whether or not the authorization is active, and the date of the last status change.

Note: Click 'Refresh' from the 'Authorizations' tab to update the data display prior to adding, editing, cloning, or deleting authorizations. Clicking 'Refresh' clears the current data and queries the server for updates to enable you to view the latest data.



User or Group	Applies to	Status	Since
limited	RS25:Q91J	Inactive	2008-04-18 03:43:06
adhlimited	RS25:Q91J	Active	2008-04-18 03:36:29
smir	RS25:Q91J	Active	2008-04-18 03:36:56
admin	RS25:Q91J	Active	2008-04-18 03:39:57
adhadmin	RS25:Q91J	Active	2008-04-18 03:35:03

4.6 Repository Tab

The Repository screen needs to be filled out so that DB2 Audit Management Expert for z/OS can use the supplied connection information to access the collected data from within the reporting UI and display reports.

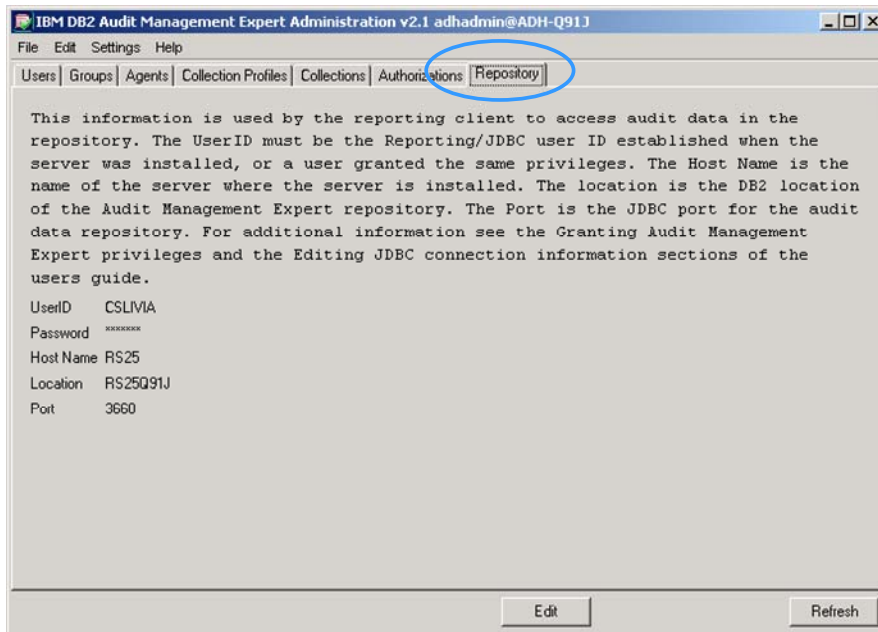
Under the Repository Tab, set the User ID that will be used by the Reporting client to access audit data in the AME repository.

This User ID must be the Reporting/JDBC User ID established when the server was installed, or a user granted the same privileges. This User ID must also be the target of the 'CREATE ALIASES' install step.

This User ID can also be used to run Log Analysis if the Log Analysis jobcard was supplied in the Agents tab: Agent Editor; JCL panel. In this case, this User ID needs authority on the objects being checked in the DB2 log.

If the TSO password is an expiring password, the Administration User Interface Repository tab needs to be updated with the new password when changed. If the Administrator forgets to update the password in the repository tab, the next person who tries to Login to the Report User Interface will get an error message that mentions the likely cause. Simply update the password and the next person that tries to Login to the Reporting User Interface will be able to Login successfully. DB2 Audit Management Expert for z/OS stores the HASH of the password.

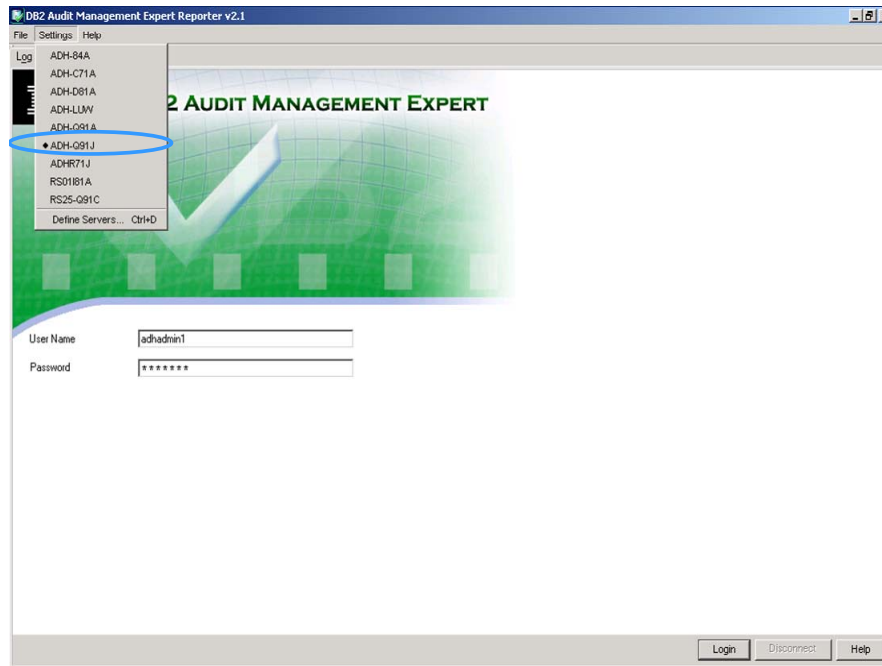
The Port number and location are of the DB2 SSID the repository is on and not the ports defined in server/agent config. Port number and location can be found by looking at the DB2 SSID's Master and search for port or location.



5 Reporting User Interface

5.1 Logging in to the Reporting User Interface

To log in to the Reporting User Interface, select the 'Settings' tab and select a host, or select, 'Define Servers' and fill in the fields. 'Server host' is the name of the system running the server', and 'Server port' is the port on which the server is listening for connections. Enter a User Name and password and click the 'Login'.



5.2 DB2 Systems Level 1 - Overview

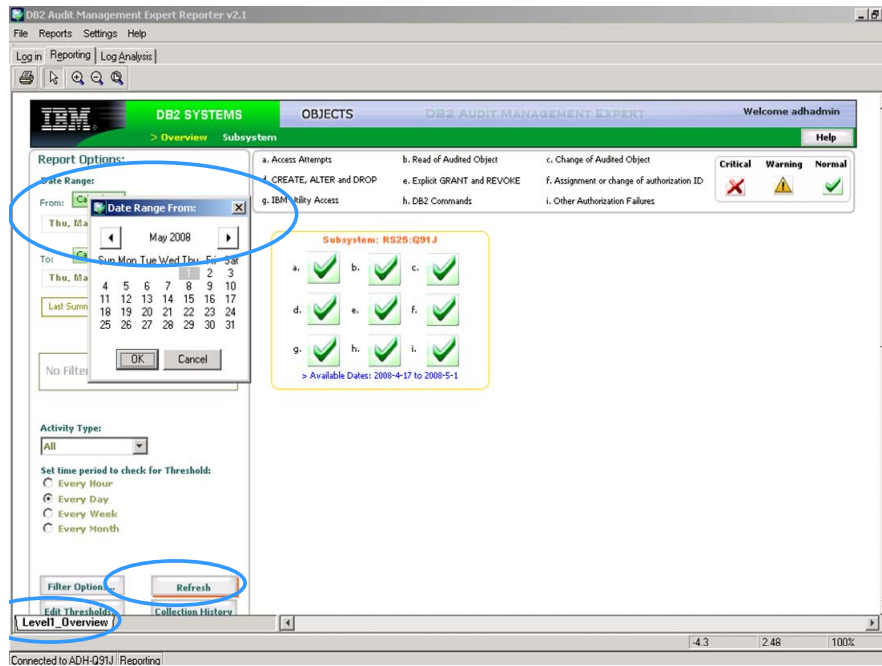
The example below shows the overview display. To get to the overview display, select the, '>Overview' tab under DB2 SYSTEMS. The overview is considered a level 1 report and is displayed in the lower left hand corner of the screen. From here you can view all of the subsystems currently being monitored, based on summarized audit data placed in summary tables. The 'Subsystem' tab is considered a Level 2 report which drills down further.

Level 1 and level 2 reports are created by using the summarization tables. These reports are summarized by AUTHID and PLANS and are the only filters available on these levels. The 'OBJECTS' tab, Level 3, contains the object details. Level 3 has extensive filtering capability as the reports are run against the underlying audit records, and not the summary tables.

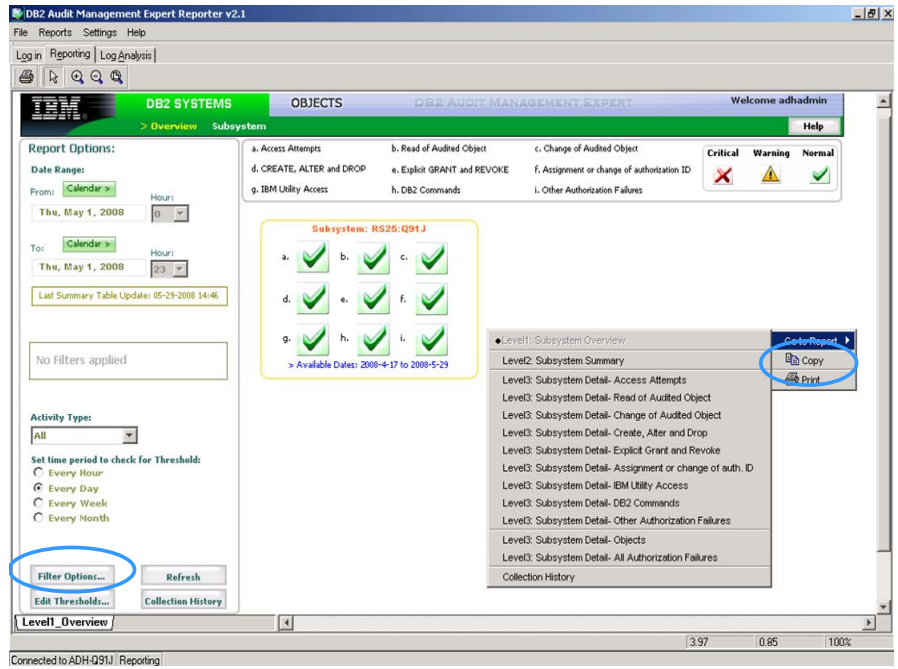
In the following example, data is shown for one DB2 subsystem, Q91J. If multiple DB2 subsystems were monitored and there was data collected for them, a box would be

displayed for each DB2 subsystem. The checkmarks within the box display threshold criteria that you can set. Each checkmark has a corresponding letter, which is shown in the legend at the top of the screen. The default threshold for each activity is 500. This example shows the monitoring of specific users and the desire to audit all activities performed by the specific users against a couple of sensitive tables, so we are not watching or modifying thresholds.

To review data for a specific day or date range, click on the calendar tab on the left to change the date. You can also change the 'From' or 'To' dates, or both. Clicking on the '>Available Dates' link at the bottom of the subsystem box will pre-fill the date range with the displayed values. Note: the 'Refresh' button on the bottom left is now outlined in red. Click it to refresh the data for the selected date range.

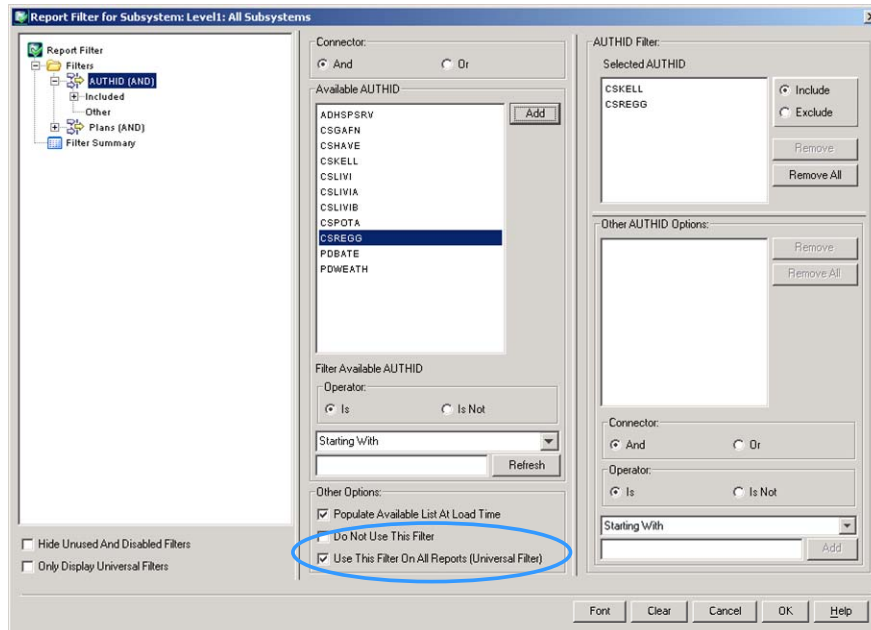


By right clicking anywhere on the screen, a pop-up menu appears that will let you navigate to any report. Note the Copy and Print options on the right. By selecting 'Copy' the entire screen is captured and can be pasted anywhere. By selecting 'Print' the entire screen is sent to the specified printer.



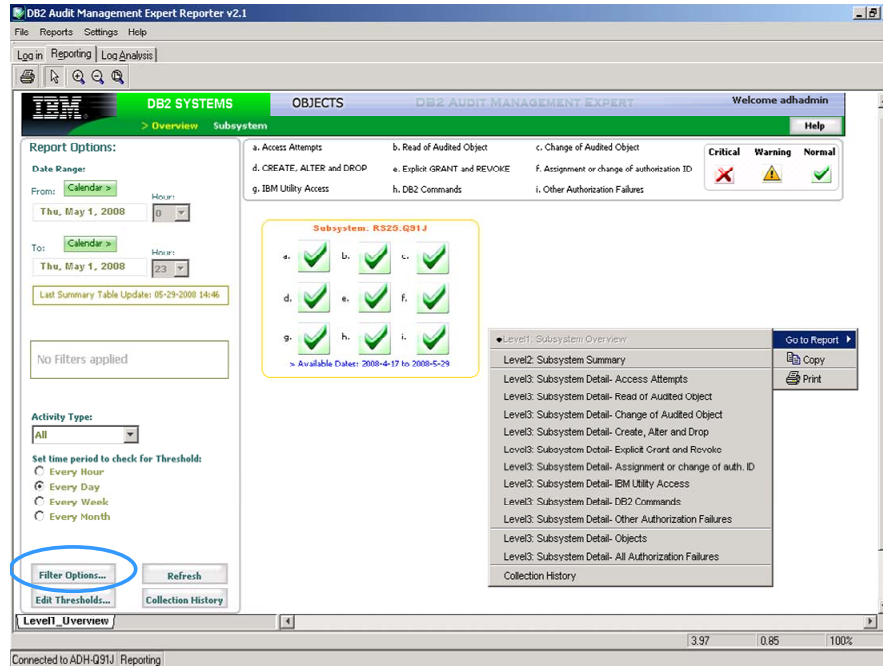
This example focuses on SYSADM users CSREGG and CSKELL, so a filter is added to focus only on those two users. To report on all SYSADM users, a user ID mask can be used. Level 1 and level 2 reports can be skipped and you can go directly to the detailed information in the Level 3 reports and create a Level 3 filter for those users if so desired.

By default, this filter will apply across reports of all levels, level 1 'Overview', level 2 'Subsystem', and level 3 'Detail reports'. If you create an AUTHID level 1 filter, it will be used on level 2 and level 3 reports, unless the checkbox 'Use This Filter on All reports' is unchecked (see screen shot below). Filters that only apply to level 3 such as the addition of table names, as one example, are used across all level 3 reports in the same fashion.

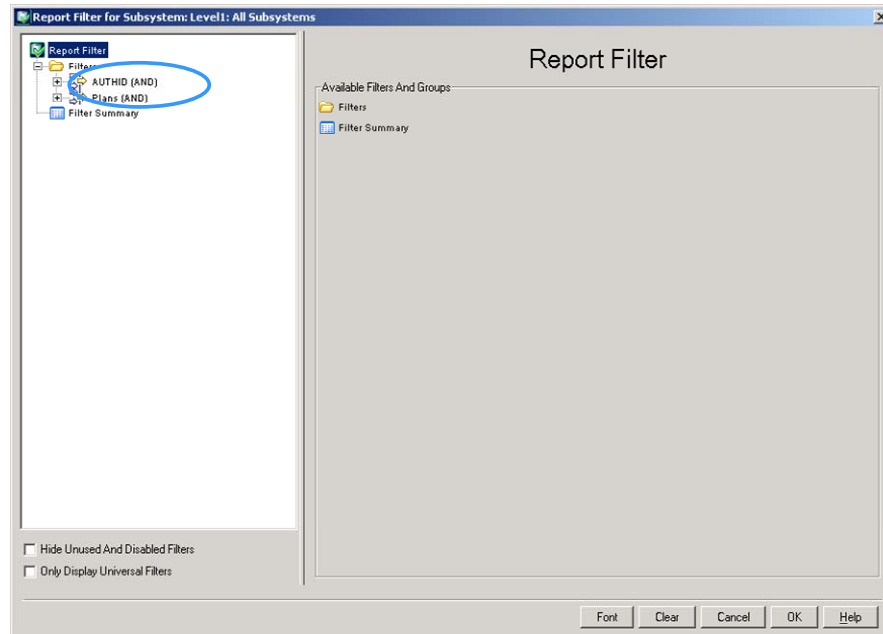


5.2.1 Add a Level 1 Filter

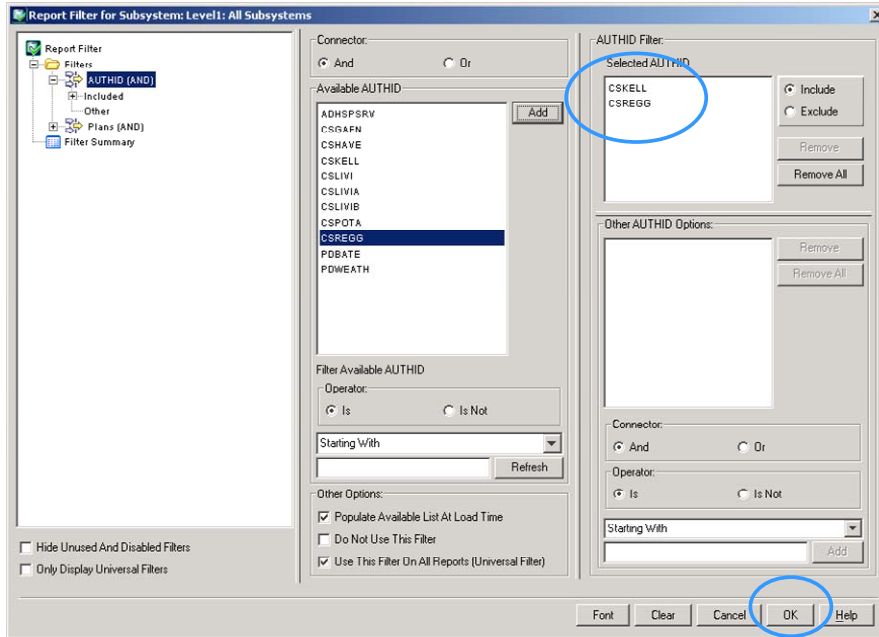
To add a filter, click the 'Filter Options', button in the lower left hand corner.



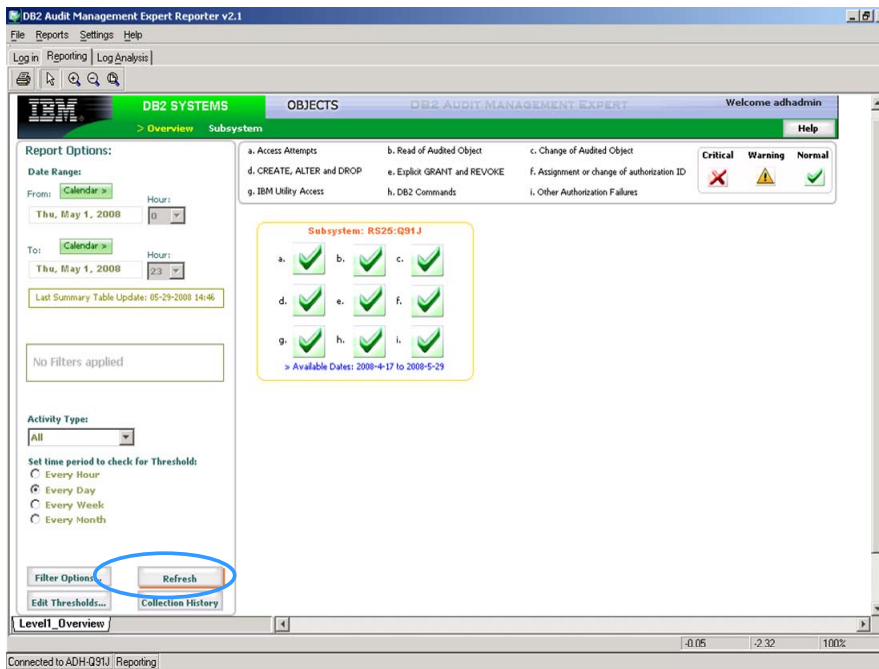
Click on 'AUTHID', as shown in the slide below.



A list of users is displayed. This example has selected and added user CSKELL, followed by selecting and adding user CSREGG'. Note that both users are now in the upper right hand box called, 'Selected AUTHID'. Click 'OK' to return to the 'Overview' screen.

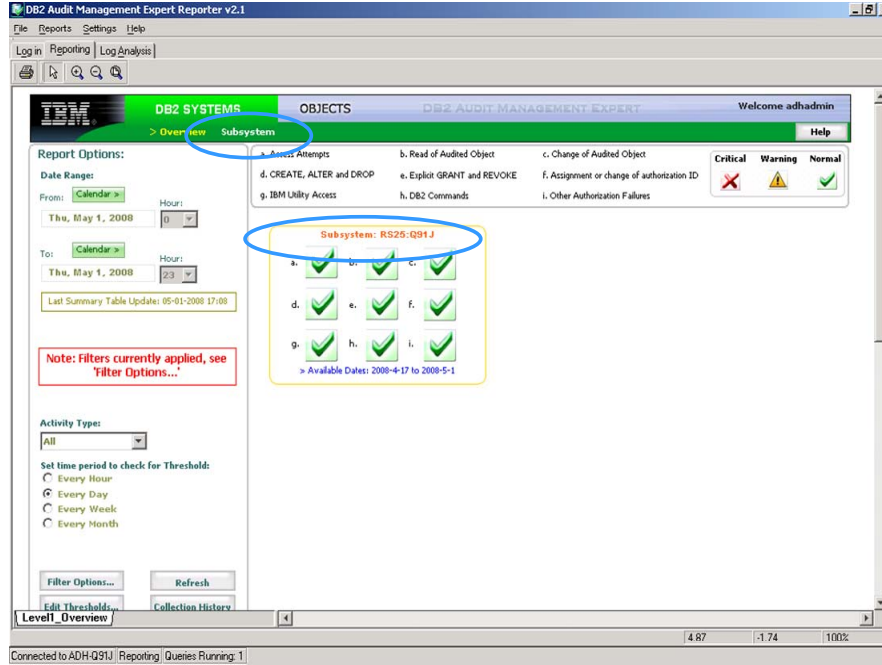


Note the 'Refresh' button on the screen below is now outlined in red. Click the button to refresh the data for the newly added filter.



As shown on the left hand side of the screen in red, the filter has been applied.

Next, click on the 'Subsystem' tab under DB2 SYSTEMS. If there were multiple subsystems displayed, click on the subsystem of interest to view the level 2 reports.



5.2.2 DB2 Systems Level 2 – Subsystem

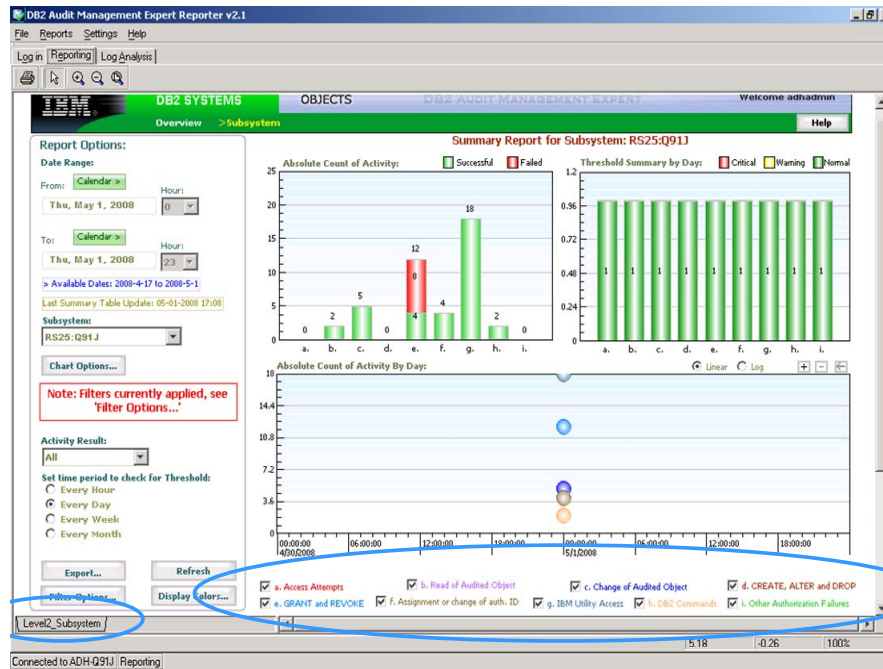
You are now in the level 2 subsystem reports as shown in the lower left hand corner of the screen shot below. Level 2 drills down deeper than the level 1 reports in 'Overview'. Note the filters still apply. If they had not been created while in Level 1, they can be created in Level 2.

Overview of the graphs:

1. The 'Absolute Count of Activity' chart, shown in the upper left corner, displays the activity count for the selected time period. In this case, it displays counts for one day. If the date range was greater than one day, the absolute count increases and reflects the totals for the days selected.
2. 'Threshold Summary by Days' compares the count of each activity (by days), against the threshold criteria.
3. The 'Absolute Count of Activity by [Hour, Day, Week, Month] graph at the bottom of the window shows an absolute activity count for the time period specified by the Date Range option (the date range you specify appears at the bottom of the graph).

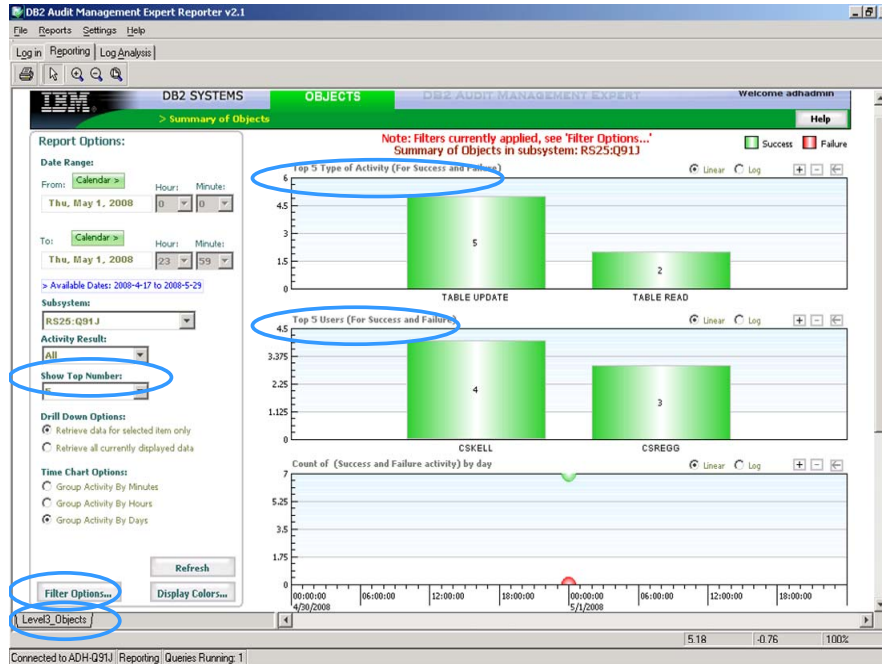
At the bottom of the upper left graph, a row of letters (a – i) is shown. Each one, and its related bar, corresponds to the legend at the bottom of the screen. If you click on any bar, you automatically drill down to a level 3 report. Because this example is currently at Level 2, the only applicable filters are AUTHID or PLANS.

Next, click on the 'OBJECTS' tab at the top of the screen to go to Level 3 – detailed data, or right click anywhere on the page to get the list of reports and go directly there, or click on one of the bar options.



The slide below indicates that we are now in Level 3 as shown in the lower left hand corner. By default, the graph displays the top 5 objects and top 5 users as you see just above each graph. This can be changed by modifying the 'show top number' drop down menu on the left side of the screen.

The OBJECTS display shows any activity against an audited table - which Update, Delete, Insert, Select, Create, Alter, Drop.



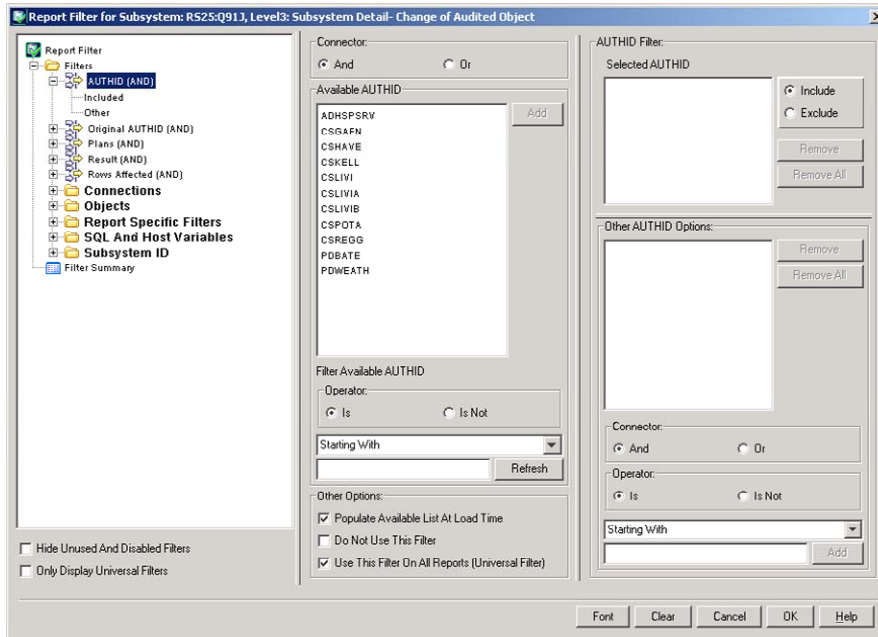
5.2.3 Add a Level 3 Filter

As noted previously, filters created during level 1 or level 2 still apply to level 3. Level 3 filters allow you to filter on specific tables, and much more. For the following example, we will ignore the fact that a level 1 filter has already been created, in order to demonstrate how to create a level 3 filter that includes both AUTHIDs and tables.

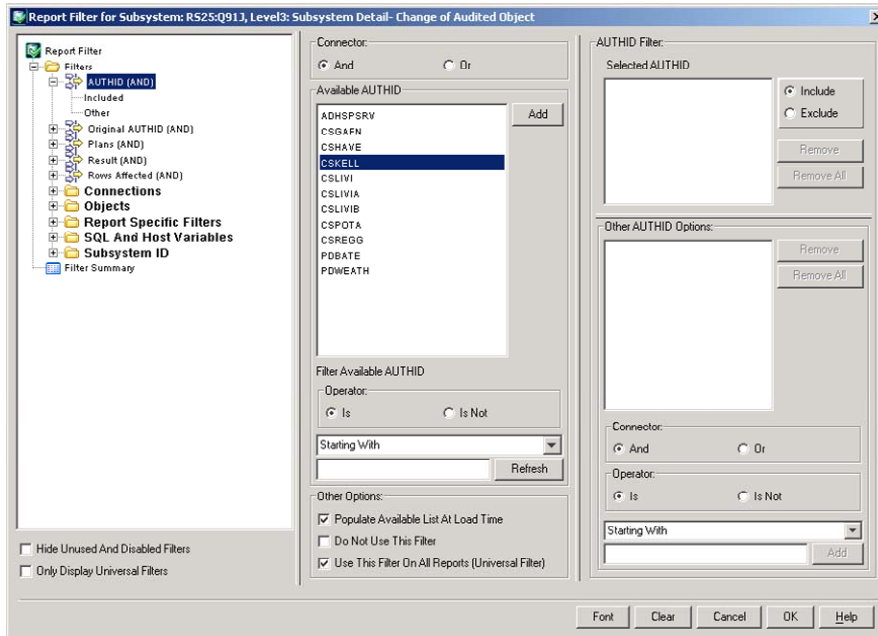
To create a level 3 filter, click the 'Filter Options' button as shown in the previous slide (lower left).

The next several screen shots will demonstrate how to create a level 3 filter to exclude all data except for SYSADM users CSREGG and CSKELL, and sensitive tables PRDA01.CSAUD1 and CREDIT_AUTH_SYS.CSCART.

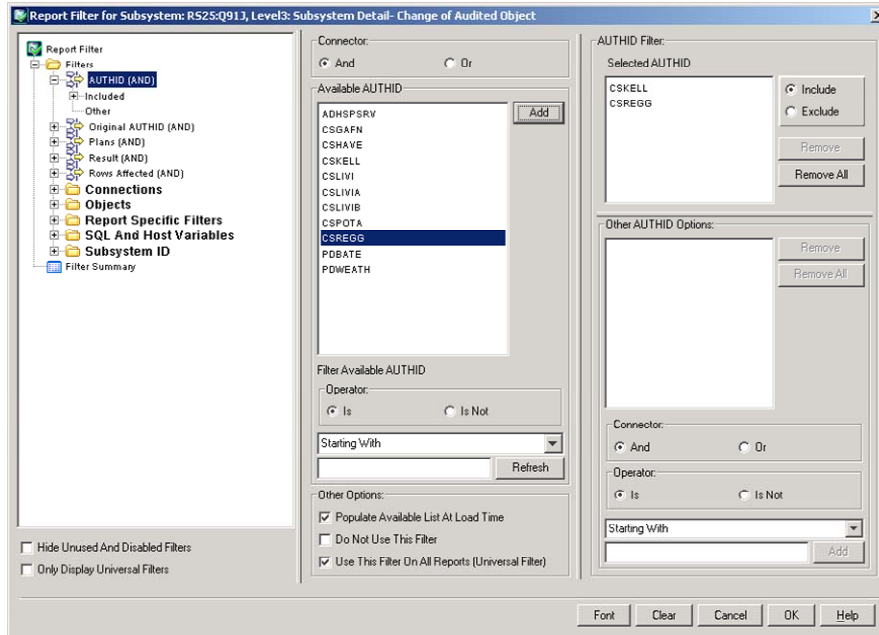
Select the AUTHID field shown below.



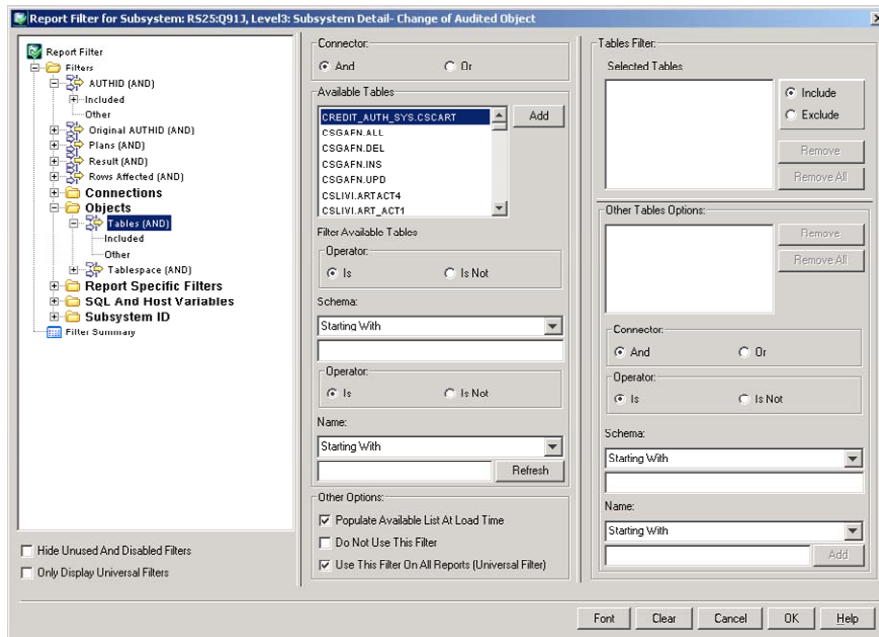
Select the user you want to add as shown below, and click 'Add'. Select the next user and click 'Add'.



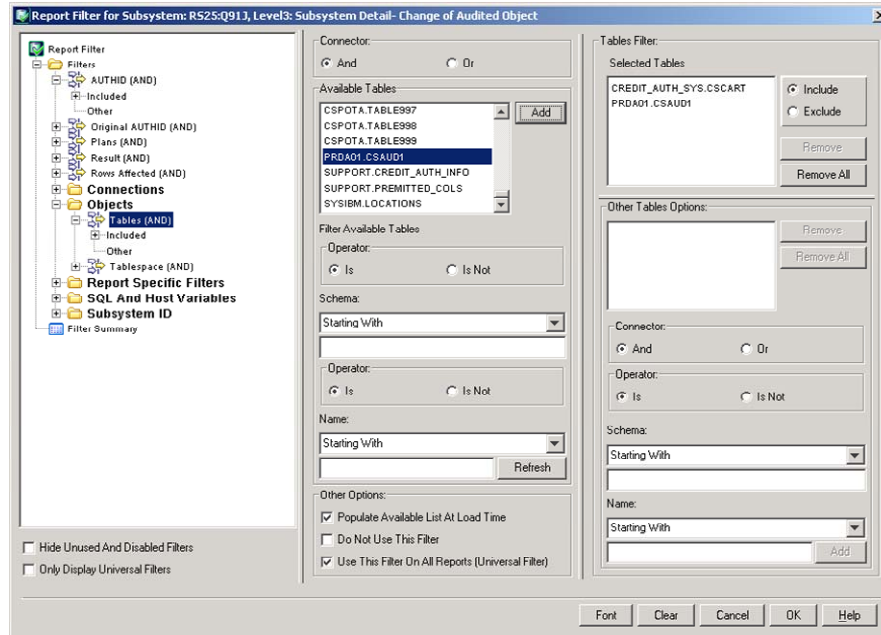
After the users have been added, they show up in the right hand screen under, 'Selected AUTHID', as shown below.



Next, click on 'Objects', and then click on 'Tables (AND)', which is underneath 'Objects' for a list of available tables. Select the table you want to find data for and click 'Add'. Select the next table, and click 'Add'.



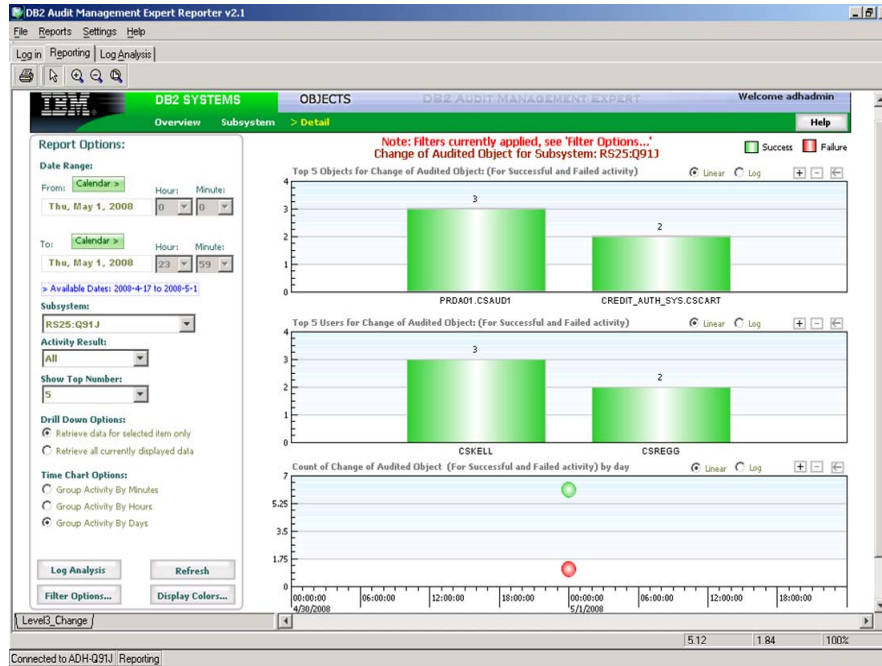
Notice that the two tables are now listed in the upper right hand corner under, 'Selected Tables'. Click 'OK' to save the filter.



After clicking ok, you are brought back to the menu you went into the filter from. The refresh button is now outlined in red, which indicates a change. Click the 'Refresh' button to apply the newly created filters.

A message in red at the top of the screen indicates that the filters have been applied. The filter will allow us to display AUTHIDs, CSREGG and CSKELL and enable us to identify what activities they have made against sensitive tables, PRDA01.CSAUD1 and CREDIT_AUTH_SYS.CSCART.

Double-click on the cylinder, shown below in the 'Top 5 Objects for Change' for table, PRDA01.CSAUD1 to drill down to the details.



The level 3 detailed data is shown below. Additional data can be seen by scrolling to the right. In the next several slides, you can see the data was collected using the ASC Collector. You can see the schema, the table name, the user ID, the plan, the DB2 subsystem, and the changes that were made – an update, delete, and insert.

The screenshot shows the 'Audit Management Expert Data for level3_change' window. It displays a table with 3 records. The table has columns: ROW, TIME, RESULT, RETURNED, RECORD_S..., SCHEMA, NAME, and IFICODE. The data is as follows:

ROW	TIME	RESULT	RETURNED	RECORD_S...	SCHEMA	NAME	IFICODE
1	2008-05-01 1...	0	SUCCESS	ASC DATA	PRDA01	CSAUD1	00143
2	2008-05-01 1...	0	SUCCESS	ASC DATA	PRDA01	CSAUD1	00143
3	2008-05-01 1...	0	SUCCESS	ASC DATA	PRDA01	CSAUD1	00143

The window also includes a 'Record Count: 3' indicator and buttons for Copy, Export, Zoom, Search, Cancel, Close, and Help.

Scroll to the right.

Audit Management Expert Data for level3_change

Option

Record Count: 3

CORRELAT...	CONTEXT_...	CONTAINER	TYPE	NEW_SQLID	AUTHORIZ...	ORIGINAL_...	ACCOUNT_...
0	TABLE UPD...	CSAUD1##	TABLE/VIEW	N/A	CSKELL	CSKELL	N/A
0	TABLE UPD...	CSAUD1##	TABLE/VIEW	N/A	CSKELL	CSKELL	N/A
0	TABLE UPD...	CSAUD1##	TABLE/VIEW	N/A	CSKELL	CSKELL	N/A

Copy Export Zoom Search Cancel Close Help

Scroll to the right.

Audit Management Expert Data for level3_change

Option

Record Count: 3

END_USER...	END_USR_...	END_USR_...	PLAN	XDATABASE	APP_ID	APP_NAME	DB2_SUBS...
N/A	N/A	N/A	DSNTEP91	N/A	N/A	N/A	Q91J
N/A	N/A	N/A	DSNTEP91	N/A	N/A	N/A	Q91J
N/A	N/A	N/A	DSNTEP91	N/A	N/A	N/A	Q91J

Copy Export Zoom Search Cancel Close Help

Scroll to the right.

Audit Management Expert Data for level3_change

Option

Record Count: 3

LOCATION	NETWORK...	LUNAME	CORR_ID	CONNECTI...	SYSTEM_C...	REQUESTO...	REQUESTO...
N/A	ROCKNET1	Q91JDB2	CSKELLUP	BATCH	1	RS25Q91J	N/A
N/A	ROCKNET1	Q91JDB2	CSKELLDE	BATCH	1	RS25Q91J	N/A
N/A	ROCKNET1	Q91JDB2	CSKELLIN	BATCH	1	RS25Q91J	N/A

Copy Export Zoom Search Cancel Close Help

Continue scrolling to the right.

Audit Management Expert Data for level3_change

Option

Record Count: 3

REQUESTO...	MEMBER_...	GROUP_NA...	CURRENT_...	STATEMEN...	HOSTVALUE	ROWS_AFF...	ACCESS_A...
N/A	Q91J	N/A	CSKELL	UPDATE PR...	N/A	1	N/A
N/A	Q91J	N/A	CSKELL	DELETE FR...	N/A	1	N/A
N/A	Q91J	N/A	CSKELL	INSERT INT...	N/A	1	N/A

Copy Export Zoom Search Cancel Close Help

At any point, you can click on any field and click on the 'Zoom' button to get more details. The following example takes a look at what has been updated.

DB2 Audit Management Expert Reporter v2.1

File Reports Settings Help

Log in Reporting Log Analysis

DB2 SYSTEMS OBJECTS DB2 AUDIT MANAGEMENT EXPERT Welcome adhadmin

Overview Subsystem > Detail

Report Options:

Date Range: From: Calendar -> Thu, May 4, 2008 To: Calendar -> Thu, May 4, 2008

Subsystems: RS25:Q91J

Activity Result: All

Show Top Numbers: 5

Drill Down Options: Retrieve data for selected item or Retrieve all currently displayed

Time Chart Options: Group Activity By Minutes Group Activity By Hours Group Activity By Days

Log Analysis Refresh Filter Options... Display Colors...

Note: Filters currently applied, see 'Filter Options...' Change of Audited Object for Subsystem: RS25:Q91J

Top 5 Objects for Change of Audited Objects (For Successful and Failed activity)

Audit Management Expert Data for level3_change

Option

Record Count: 3

REQUESTO...	MEMBER_...	GROUP_NA...	CURRENT_...	STATEMEN...	HOSTVALUE	ROWS_AFF...	ACCESS_A...
N/A	Q91J	N/A	CSKELL	UPDATE PR...	N/A	1	N/A
N/A	Q91J	N/A	CSKELL	DELETE FR...	N/A	1	N/A
N/A	Q91J	N/A	CSKELL	INSERT INT...	N/A	1	N/A

Zoom: STATEMENT_TXT

Cell Value

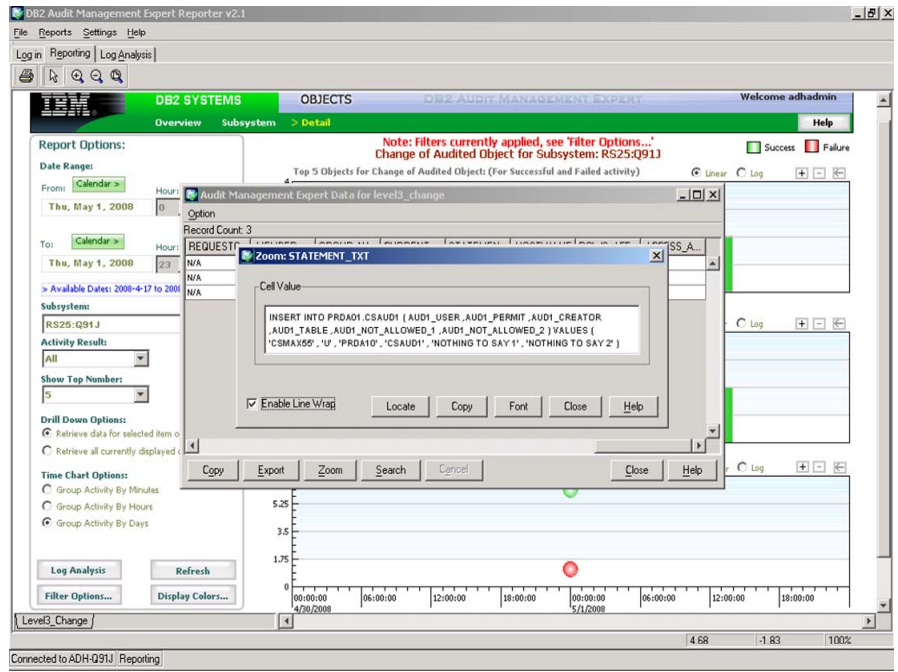
```
UPDATE PRDA01.CSAUDI SET AUD1_USER = 'TSOUSR1' WHERE AUD1_USER = 'CSLIM'
```

Enable Line Wrap Locate Copy Font Close Help

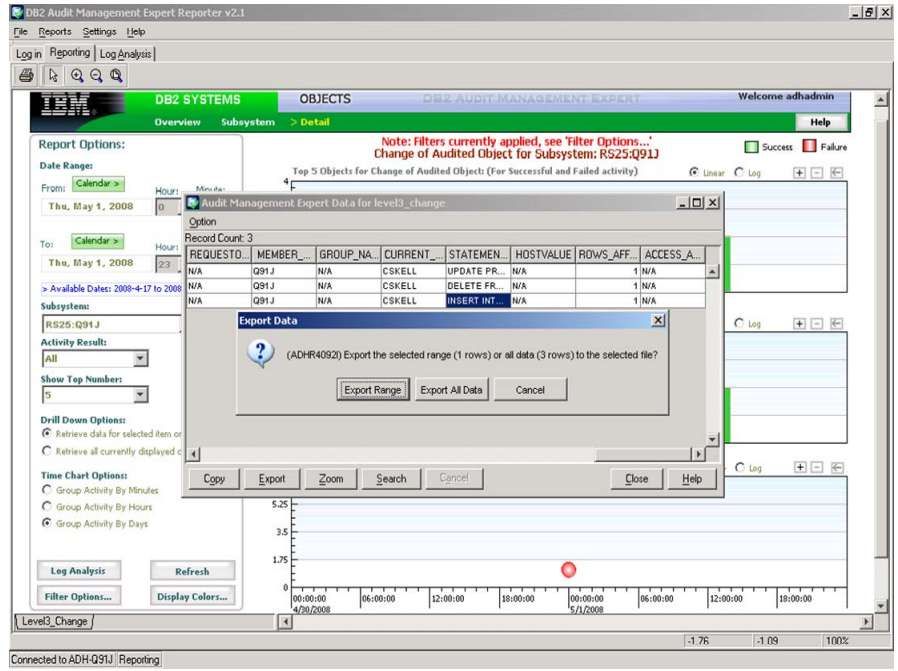
Copy Export Zoom Search Cancel Close Help

Level3_Change / 5.16 0.58 100%

The following example takes a look at what has been inserted. In order to see the whole text, click 'Enable line wrap'.



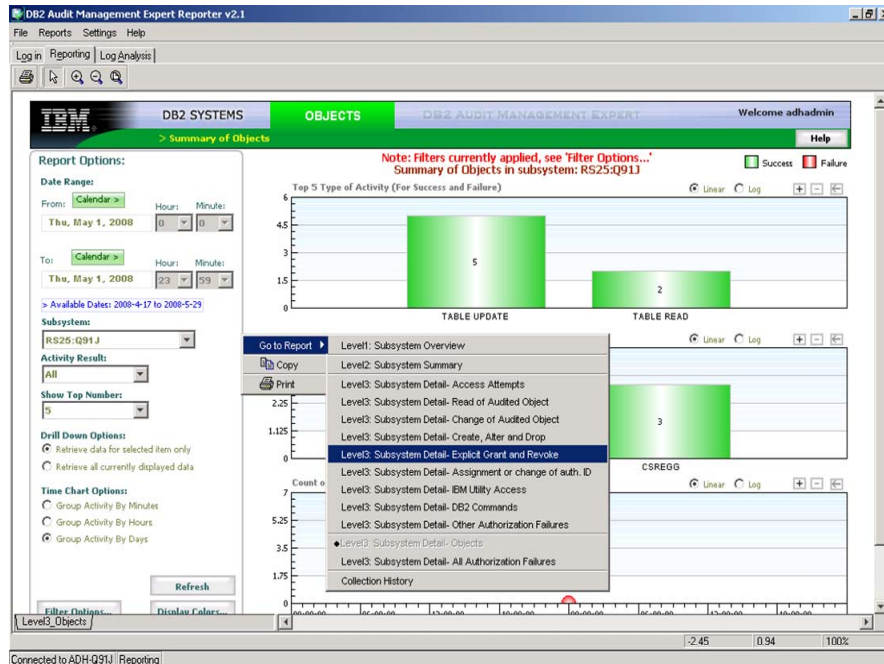
To save this data, click the 'Export Range' to export the data to a csv file.



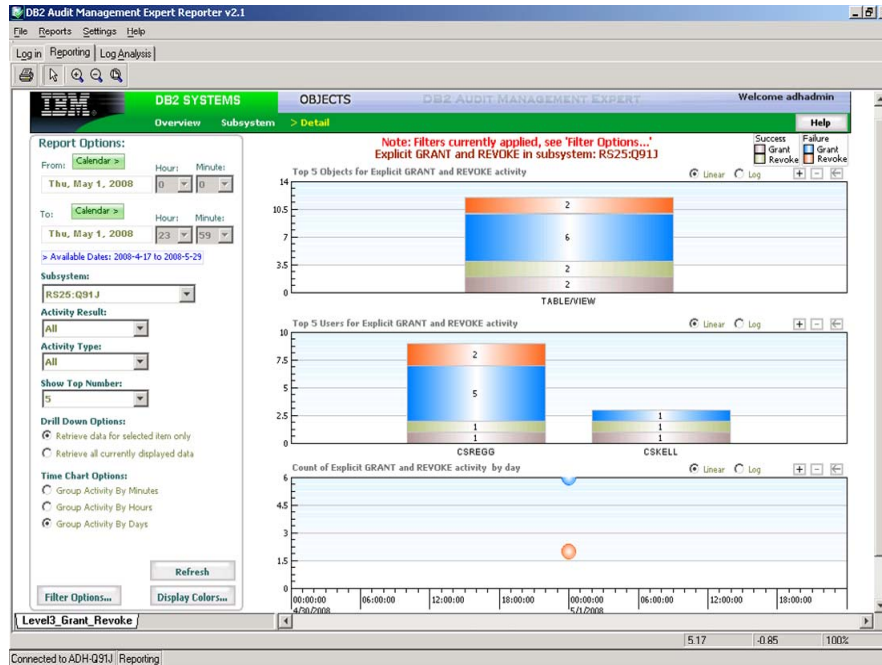
The csv file is shown below.

1	NETWORK/LUNAME	CORR_ID	CONNECT	SYSTEM	REQUEST	REQUEST	REQUEST	MEMBER	GROUP	CURRENT	STATEMENT_TXT	HOSTVAL
2	ROCKNETQ91JDB2	CSKELLUI	BATCH		1	RS25Q91J	N/A	N/A	Q91J	N/A	CSKELL	UPDATE PRDA01.CSAUD1 SET #N/A
3	ROCKNETQ91JDB2	CSKELLDI	BATCH		1	RS25Q91J	N/A	N/A	Q91J	N/A	CSKELL	DELETE FROM PRDA01.CSAUD1#N/A
4	ROCKNETQ91JDB2	CSKELLIN	BATCH		1	RS25Q91J	N/A	N/A	Q91J	N/A	CSKELL	INSERT INTO PRDA01.CSAUD1 (N/A

To see additional level 3 detail, right-click anywhere on the panel to view additional reports as shown below, or select one of the cylinders for the category you are interested in. In the example below, click on the Grant and Revoke report.



Click on the cylinder in the top graph.

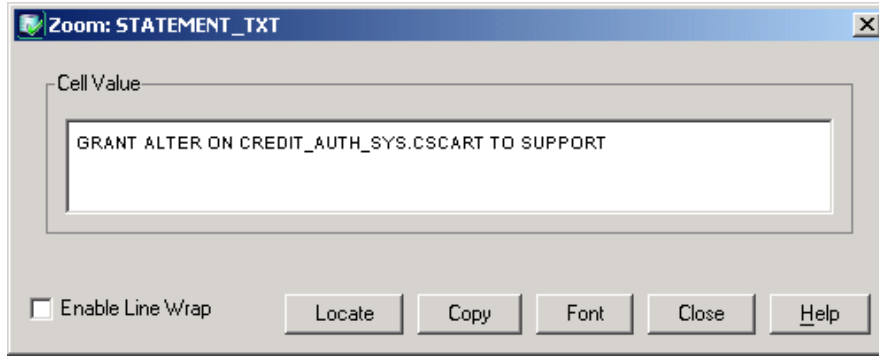


A pop-up is displayed, as shown below. In the following example, we are only interested in successful actions and only grants, so we click on the RETURNED field to sort by SUCCESS.

The screenshot shows a pop-up window titled 'Audit Management Expert Data for level3_grant_revoke'. It displays a table with 12 records. The table columns are ROW, TIME, RESULT, RETURNED, RECORD_S..., SCHEMA, NAME, and IFICODE. The records are sorted by the RETURNED field, showing both SUCCESS and FAILURE results.

ROW	TIME	RESULT	RETURNED	RECORD_S...	SCHEMA	NAME	IFICODE
5	2008-05-01 1...	0	SUCCESS	IFI DATA	N/A	N/A	00141
6	2008-05-01 1...	0	SUCCESS	IFI DATA	N/A	N/A	00141
11	2008-05-01 1...	0	SUCCESS	IFI DATA	N/A	N/A	00141
12	2008-05-01 1...	0	SUCCESS	IFI DATA	N/A	N/A	00141
1	2008-05-01 1...	-551	FAILURE	IFI DATA	N/A	N/A	00141
2	2008-05-01 1...	-551	FAILURE	IFI DATA	N/A	N/A	00141
3	2008-05-01 1...	-556	FAILURE	IFI DATA	N/A	N/A	00141
4	2008-05-01 1...	562	FAILURE	IFI DATA	N/A	N/A	00141
7	2008-05-01 1...	-551	FAILURE	IFI DATA	N/A	N/A	00141
8	2008-05-01 1...	-551	FAILURE	IFI DATA	N/A	N/A	00141
9	2008-05-01 1...	-556	FAILURE	IFI DATA	N/A	N/A	00141
10	2008-05-01 1...	562	FAILURE	IFI DATA	N/A	N/A	00141

At this point, research can determine who did the grant and what they granted. The report can be saved to a CSV file. This process can be continued for any other category of interest.

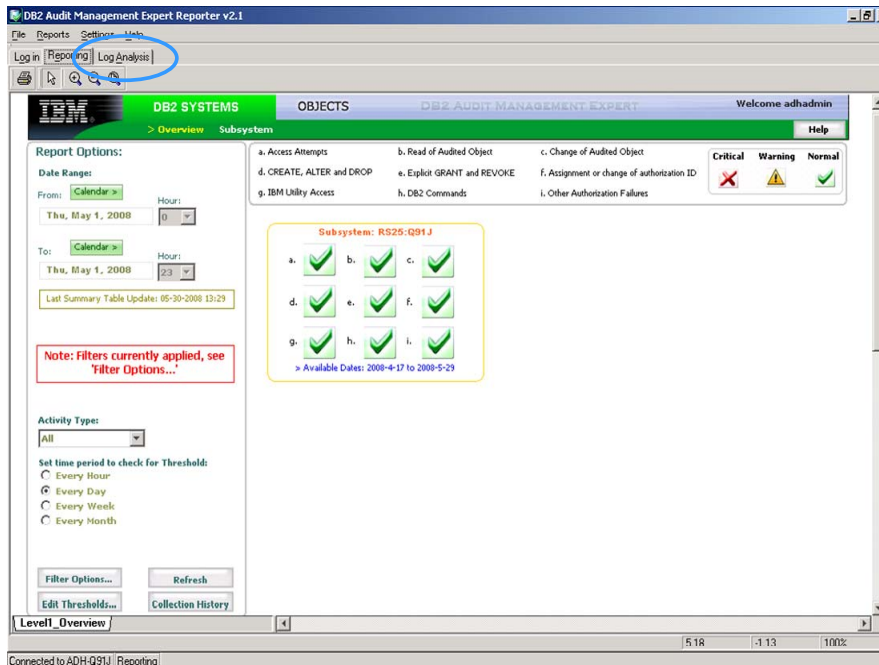


The filters and the criteria for the reports (date range) can be saved at the server and later recalled. This ensures that work is not lost when the client is shut down, and allows it to be used by other users.

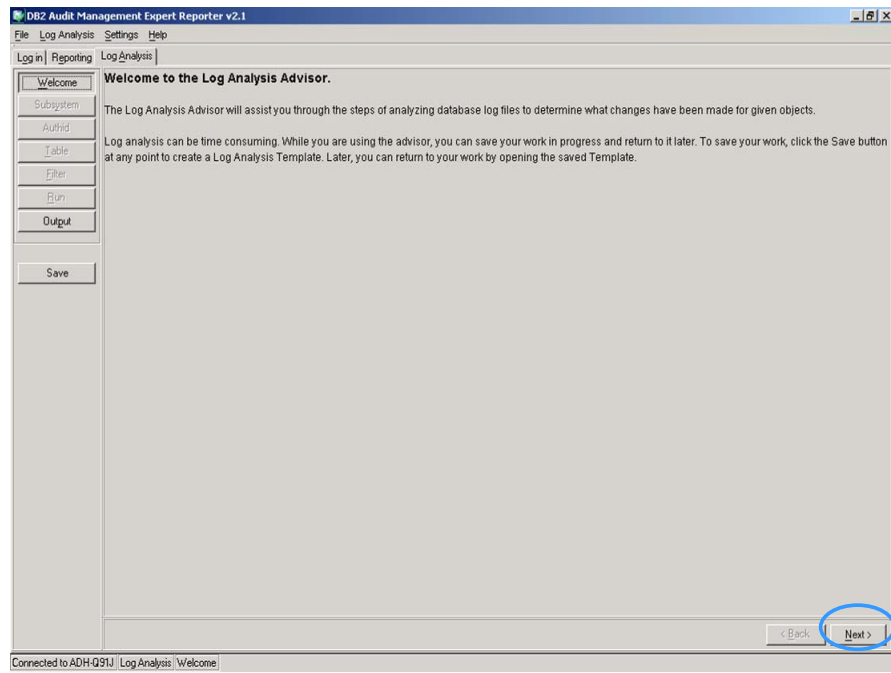
5.2.4 LOG ANALYSIS

The Log Analysis feature of DB2 Audit Management Expert for z/OS captures before and after images for updates, after images for inserts, and before images for deletes to rows in an audited table (on demand).

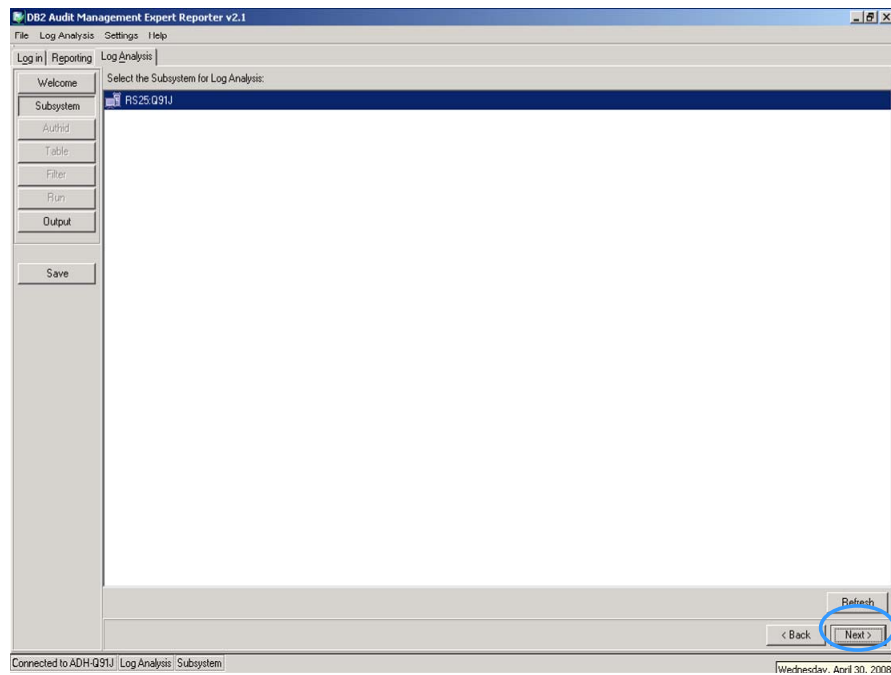
To use the Log Analysis feature, click on the 'Log Analysis' button shown on the upper left-hand side of the screen below. When defining users, authority to use log analysis must be granted in the Administration User Interface in order to use this feature.



Click 'Next' in the lower right hand corner as shown below.

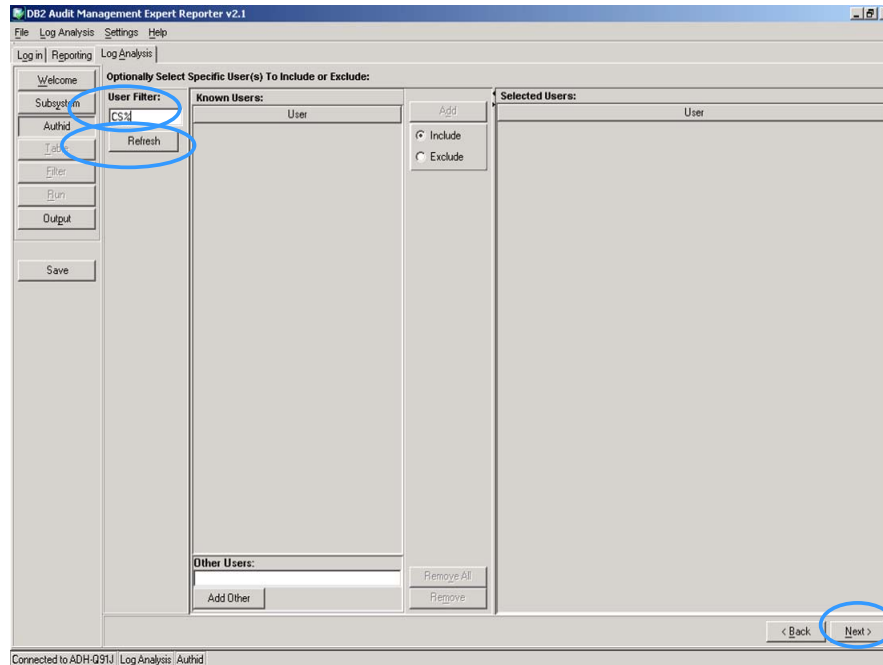


Select a subsystem, as shown below, and click 'Next'.

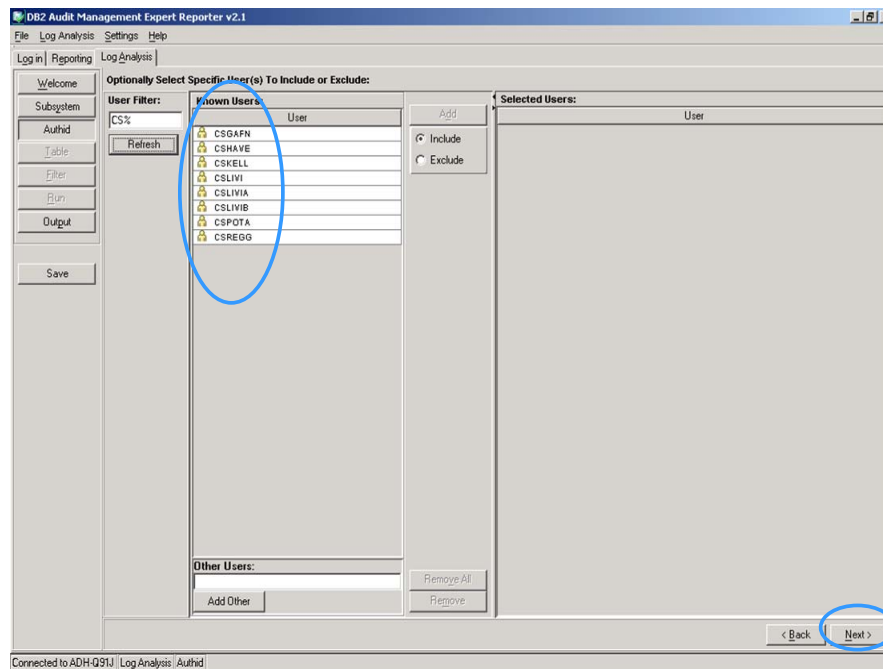


Add a 'User Filter'. The 'User Filter:' must be in upper case. Then click the 'Refresh' button.

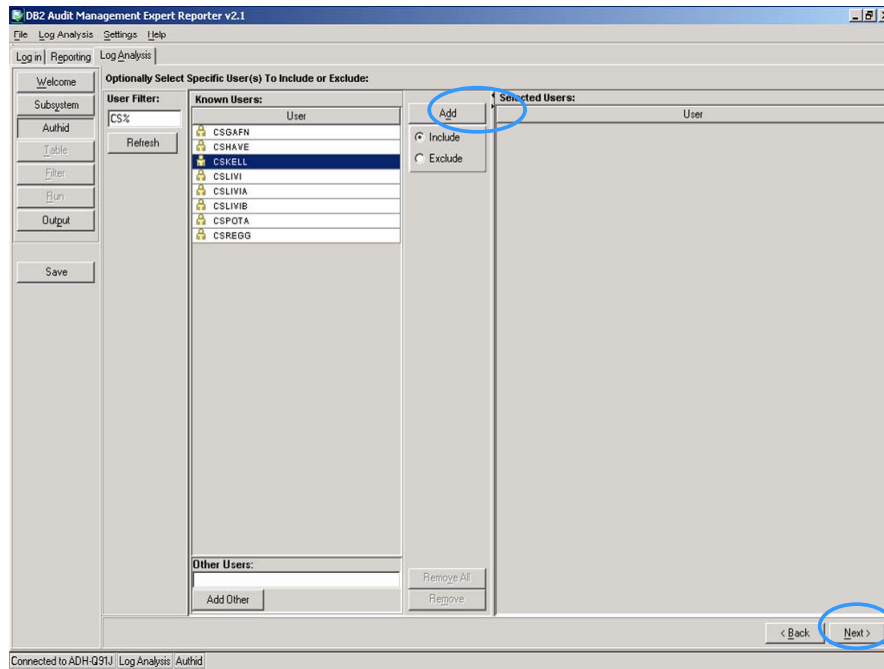
If you leave it empty and click 'Refresh', you will get all available users from which to select from. The example below looks for users that start with CS because we are monitoring SYSADM Users CSKELL and CSREGG.



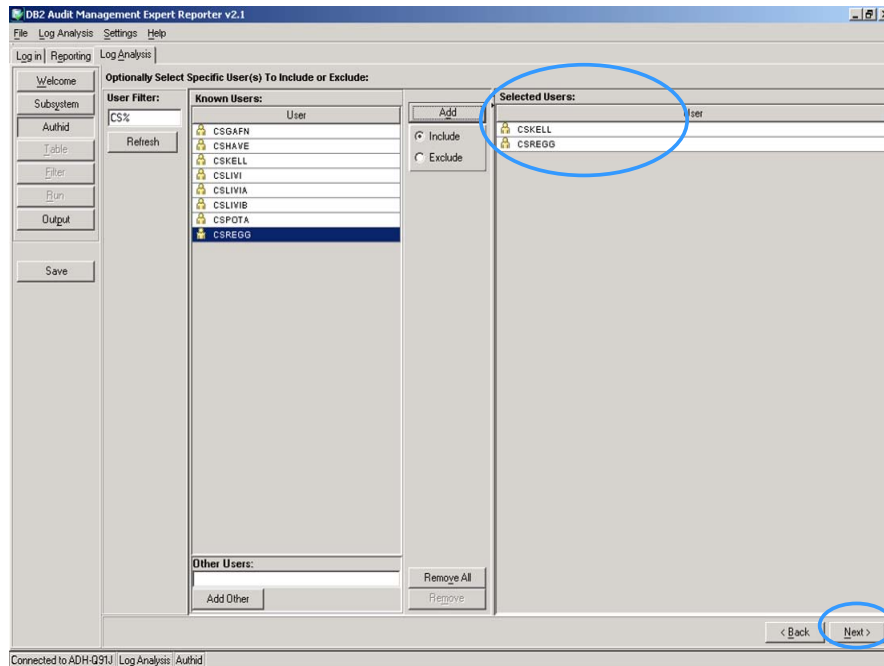
A list of users appears as shown below from which to select from.



Select a user as shown below and click 'Add'. Then click 'Next>'.

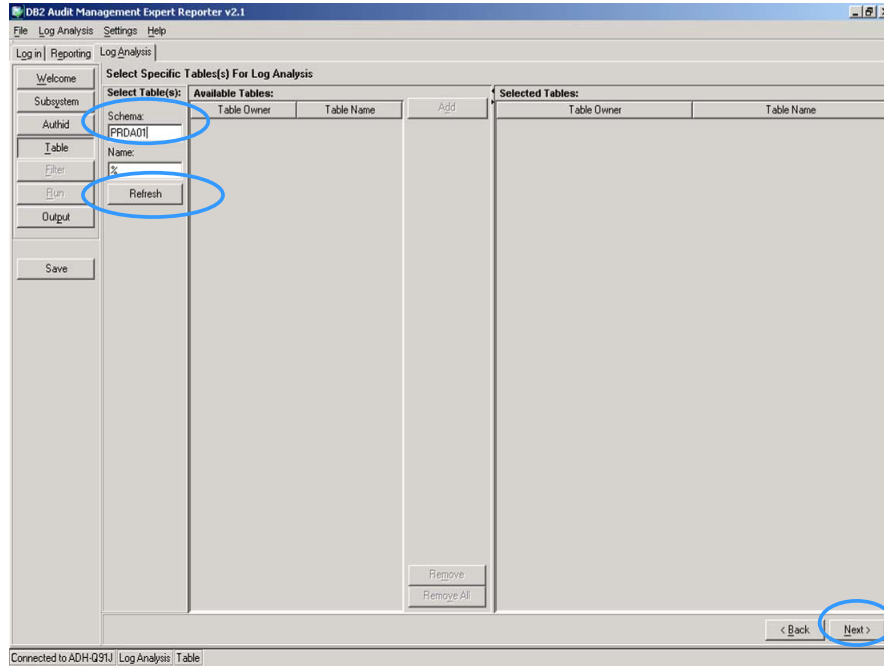


Optionally select another user and click 'Add'. Then click 'Next>'. The two selected users are now in the 'Selected Users' list in the upper right hand corner as shown below.

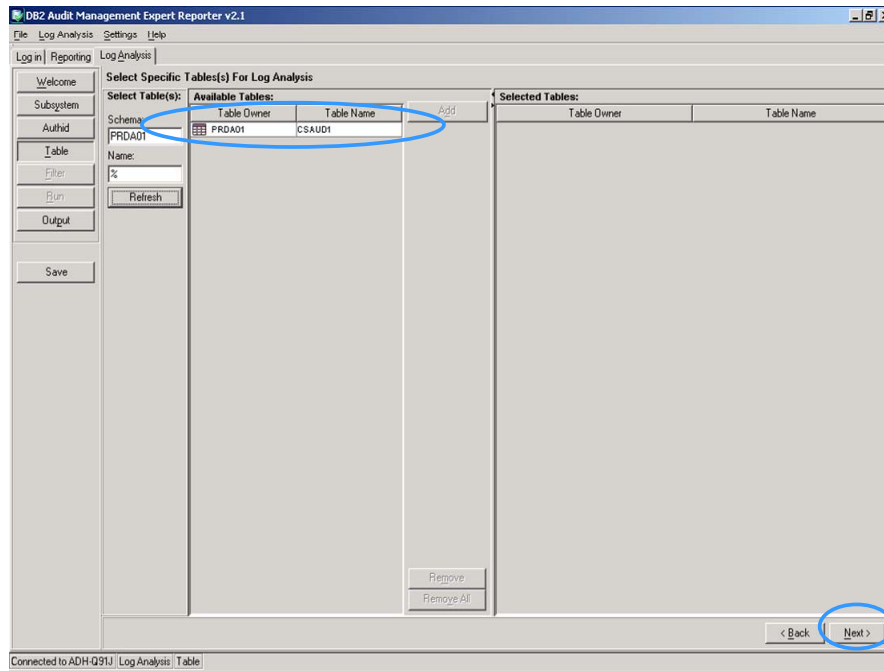


Next select the schema and put a % in 'Name' to find all tables matching that schema. I have selected schema, PRDA01 as shown below. After entering it, click the 'Refresh' button to refresh the list. Click 'Next>'.

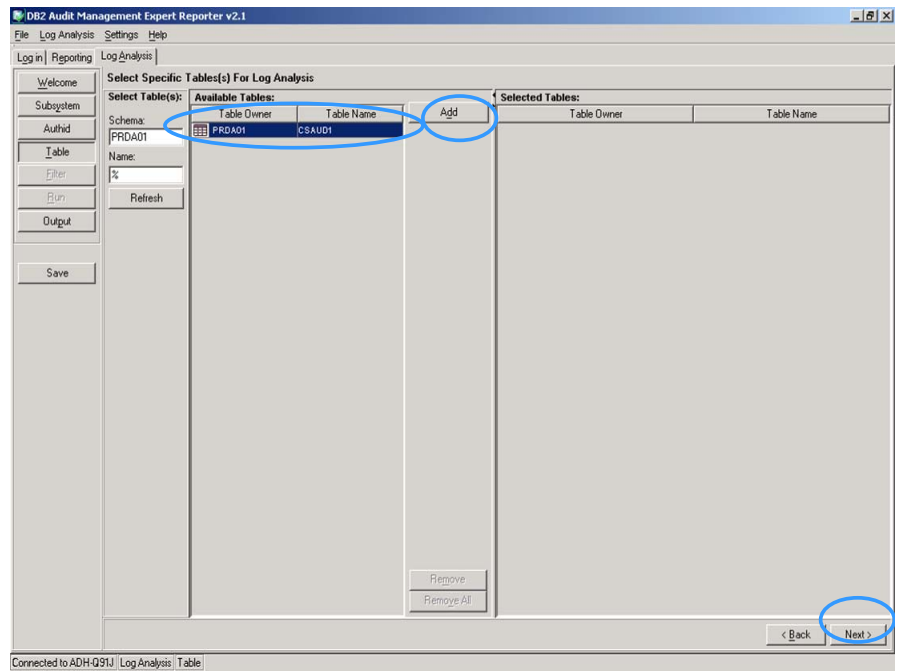
If you leave it empty and click 'Refresh', you will get all available schemas and tables from which to select.



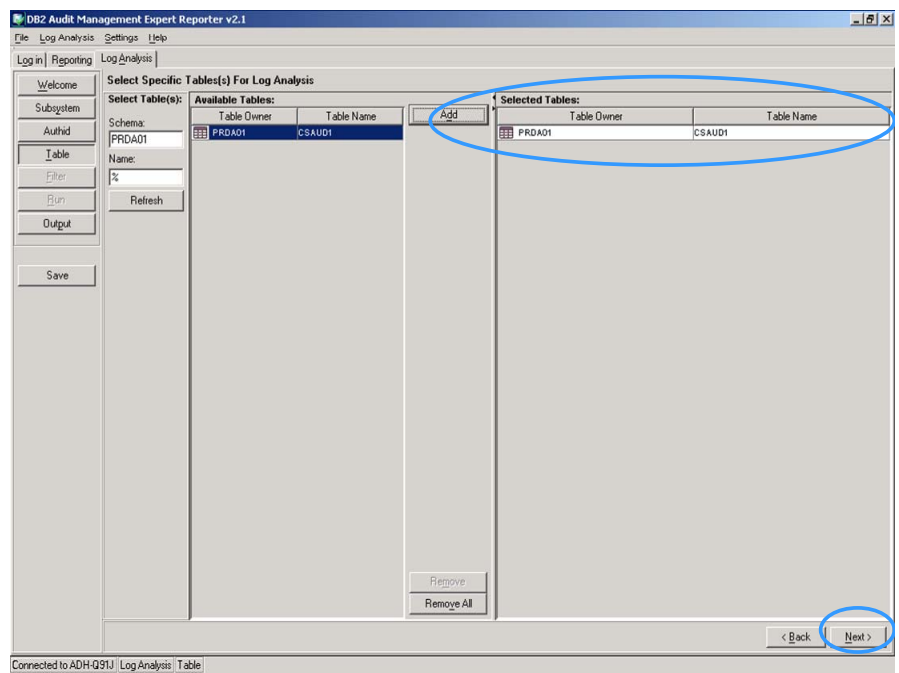
The schema and table are shown below.



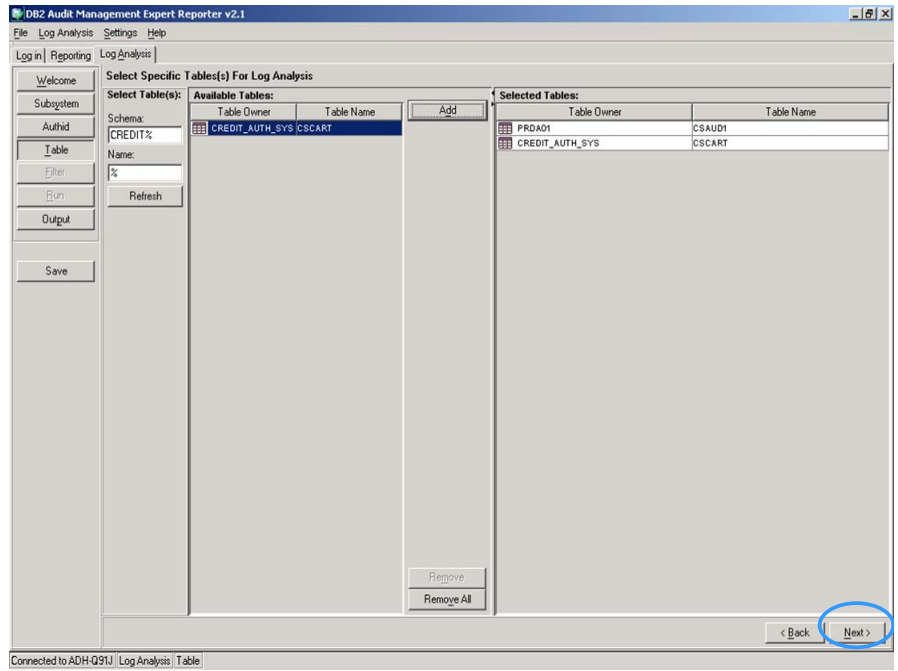
Highlight the table, as shown below, and click 'Add'.



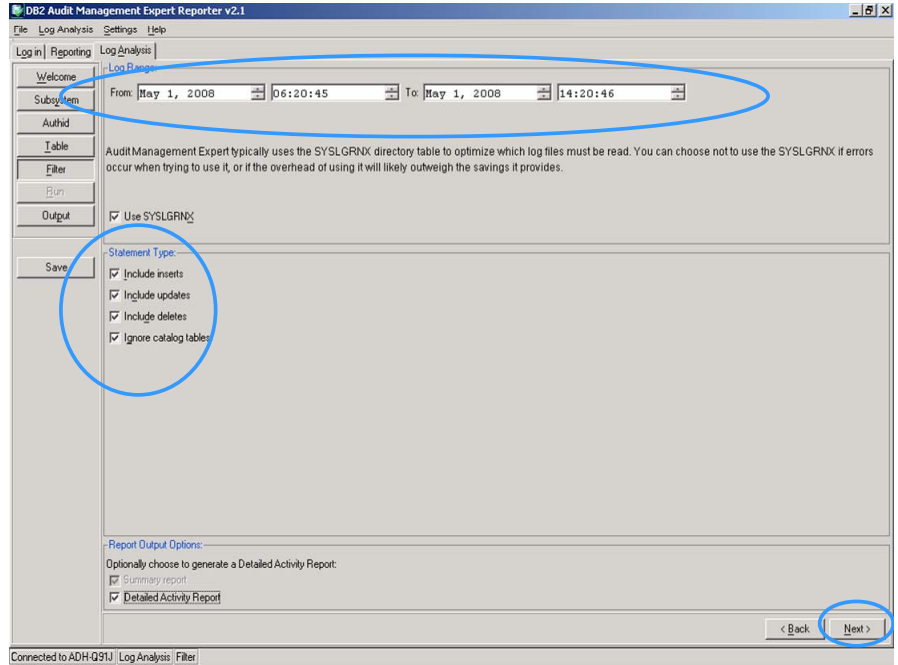
The table is now shown on the right-hand side under 'Selected Tables'. Click 'Next>'



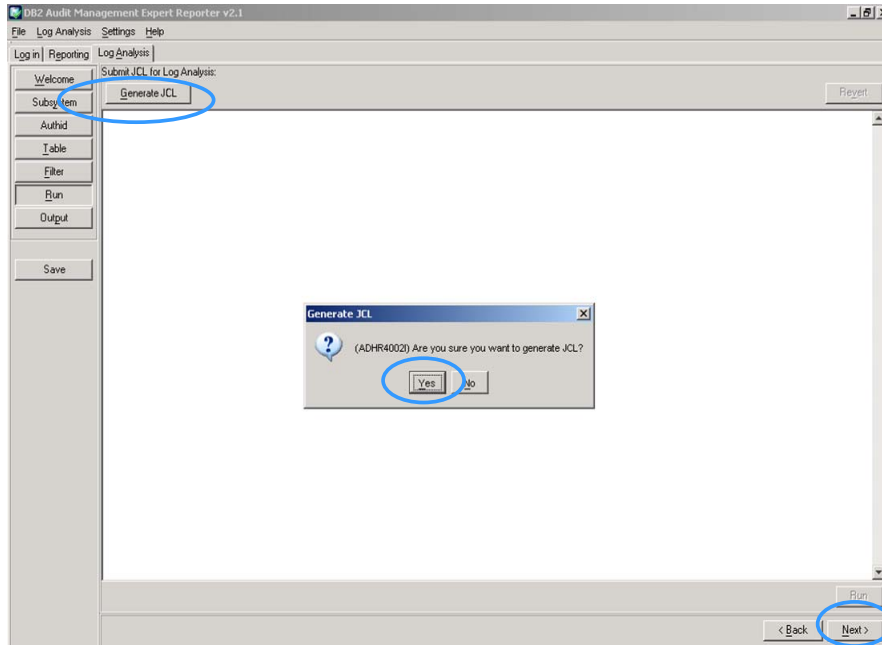
Repeat this process for any other tables for which you want to run log analysis.



Select the date range and statement types you are interested in, as shown below, and click 'Next>'.



Click on the 'Generate JCL' button, as shown below, and then click 'Yes' to the pop-up. Then click 'Next>'.



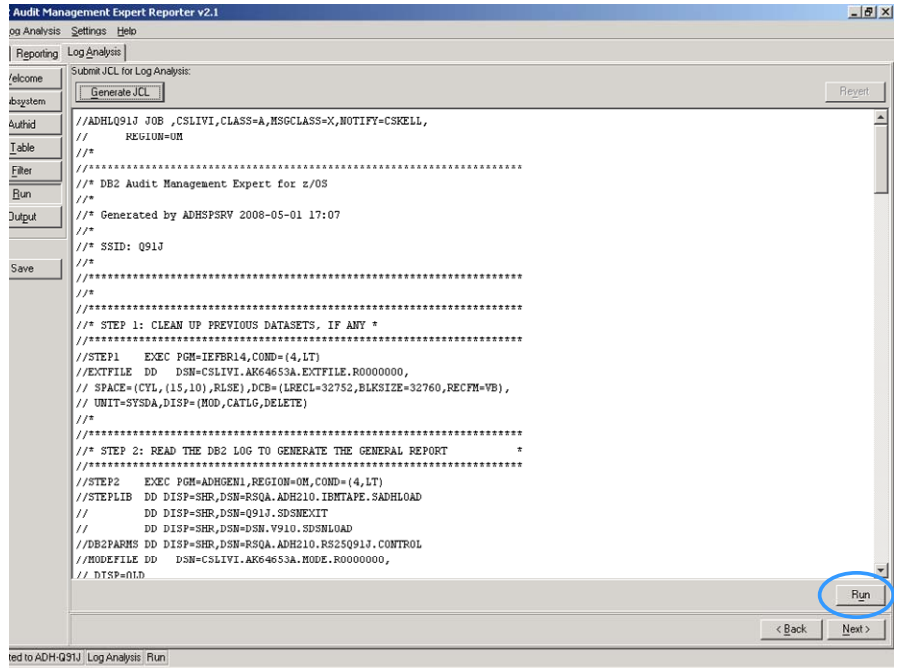
To save the report template, click the 'Save' tab on the middle-left and give the report a name.

When you load a saved template, it will pull back all the settings you made in the wizard. Loading the template will not submit the JCL. (Depending where you were in the wizard when you saved, JCL may or may not have been even generated.) Dates can then be modified before generating the new JCL.

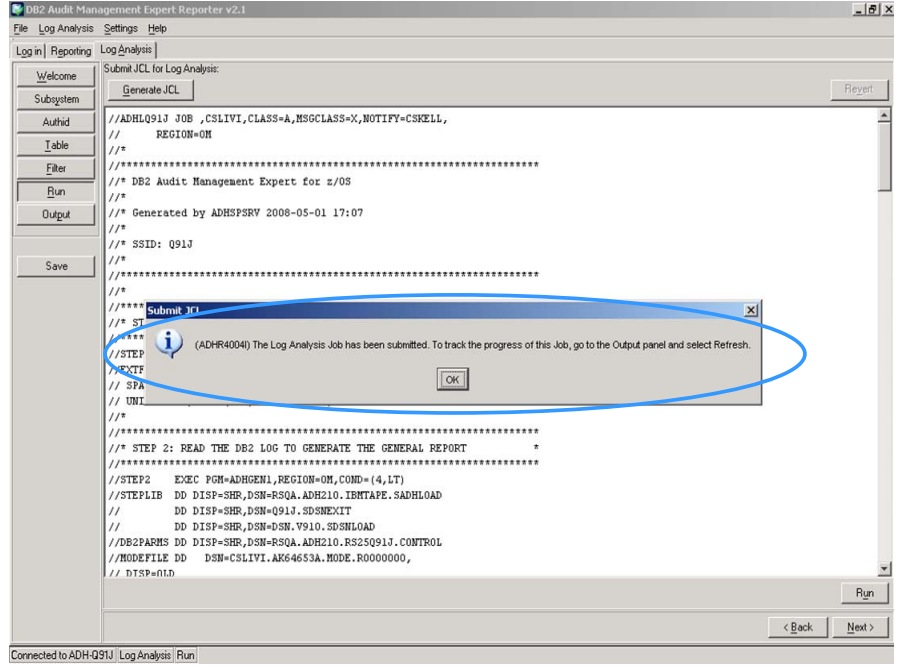
Click 'Run' on the lower right as shown below.

The jobcard used for Log Analysis can be set up by the Administrator in the Administration User Interface under the 'Agents' tab using the Agent Editor. On the left hand side of the screen, select 'JCL' and add a job card that auditors will have the authority to use. Add the job card in the box to the right of 'Log Analysis JCL Job Card'. In this example, the Log Analysis jobcard was set up in agent.

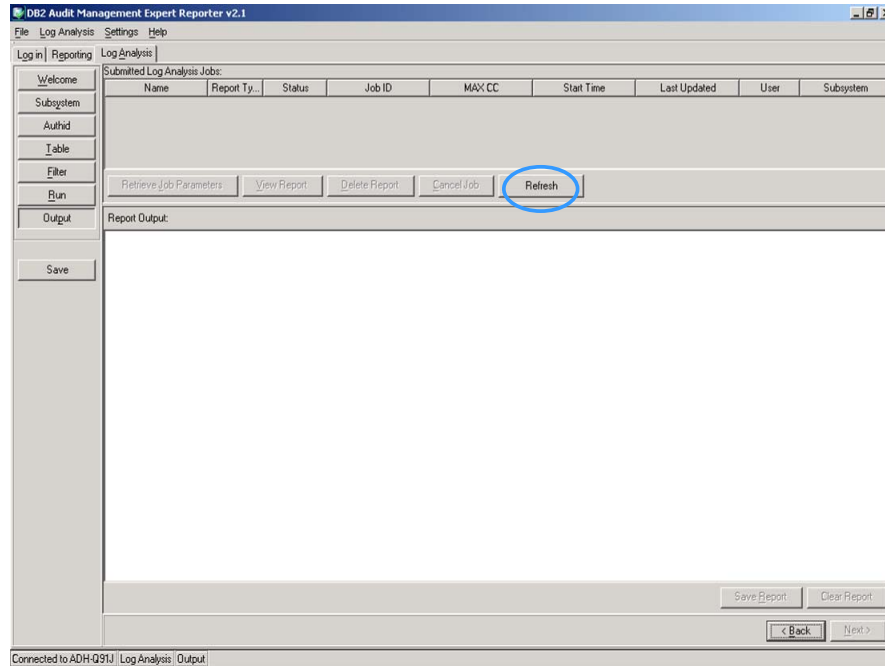
If no Log Analysis Job card is defined in the Agents tab, the Log Analysis job is built using a default jobcard. Click the 'Run' button in the lower right hand corner and respond 'Yes' to the pop up that asks you 'Are you sure you want to submit the JCL?'. You will then be prompted with a pop up that asks you for your TSO User ID and password.



After you click 'Run', the following pop-up appears, as shown below, verifying you really want to run it. Click 'OK'.

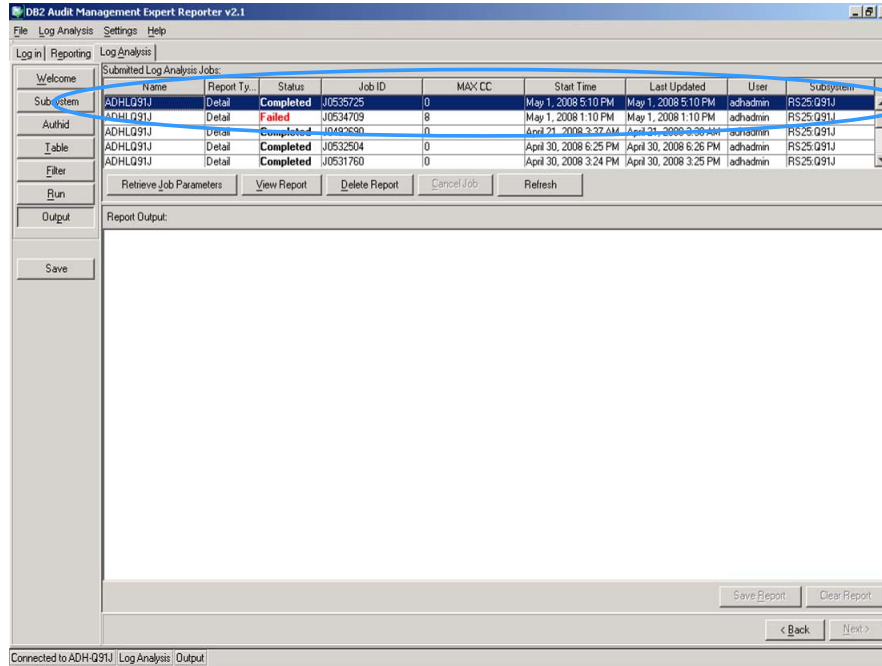


Go to the 'Output' button on the left hand side of the screen, as shown below. Then click 'Refresh' in the middle of the screen to refresh the data. If nothing is there, the job is still running. Allow the job time to finish, and then click 'Refresh' again.

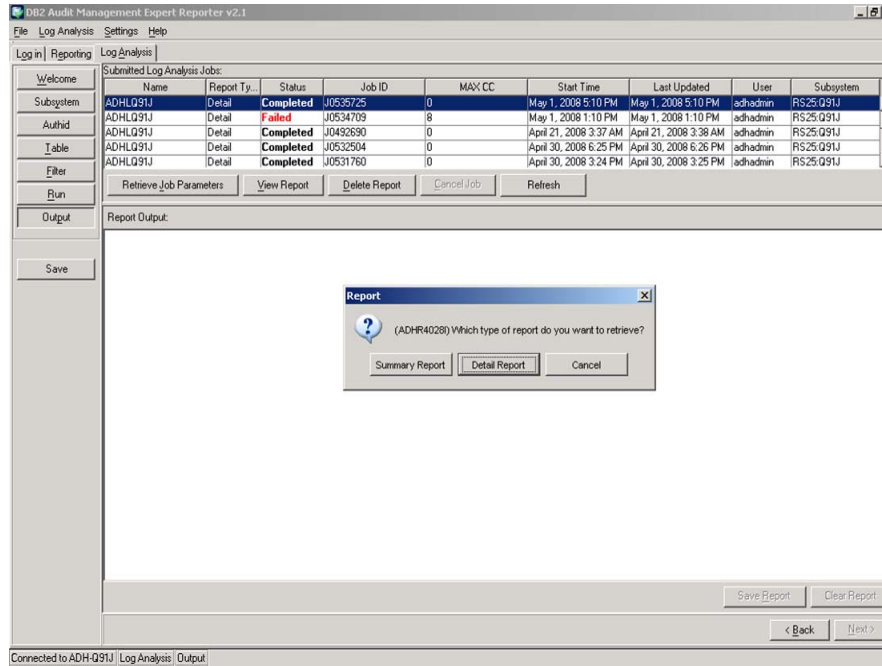


Highlight the log analysis run you are interested in, as shown below, and click on the 'View Report' tab.

Note: if the list contains previous runs, this does not necessarily mean the data is still available. A table in the repository contains information about each run, but the sysout may have been deleted. This is site specific.



Select either the Summary Report or Detail Report shown below.



Summary report

The screenshot shows the 'DB2 Audit Management Expert Reporter v2.1' interface. The 'Log Analysis' tab is active, displaying a table of submitted log analysis jobs. The 'Report Output' pane shows a summary report for job Q91J.

Name	Report Ty.	Status	Job ID	MAX CC	Start Time	Last Updated	User	Subsystem
ADHLG91J	Detail	Completed	J053725	0	May 1, 2008 5:10 PM	May 1, 2008 5:10 PM	adhadm	RS25 Q91J
ADHLG91J	Detail	Failed	J0534709	8	May 1, 2008 1:10 PM	May 1, 2008 1:10 PM	adhadm	RS25 Q91J
ADHLG91J	Detail	Completed	J0492690	0	April 21, 2008 3:37 AM	April 21, 2008 3:38 AM	adhadm	RS25 Q91J
ADHLG91J	Detail	Completed	J0532504	0	April 30, 2008 6:25 PM	April 30, 2008 6:26 PM	adhadm	RS25 Q91J
ADHLG91J	Detail	Completed	J0531760	0	April 30, 2008 3:24 PM	April 30, 2008 3:25 PM	adhadm	RS25 Q91J

```

DB2 LOG ANALYSIS- SUMMARY REPORT: Q91J
*****

LOG RANGE
-----
START DATE   : 2008/05/01
START TIME   : 06:20:45
END DATE     : 2008/05/01
END TIME     : 14:20:46

FILTERS
-----
SHOW UPDATES : Y
SHOW INSERTS : Y
SHOW DELETES : Y
SHOW ROLLBACKS : N
CATALOG DATA : Y
INCLUDE-TABLE..... PRDA01.CSAUD1
INCLUDE-TABLE..... CREDIT_AUTH_SYS.CSCART
INCLUDE-AUTHID..... CSKELL
INCLUDE-AUTHID..... CSREGG
    
```

Detail report

The screenshot shows the 'DB2 Audit Management Expert Reporter v2.1' interface. The 'Log Analysis' tab is active, displaying a table of submitted log analysis jobs. The 'Report Output' pane shows a detail report for job Q91J.

Name	Report Ty.	Status	Job ID	MAX CC	Start Time	Last Updated	User	Subsystem
ADHLG91J	Detail	Completed	J053725	0	May 1, 2008 5:10 PM	May 1, 2008 5:10 PM	adhadm	RS25 Q91J
ADHLG91J	Detail	Failed	J0534709	8	May 1, 2008 1:10 PM	May 1, 2008 1:10 PM	adhadm	RS25 Q91J
ADHLG91J	Detail	Completed	J0492690	0	April 21, 2008 3:37 AM	April 21, 2008 3:38 AM	adhadm	RS25 Q91J
ADHLG91J	Detail	Completed	J0532504	0	April 30, 2008 6:25 PM	April 30, 2008 6:26 PM	adhadm	RS25 Q91J
ADHLG91J	Detail	Completed	J0531760	0	April 30, 2008 3:24 PM	April 30, 2008 3:25 PM	adhadm	RS25 Q91J

```

DB2 LOG ANALYSIS - DETAILS REPORT: Q91J
*****

ACTION DATE   TIME   TABLE OWNER  TABLE NAME  URID
-----
DELETE 2008-05-01 13.37.59 CREDIT_AUTH_ CSCART  00005A388BC9
SYS

DATABASE TABLESPACE DBID  PSID  OBID  AUTHID  PLAN  CONNTYPE  LRSN
-----
CSKELLD  CSCART##  00274 00007 00008 CSREGG  DSNTPE91 BATCH  C253F02BAA0F

MEMID CORRID  CONNID  LUW=NETID/LUNAME/UNIQUE/COMMIT  PAGE/RID
-----
00000 CSREGGDE  BATCH  ROCKNET1/Q91JDB2 /C253F02B33FB/0001 00000012/07

ROW STATUS  CART_SSN  CART_CARDNUM  CART_EXPDT  CART_STATUS
-----
CURRENT - - - -
POST-CHANGE - - - -
    
```

To save the report output to a text file, click the 'Save Report' tab in the lower right hand corner Save Reports, displays a windows explorer like interface where you save the text report to your local PC.

An example of a report produced by the log analysis feature is shown below.

Example of Log Analysis Output

```

-----
ACTION DATE          TIME          TABLE OWNER  TABLE NAME          URID
-----
UPDATE 2008-05-01 13.45.01 PRDA01          CSAUD1                00005A489000

DATABASE TABLESPACE DBID  PSID  OBID  AUTHID  PLAN          CONNTYPE LRSN
-----
CSKELLDDB CSAUD1##      00274 00002 00014  CSKELL  DSNTPE91 BATCH  C253F1BDC9CB

MEMID CORRID          CONNID          LUW=NETID/LUNAME/UNIQUE/COMMIT          PAGE/RID
-----
00000 CSKELLUP          BATCH          ROCKNET1/Q91JDB2 /C253F1BD24CC/0001 00000002/04

ROW STATUS  AUD1_USER#  AUD1_PERMIT  AUD1_CREATOR  AUD1_TABLE
-----
CURRENT    TSUSR1      R            SUPPORT       CSAUD1
POST-CHANGE TSUSR1      R            SUPPORT       CSAUD1
PRE-CHANGE CSLIMO      R            SUPPORT       CSAUD1

```




© Rocket Software Inc. 2008
© Copyright IBM Corporation 2008

IBM United States of America
Produced in the United States of America
All Rights Reserved

The e-business logo, the eServer logo, IBM, the IBM logo, OS/390, zSeries, SecureWay, S/390, Tivoli, DB2, Lotus and WebSphere are trademarks of International Business Machines Corporation in the United States, other countries or both.

Lotus, Lotus Discovery Server, Lotus QuickPlace, Lotus Notes, Domino, and Sametime are trademarks of Lotus Development Corporation and/or IBM Corporation.

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

Other company, product and service names may be trademarks or service marks of others.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PAPER "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

Information in this paper as to the availability of products (including portlets) was believed accurate as of the time of publication. IBM cannot guarantee that identified products (including portlets) will continue to be made available by their suppliers.

This information could include technical inaccuracies or typographical errors. Changes may be made periodically to the information herein; these changes may be incorporated in subsequent versions of the paper. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this paper at any time without notice.

Any references in this document to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
4205 South Miami Boulevard
Research Triangle Park, NC 27709 U.S.A.
