IBM DB2 Audit Management Expert for z/OS, V.1.1

This brief presentation on DB2 Audit Management Expert highlights the capabilities and value of this new tool from IBM.

Database Security and Auditability

Safeguarding your company's data security is a significant business issue. In recent years, there has been increased demand to track, analyze and report on regulatory compliance. World-wide regulations, for example the Sarbanes-Oxley Act (SOX), have placed a heavy technical burden on IT staff to fulfill auditors' requests. Until now there has not been an easy way for auditors to get the information they need. Manually providing the data that auditors request consumes valuable IT staff time that could be devoted to more strategic activities.

DB2 Audit Management Expert – Overview

To meet this challenge, IBM offers DB2 Audit Management Expert, a comprehensive tool that monitors and collects audit data for DB2 resources, and generates flexible reports on the collected data. DB2 Audit Management Expert eliminates the need to use multiple tools to access multiple systems in order to obtain the required information. DB2 Audit Management Expert separates the roles of auditing and database administration, freeing up valuable resources that are needed to support today's growing number of auditing requests. It does this without requiring that auditors be privileged users on the systems they are auditing. It also ensures that there is no security conflict between the gathering of audited data and the users being audited.

Two Tailored Graphical User Interfaces

DB2 Audit Management Expert provides a graphical user interface that DBAs can use to customize data collection. It also provides a reporting user interface to facilitate common auditing tasks such as determining who updated a particular object in a certain time frame or monitoring authorized access for specific systems or objects. Robust reporting options enable auditors to view and report on data from several perspectives.

Audited Information

DB2 Audit Management Expert can collect and correlate many different types of data, including: modifications to an audited object, reads of an audited object, and capture events in which users may be trying to modify authorization levels. In addition, AME can audit utility access and DB2 commands.

AME provides a wealth of auditing information on your critical DB2 systems. Gathering this information on your own can be time-consuming and involve multiple people in your organization.

Architecture Overview

DB2 Audit Management Expert is based on a client-server architecture.

Scenario: Using DB2 AME to uncover unauthorized access attempts to read and update sensitive data

Now we'll walk through a scenario to show how DB2 Audit Management Expert can help auditors uncover unauthorized access attempts to read and update sensitive data. Let's say the sensitive data in question is an employee table that contains social security numbers and salary information. We'll show how DB2 Audit Management Expert helps the auditors spot unauthorized access attempts, both failed and successful, to this table.

Administration User Interface

Let's begin by looking at the audit data that is being collected. The audit data to collect is defined in a collection profile within Audit Management Expert's Administration user interface. In this scenario, the administrator has already defined a few collection profiles.

Let's look at the one named "Emp Audit Profile", since this one covers the employee table. The profile summary shows the rules that determine how Audit Management Expert performs auditing.

The list of Audit targets/tables shows the objects to be audited. We can see that in this collection profile, auditing is turned on for several tables including the Employee table that contains our sensitive data. For each audited table, we are monitoring the read (or selects) events and the change (insert, update, and delete) events for those tables.

Reporting User Interface

Now let's look at Audit Management Expert's Reporting User interface to see the auditing reports that are generated after the data has been collected. The left side of the Reporting User Interface lists the various report options. You can filter by date, user ID, activity type and threshold.

The right side of the user Interface shows a summary/overview of all the audit activity for a given subsystem. Thresholds can be set by the user in order to flag potential warning and problem situations that would need to be further investigated.

Continuing with this scenario, we're interested in looking at read attempts on the Employee table, so we'll click on Detail, then select the First Read of the Audit Object, which provides a more detailed view of this audit activity. The first graph shows the top five objects that have the most read attempts. (The number of objects shown is a user setting.) Red represents a failed read attempt and green represents a successful read attempt. The Employee table that contains the sensitive data, Emp2, is one of these top objects. The Emp2 table had 4 successful and 3 failed read attempts. Clicking on the Emp2 table will generate a more detailed report for first read audit activity.

The detailed audit activity report shows several interesting things. We can see the time in which the read events were attempted, and the auth ID attempting to read as well as what they were attempting to read: social security numbers. We also see the same auth ID (sfvt008) had several failed read attempts followed by successful read attempts.

Now let's take a look at the First Change of Audited Object activity, that is, any attempt failed or successful to change the data. The graph shows that for the Employee table (EMP2), there were 4 failed change attempts and 1 successful change attempt. In DB2 parlance, changes would be an insert, update, or delete. Clicking on the Employee table will generate a more detailed report for first change audit activity, which can be reviewed online or saved for further review.

The audit activity report shows the time in which the change events (insert, update, or delete) were attempted. We can see the failed and successful change attempts and the auth ID that attempted the change as well as what they were attempting to change (salary and salary rate). We also see the same auth ID (sfvt008) had several failed change attempts followed by a successful change attempt. Now that we have determined that a given auth ID gained unauthorized access to sensitive data, we can use the report to determine how the auth ID gained access in the first place. To do this, we'll look at Explicit Grant and Revoke audit activity.

This report shows the successful and failed grants and revokes (failed grants are shown here in blue and successful in gray). (The color scheme is a user setting.) Clicking on the Table/View data will bring up a more detailed report. The detailed report shows the various grant and revokes that have been made and indicates the associated objects. We can see that all the grants have been made to specific auth IDs except for those on 2 lines. Those grants were made to a group. Also note that these grants pertained to the Employee table, EMP2. From this we're able to gather that the auth ID sfvt008 gained unauthorized access to the sensitive data because access was granted to the group to which that auth ID belonged. These reports can be saved (and printed) if needed.

DB2 Audit Management Expert provides a log analysis feature that allows us to determine what data was modified as a result of the unauthorized access. Let's look at a log analysis report that has been run. The detailed report shows us what data was actually modified (via insert, update, or delete). Each of the modified columns is identified with a special character, ! or #. In this case you can see columns SRATE and SAL were updated. As with all the other reports, these can be saved for review and action can be taken to correct any unwanted modifications to the data.

To recap, we briefly illustrated how DB2 Audit Management Expert can be used to find reveal unauthorized attempts to access sensitive data. We saw first that a collection profile is used to monitor and collect audit data for objects that contain sensitive data. The Reporting UI showed the various access attempts. Finally, we saw how a user with a particular auth ID gained the unauthorized access and we determined what data was modified as a result of the access.

Summary

To summarize, DB2 Audit Management Expert facilitates common auditing tasks, empowers auditors by allowing them to obtain the information they need, provides comprehensive reporting facilities and filtering policies for data collection.

Conclusion

DB2 Audit Management Expert is an important new tool that helps your company comply with regulations while saving time and expense in the data center. It is one of the tools that comprise IBM's regulatory compliance tools suite. For more information about this and other tools in the regulatory compliance suite, see the IBM DB2 Audit Management Expert website:
http://www.ibm.com/software/data/db2imstools/db2tools/db2ame-zos/