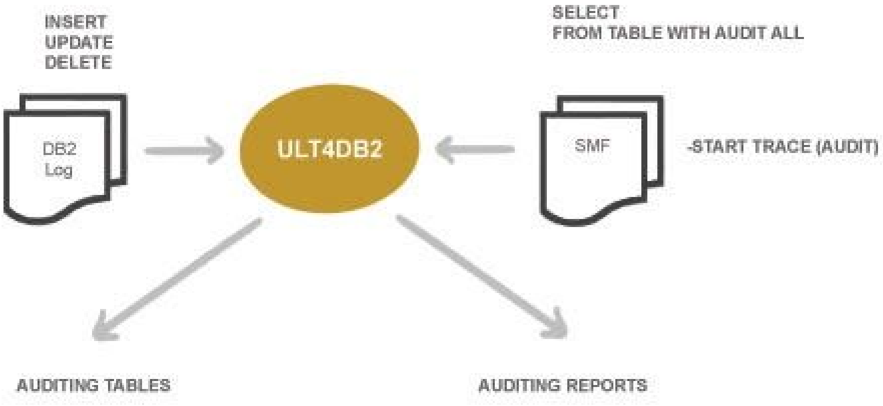
ULT4DB2

AUTOMATING LOG ANALYSIS

Auditing

Log analysis allows you to track changes made to tables and identify details related to each change such as the user id, the plan name, connection id and correlation id, timestamp and the changed data. These details can help in investigating who made a change, when and how the change was made, and what exactly was changed. Investigation is easier when you can use SQL to run queries and reports. ULT4DB2 allows you to generate flat files and matching load statements to load the auditing information into target auditing tables. ULT4DB2 execution can be restarted to resume log tracking from the end log point analyzed in the previous execution. This way no change is left without being audited. The auditing information can be loaded into matching auditing tables, including all the columns of the audited table plus additional auditing columns. These tables can be created automatically. If new columns are added to the audited tables, the new columns can be also added automatically to the auditing tables. The entire process of analyzing the logs, generating the auditing files and finally, creating and loading the auditing tables is fully automated and integrated. Immediately after executing the log analysis job, you can run your SQL queries or reports to investigate the changes made on your audited tables.

Since the DB2 logs record only update activity, it is necessary to use the audit trace to get a complete picture of all types of access, including read access. ULT4DB2 can analyze both the DB2 log and audit trace records and allow you to see who made changes when and how and also who accessed the data, when and how. This way you can detect suspicious activity against critical tables. In addition, you can identify read-only tables and tables that are no longer in use.



Propagation

Log analysis allows you to propagate changes on source tables. ULT4DB2 can generate REDO SQL to apply the changes on your target tables. This way you can keep source and target tables in sync. To synchronize tables, a point of reference must be created. This is a point in time when the data in both the source and target tables is exactly the same. Only then can any change made on the source table can be propagated to the target table. To achieve a point of reference, the target tables can be loaded or initialized using the data in the source tables. ULT4DB2 allows the use of the last image copies to create a point of reference. You can unload all the last full image copies of your source tables and then reload the data into your target tables. ULT4DB2 can then generate REDO SQL starting from the log point recorded for each image copy. Alternatively, ULT4DB2 allows you to start all your source tables in read-only before unloading the data directly from your source tables. This way, data consistency can be preserved and target tables can be synchronized. Following the first synchronization, ULT4DB2 can analyze the logs repeatedly and frequently to propagate all changes made on the source tables.

Quiet Points

Log analysis detects logical units of recovery and quiet points, periods of no activity against a group of objects that can be used as points of consistency. The user can then select a valid point of consistency for recovery and generate recovery jobs. Often QUIESCE is used to set a point of consistency in signifcant buisness points in time. However, sometimes it is required to recover to a point in time that has not been recorded using QUIESCE. ULT4DB2 can detect a quiet point when requesting to recover objects to a point in time that is not known as a point of consistency for a group of objects.