HPE Shadowbase Solution Brief

Shadowbase Audit Compliance Reporting and Analysis

Ensure Audit Compliance and Database Consistency

Audit compliance has become an increasingly important part of most businesses. Failure to meet compliance requirements can result in heavy fines, or even suspension of operations.

Fraudulent activity can result in significant costs if left unchecked. It is imperative that you know what data is being changed, when, how, and by whom. Fortunately, Shadowbase solutions include products to address these important requirements.

HPE Shadowbase Audit Log (SAL) software creates a searchable historical archival log of transactional activity, recording all inserts, updates, and deletes to the files and tables being monitored in a reporting database for application change data auditing purposes. This software can satisfy *proof of performance* requirements, proving in a log that a transaction happened.

The HPE NonStop TMF audit trail records all changes made to the system's audited database files and tables. HPE Shadowbase Audit Reader (SAR) software allows the user to selectively mine this activity to review the change details and produce reports on the activity.

Shadowbase Audit Log Software

Figure 1 shows a sample SAL architecture, where transactions from the production application modify the source database, with the changes being captured in the TMF Audit Trail. Shadowbase Collector, Consumer, and Database of Change (DOC) Writer extracts, transforms, replicates, and stores these changes in the DOC database on the target. Then, SAL extracts these changes and replicates them to the SAL Replay Server, and then the SAL DB target database, recording each activity as a separate row with details of the data that changed.

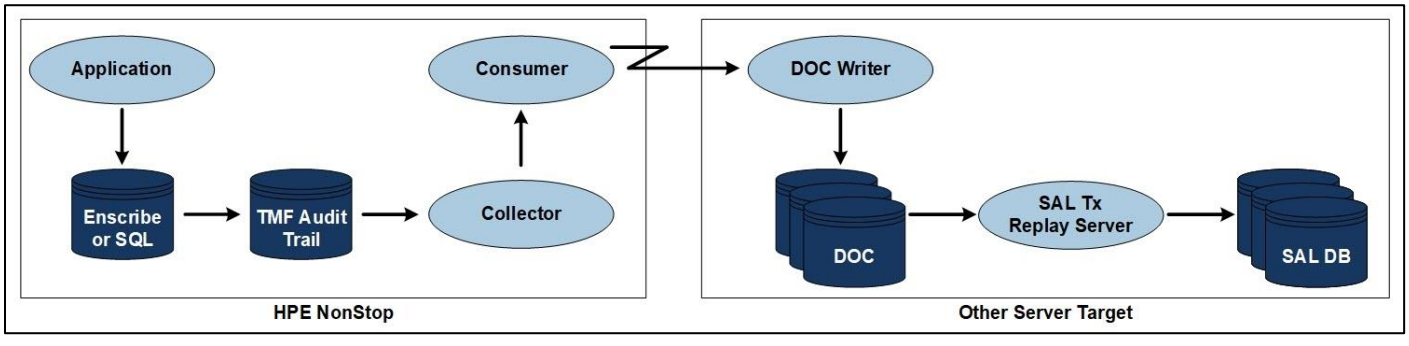

Figure 1 – Shadowbase Audit Log Architecture

SAL is available for the HPE NonStop Server platform as a source (Enscribe, NonStop SQL/MP, and NonStop SQL/MX), and the archival reporting database is created on an off-platform target database (e.g., Oracle or SQL Server). This archival reporting database enables searching and reviewing historical data that was changed, and when, using a simple and powerful query language.

Shadowbase Audit Reader Software

Investigate How Data is Being Changed

Analyze both current and historical transactional information using a variety of search criteria. All of these features are available using a simple and easy to learn command line interface.

Figure 2 shows a sample SAR architecture, where the application makes transactional changes to the source database, the TMF Audit Trail collects these changes, and SAR mines these changes for display and querying/reporting. This software allows the user to determine what data was changed, and when, using the TMF audit trail as the "database."

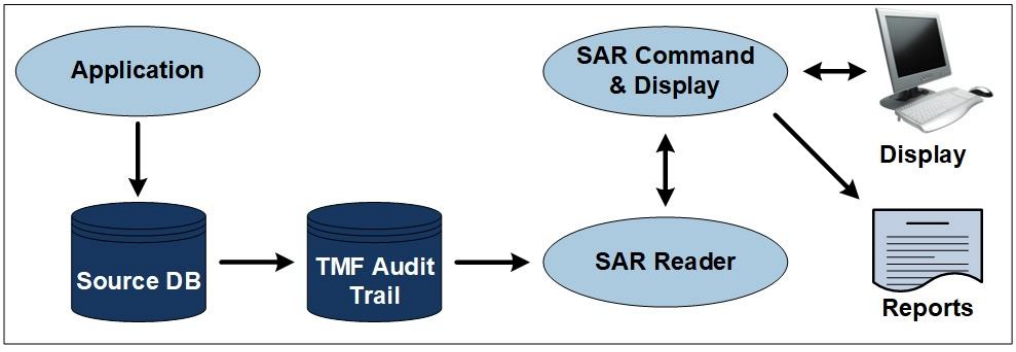

Figure 2 – Shadowbase Audit Reader Architecture

Analyze Database Change Results of an Application

When used during the development of code, for example, you can learn the exact order or sequence in which the application applies changes to a database. These I/O executions can be analyzed to make sure the code is producing results based upon the correct implementation of the intended design algorithm or business rule.

Analyze the TMF Audit Trail for Problem Areas and Assist in Remediating the Database When Discovered

Another use for SAR is to analyze the TMF audit trail contents to determine where application problems may have occurred and assist in the remediation of the database when these problems are discovered. It is particularly useful for vendor-supplied software (i.e., for cases where you do not have access to the source code) so that you can see exactly how the application is changing the database for each transaction it performs.

Write Simple Queries Against the Audit Trail for the Timeframe and Enscribe File or SQL Table in Question

SAR allows you to query the audit trail by timestamp, transaction id, or type of statement (insert, update, delete, transactional boundary-begin commit, etc., for local and network events). It permits the assignment of Data Definition Language (DDL) data format for Enscribe I/O events, uses the SQL table schema for SQL events, and provides the ability to display the output data in a variety of views and formats, showing both the before and after images of the change that was performed by the application. SAR also optionally reads "foreign" audit (audit generated on another HPE NonStop Server system) and supports both Enscribe and NonStop SQL I/O events.

SAR is a Powerful Utility for Displaying the Transactional Activity that Changed your Database

It is particularly useful for understanding how and when the database changes occur, and for analyzing the before and after values of every insert, update, and delete that was applied against your data.

When Using SAR

- Understand how your applications and the file system are affecting your database
- Find long-running transactions, and transactions that have damaged your database
- Recover lost or corrupted data (when used with optional Shadowbase components)
- Find transactions matching almost any given criteria, like those setting an account balance to values below or above thresholds
- Detect bugs in applications by analyzing transaction contents
- Isolate application performance bugs by understanding the audited disk activity

- Product reports of all activity that is changing your data

SAL Example

Problem

Within an application, one transaction creates an account (as in insert operation) with an initial balance of $1,000, another transaction transfers the balance to another account (via an update operation), and a third transaction deletes the account. In the end, the source database has no knowledge of the removed account – it has been removed. How can this activity be saved without interfering with the application's operations?

Solution

Configure SAL, and it will automatically log the I/O's for the three transactions as three separate rows in its historical/archival database:

1. The creation of the account with the initial balance (preserving the inserted "before image" values)
2. The transfer of the balance to another account (preserving the updated "after image" values)
3. The removal of the account (preserving the deleted "before image" values)

Each of these entries in the SAL database can subsequently be queried to find specific information.

SAR Examples

Problem #1

Find all transactions for any account that exceeded $2,000,000 between 9:00 November 4th and 16:00 November 5th, 2019.

Assume
The SQL table TRANSTBL holds the transaction detail information for a checking account banking application and TRANS_AMOUNT is the transaction amount column.

Solution

```
STARTTIME 2019-11-04:09:00:00
ENDTIME 2019-11-05:16:00:00
SELECT *
FROM TRANSTBL
WHERE TRANS_AMOUNT > 200000.00;
RUN
```

Note
This query will return any and all times the transaction amount exceeded $2,000,000, regardless of the number of times it did so for any account during that interval. This query will also return all DML including any INSERT, UPDATE, and/or DELETE events where the transaction amount exceeded $2,000,000.

Problem #2

List ALL events in one of the transactions returned in the prior query.

Assume
The selected transaction identifier is \NODE.CPU.NNNNN

Solution

```
ADD TRANSACTION \NODE.CPU.nnnnn;
RECORD TYPE ALL;
```

```
SELECT * FROM TRANSTBL;
RUN
```

Problem #3

An errant batch program started at 03:00 and accidentally deleted rows from the TRANSTBL. List the account number (ACCT_NUM) and business transaction ID (BTX_ID) columns for all deleted rows for this table.

Solution

```
STARTTIME 03:00:00
RECORD TYPE DELETE;
SELECT ACCT_NUM, BTX_ID
FROM TRANSTBL;
RUN
```

Note
This output provides the customer account details to allow you to recover the deleted information.

Summary

Data replication is at the heart of the HPE Shadowbase product portfolio. However, it is also important to be able to monitor and query that data in order to detect anomalous behavior, ensure continuation of proper business operations, and for audit compliance and regulatory purposes. Shadowbase SAL and Shadowbase SAR software provide the necessary features to address these needs.

Learn more:
shadowbasesoftware.com
hpe.com

Contact us:

Gravic, Inc.
17 General Warren Blvd Malvern,
PA 19355-1245 USA
Tel: +1.610.647.6250
Fax: +1.610.647.7958
Email Sales: shadowbase@gravic.com
Email Support: sbsupport@gravic.com

Please follow: