

HPE Shadowbase Audit Compliance Reporting and Analysis



Ensure Audit Compliance and Database Consistency

Audit compliance is an important and growing part of business. Failure to meet compliance requirements can result in heavy fines, significant disruptions, or even business closure.

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, HPE Shadowbase Audit Compliance solutions address these requirements.



HPE NonStop Shadowbase Audit Log (SAL) software monitors files and tables for transactional activity (such as inserts, updates, and deletes), creating and updating an archival database describing the changes. This database can serve as a reporting database that includes a history or archive of the changes made on an existing operational database. This reporting database can be searched via SQL queries, to satisfy a variety of business needs, such as proof of performance requirements, or for providing a searchable database for specific record changes.

HPE NonStop Shadowbase Audit Reader (SAR) software allows the user to selectively mine HPE NonStop TMF audit trail activity to review database changes and generate reports. SAR is similar to HPE's SNOOP utility, but is much more powerful for querying and displaying the audited file and table activity.

HPE Shadowbase Audit Log Software

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

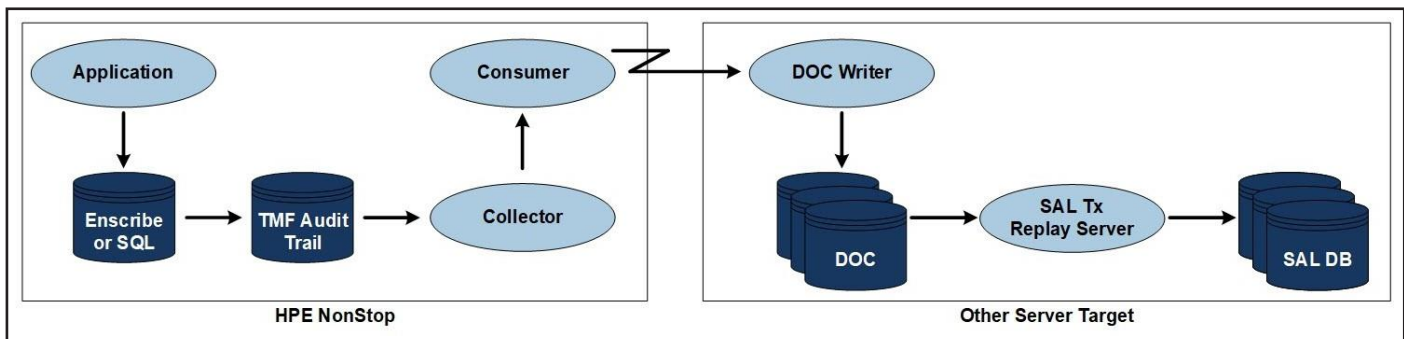


Figure 1 – HPE Shadowbase Audit Log Architecture

SAL is available for the HPE NonStop Server platform as a source, capturing Enscribe, NonStop SQL/MP, and NonStop SQL/MX database changes, 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 change data operations, showing what was changed and when, using a simple and powerful query language.

HPE NonStop Shadowbase Audit Reader Software

Investigate How Data is Being Changed

SAR enables users to 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. The application makes transactional changes to the source database. The TMF Audit Trail collects these changes, and SAR mines them for display and querying/reporting. SAR allows the user to determine what data was changed and when, via referencing the TMF audit trail.

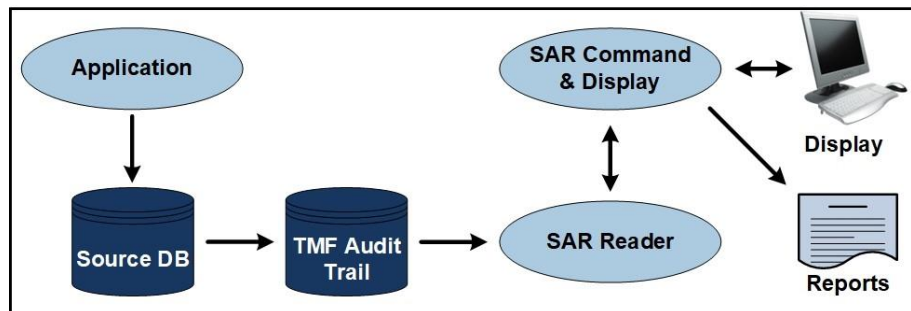


Figure 2 – HPE Shadowbase Audit Reader Architecture

Powerfully Search and Review Transactional Activity to Analyze the Application's Database Changes

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) to see exactly how each transaction affects the database.

Write Simple Audit Trail Queries by Specifying the Timeframe and File or Table in Question

SAR enables querying the audit trail by timestamp, transaction id, file or table name, or type of statement (DML events such as INSERTs, UPDATES, DELETES and transactional boundary such as BEGINs, COMMITs, etc., for local and network events). You can specify the Data Definition Language (DDL) data format for Enscribe I/O events, and the SQL table schema for SQL events. Output data can then be displayed in a variety of views and formats, showing before and after images of the application changes. SAR also optionally reads "foreign" audit (audit generated on a different HPE NonStop system) and supports both Enscribe and NonStop SQL I/O events.

Key Benefits

- Understand how your applications and file systems are affecting your database
- Find long-running ("hanging") transactions, and transactions that damage your database
- Recover lost or corrupted data (when used with other Shadowbase add-on components such as Shadowbase UNDO)
- Filter transactions based on thresholding, such as those that cause account balances to reach upper or lower limits
- Detect application bugs by analyzing transaction contents
- Isolate application performance bugs by gaining insight from audited disk activity
- Produce reports on all change data activity

SAL Example

Problem

An application processes a transaction that creates an account (an INSERT operation) with an initial balance of \$1,000. A second transaction transfers the balance to another account (an UPDATE operation), and a third transaction DELETES the account. Afterwards, the source database has no record of the removed account. How can this activity be saved without affecting the application?

Solution

Configure SAL, and it automatically logs 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)

Then, each of these entries in the SAL database can be queried.

SAR Examples

Problem #1

Find accounts with any transactions exceeding \$2,000,000 between 9:00 AM November 4th and 16:00 PM November 5th, 2024.

Assume

In this example, 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 2024-11-04:09:00:00
ENDTIME 2024-11-05:16:00:00SELECT
*
FROM TRANSTBL
WHERE TRANS_AMOUNT > 2000000.00;
RUN
```

Note

This query will return any and all times transaction amounts exceeded \$2,000,000 regardless of the number of times it did so for any single account during that interval. This query will also return all DML events including 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 AM and accidentally deleted rows from the TRANSTBL. List the account number (ACCT_NUM) and business transaction ID (BTX_ID) columns for the rows that were deleted from 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, enabling you to recover the deleted account data.

Summary

HPE Shadowbase software performs powerful data replication capabilities. HPE Shadowbase Audit Log and Audit Reader enable users to monitor and query the database's change data in order to detect anomalous behavior, ensure the business runs smoothly, and to meet audit compliance and regulations.

Hewlett Packard Enterprise globally sells and supports Shadowbase solutions under the name HPE Shadowbase. For more information, please contact your local HPE Shadowbase representative or visit our website. For additional information, please view our Shadowbase solution videos: <https://vimeo.com/shadowbasesoftware>.

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:



Copyright © 2016, 2018, 2020, 2024 by Gravic, Inc. Gravic, Shadowbase and Total Replication Solutions are registered trademarks of Gravic, Inc. All other brand and product names are the trademarks or registered trademarks of their respective owners. Specifications subject to change without notice.