SQL Server Audit (Database Engine)[[1]](#footnote-1)

Audit trong phiên bản Microsoft SQL server 2016 có một số cải tiến đáng kể về CDC và Temporal Tables, đem lại khả năng tốt hơn cho quản trị server.

Chúng ta đôi lúc có nghe nói về một vài trường hợp nhân viên bệnh viện xem lén hồ sơ bệnh án của những người nổi tiếng. Trong nhiều trường hợp, các nhân viên này có lí do chính đáng để truy cập hồ sơ đó. Việc xác định hành vi của nhân viên đó có đang bị lạm dụng hay không trở nên rất phức tạp. Và tất nhiên, ban quản lí của bệnh viện cũng không thể thu hồi quyền truy cập của nhân viên đó tới cơ sở dữ liệu do còn rất nhiều bệnh nhân khác.

Nếu chúng ta không thể ngăn nhân viên truy cập dữ liệu trái phép, chúng ta có thể theo dõi cách nó đang được sử dụng. Sau đó dựa trên kết quả này để xác định có hành vi đáng ngờ nào dẫn tới vi phạm hay không, quy mô và bản chất của vi phạm. Chính vì vậy Microsoft đã thêm tính năng Audit vào các phiên bản SQL Server từ phiên bản 2008 trở đi.

SQL Server Auditing có được Microsoft giới thiệu thông qua một số kĩ thuật:

# Manual auditing

Điều này có thể liên quan đến một tập hợp các truy vấn và có thể là báo cáo để theo dõi hoạt động trên mỗi bảng, giao dịch của người dùng, các thay đổi gần đây đối với các bảng nhạy cảm, v.v. Tuy nhiên, ngoài việc tốn thời gian, hầu như không thể chia tỷ lệ này cho tất cả các sự kiện kiểm toán có thể có.

# SQL Server Extended Events

Là sự thay thế cho SQL Server profiler and traces (từ trước phiên bản 2008), Extended Events cung cấp một số lợi thế bao gồm các công cụ GUI được tích hợp sẵn và có khả năng hoạt động tốt hơn. Extended Events có thể kiểm tra một loạt các hành động, nhưng mắc phải một số thiếu sót như không thể cung cấp thông tin về những gì đã bị xóa hoặc chèn. Ngoài ra, không có phương tiện nào để kiểm tra trước và sau để so sánh các giá trị mới và cũ cho các bản cập nhật.

# SQL Server triggers

SQL Server triggers là một trong những công cụ được đánh giá khá mạnh trong một khoảng thời gian dài. SQL Server triggers có thể được thiết lập dễ dàng và có khả năng theo dõi nhiều loại thông tin. Trigger cũng cho phép người quản trị có khả năng tùy chỉnh và tạo ra kho lưu trữ thông tin Audit của riêng họ. Tuy nhiên Trigger là một công nghệ dựa trên Hook và có thể gây ra lỗi trong quá trình thực thi. Tính năng này không được khuyến nghị sử dụng trên các bảng có khối lượng truy vấn lớn do vấn đề hiệu năng và thời gian sử lí khá tệ của Hook.

Có hai loại template Trigger được Microsoft giới thiệu là DDL Trigger và DML Trigger.

# SQL Server transaction logs

SQL Server transaction logs giống như hộp đen của máy bay. Nó sẽ ghi lại mọi thứ xảy ra, không chiếm quá nhiều hiệu năng vì đây đã là một quy trình tích hợp sẵn trong SQL Server. Nhưng các tệp logs này nổi tiếng là khó đọc do chúng được ghi dưới dạng binary và chỉ có SQL Server được tích hợp sẵn để đọc chúng. Việc build các công cụ khác để đọc chúng cho mục đích report, phân tích trở nên rất khó khăn.

# SQL Server Audit

Tính năng này đã xuất hiện từ SQL Server 2008 và cung cấp các khả năng kiểm tra thô sơ, “tổng hợp” như ai đã thực hiện thay đổi và khi nào, nhưng không cung cấp thông tin khác, mà ngày nay sẽ được coi là cần thiết, giống như những gì thực sự thay đổi.

# Change tracking

Tính năng SQL Server này là một tiến so với SQL Server Audit nhưng yêu cầu một số kinh nghiệm và hiểu biết về cấu trúc bảng bên dưới và chỉ theo dõi các thay đổi đối với khóa chính, khiến nó không hữu ích cho bất kỳ điều gì khác ngoài kiểm tra rất hời hợt.

# Change data capture (CDC)

Đây là cải tiến của SQL Server về Change tracking và có sẵn trong phiên bản Standard kể từ SQL Server 2016. CDC cung cấp khả năng kiểm tra và thông tin tốt hơn nhiều so với Change tracking nhưng thiếu giao diện người dùng để giúp việc xem và xử lý thông tin dễ dàng. Kiến thức T-SQL sẽ được yêu cầu để truy vấn các bảng và lấy thông tin.

# Temporal tables

Đây là một tính năng khác mà SQL Server đã giới thiệu cung cấp giải pháp miễn phí cho CDC. Với bảng thời gian, bạn có thể xem toàn bộ lịch sử thay đổi và nó cũng có thể được sử dụng cho mục đích khôi phục. Tính năng này yêu cầu tạo bảng lịch sử cho mỗi bảng kiểm tra và yêu cầu tương tác với T-SQL để xem kết quả.

Việc sử dụng tính năng nào phụ thuộc vào yêu cầu kiểm tra, thời gian thiết lập và duy trì các đường kiểm tra, cũng như các yêu cầu về lưu trữ, bảo mật và báo cáo.

1. <https://www.sqlshack.com/various-techniques-to-audit-sql-server-databases/> [↑](#footnote-ref-1)