# LO#03: 1049-1056

## Lệnh DBCC

Các lệnh của Trình kiểm tra tính nhất quán của cơ sở dữ liệu (DBCC) có thể cung cấp thông tin chi tiết có giá trị cho các nhà điều tra về các hoạt động diễn ra trong hệ thống máy chủ. Lệnh DBCC LOG cho phép điều tra viên xem và truy xuất các tệp nhật ký giao dịch đang hoạt động cho một cơ sở dữ liệu cụ thể.

**Syntax: DBCC LOG(<databasename >, <output >)**

*Tham số đầu ra chỉ định mức thông tin mà điều tra viên muốn truy xuất*

0 = thông tin tối thiểu của từng hoạt động như LSN hiện tại, Hoạt động,

ID giao dịch, v.v.

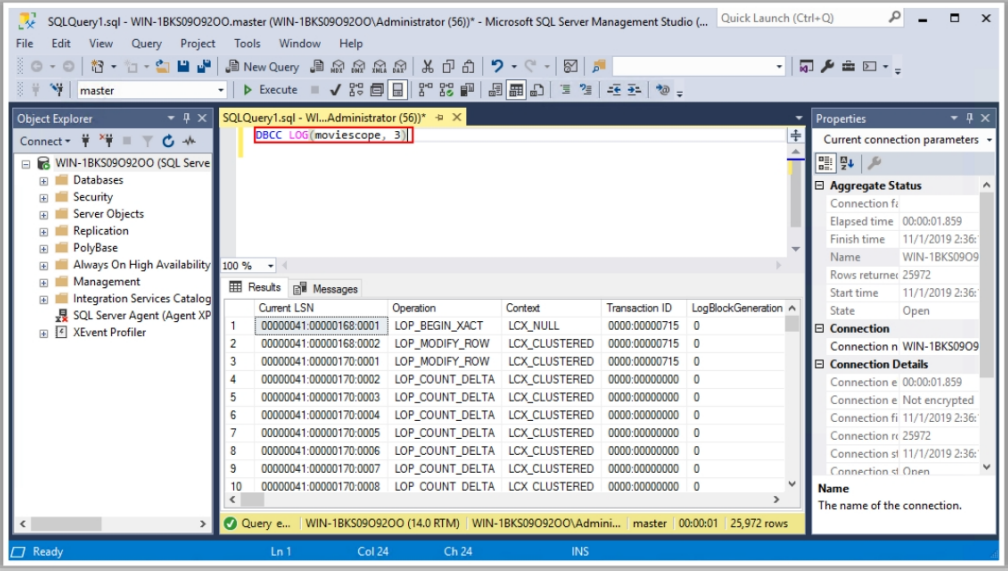
1 = nhiều thông tin hơn 0 một chút, chẳng hạn như Bit cờ và LSN trước đó

2 = thông tin chi tiết, bao gồm (AllocUnitId, id trang, id vị trí, v.v.)

3 = thông tin đầy đủ về từng thao tác

4 = thông tin đầy đủ về từng hoạt động cùng với kết xuất hex của hàng giao dịch hiện tại

Đưa ra truy vấn **DBCC LOG(moviescope, 3)** để xem tệp nhật ký giao dịch cho cơ sở dữ liệu moviescope, với thông tin chi tiết cho từng thao tác:



Hình 11.8: Sử dụng lệnh DBCC LOG

Sau đây là các lệnh DBCC khác cho phép điều tra viên lấy thông tin bổ sung liên quan đến cơ sở dữ liệu được chỉ định:

**DBCC DBTABLE**: Trả về cấu trúc của bảng cơ sở dữ liệu đã chọn

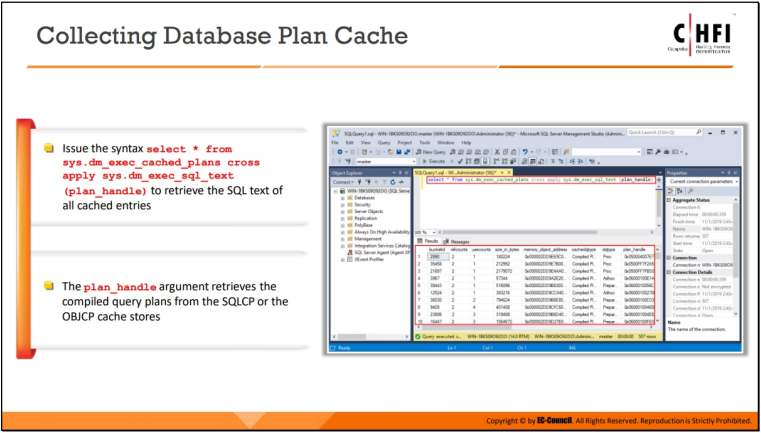
**DBCC DBINFO**: Trả về thông tin liên quan đến siêu dữ liệu cơ sở dữ liệu

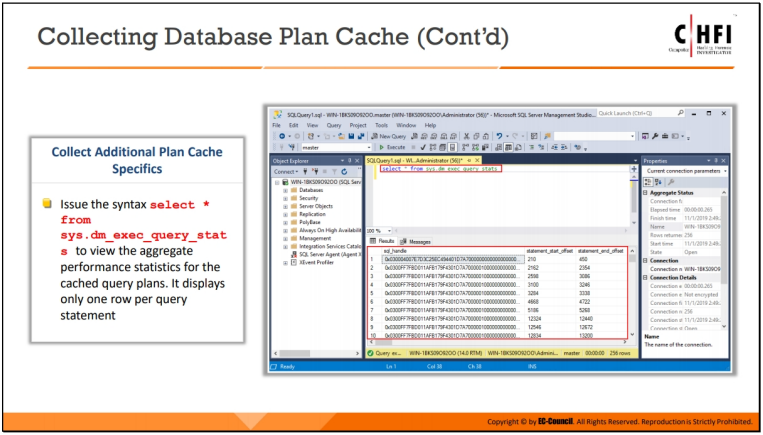
**DBCC PROCBUF**: Trả về nội dung của bộ đệm thủ tục SQL Server. Bộ đệm chứa các câu lệnh thực thi được lưu trong bộ nhớ cache của SQL Server, chẳng hạn như các thủ tục được lưu trữ và các truy vấn SQL.

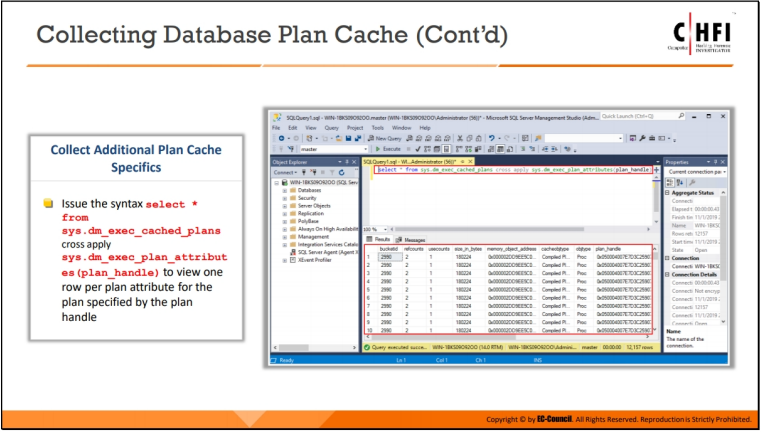
**DBCC CACHE**: Trả về tiêu đề bộ đệm và các trang từ bộ đệm bộ đệm SQL Server nơi lưu trữ kết quả

**DBCC SHOWFILESTATS**: Trả về thông tin liên quan đến không gian bị chiếm bởi các tệp dữ liệu trong cơ sở dữ liệu đang hoạt động

**DBCC PAGE**: Trả về cấu trúc trang dữ liệu của cơ sở dữ liệu đã chọn







## Thu thập bộ đệm gói cơ sở dữ liệu

*Để thu thập bộ đệm gói cơ sở dữ liệu, truy vấn sau đây được sử dụng:*

**select \* from sys.dm\_exec\_cached\_plans cross apply**

**sys.dm\_exec\_sql\_text(plan\_handle)**

Việc phát hành **sys.dm\_exec\_cached\_plans** theo cú pháp sẽ trả về một hàng cho từng gói truy vấn được SQL Server lưu vào bộ nhớ cache để tăng tốc thực thi truy vấn. Chế độ xem quản lý động này sẽ giúp người dùng

tìm các gói truy vấn được lưu trong bộ nhớ cache, văn bản truy vấn được lưu trong bộ nhớ cache, dung lượng bộ nhớ mà các gói đã lưu trong bộ nhớ cache chiếm dụng và số lần sử dụng lại của các gói đã lưu trong bộ nhớ cache.

Lệnh truy xuất văn bản SQL của tất cả các mục được lưu trong bộ nhớ cache. Lưu ý rằng đối số **plan\_handle** trong cú pháp xác định duy nhất một kế hoạch truy vấn cho một đợt được lưu vào bộ đệm ẩn hoặc hiện đang được thực thi bởi máy chủ. Đối số **plan\_handle** truy xuất các kế hoạch truy vấn đã biên dịch từ các kho lưu trữ bộ đệm ẩn SQLCP hoặc OBJCP.

Để thu thập các chi tiết cụ thể về bộ đệm của gói bổ sung từ cơ sở dữ liệu, chẳng hạn như xem thống kê hiệu suất tổng hợp, truy vấn sau đây được sử dụng:

**select \* from sys.dm\_exec\_query\_stats**

Kết quả chứa một hàng cho mỗi câu lệnh truy vấn trong gói được lưu trong bộ nhớ cache và thời gian tồn tại của các hàng được đính kèm với chính gói đó. Khi một kế hoạch bị xóa khỏi bộ đệm, các hàng tương ứng sẽ bị xóa khỏi chế độ xem này.

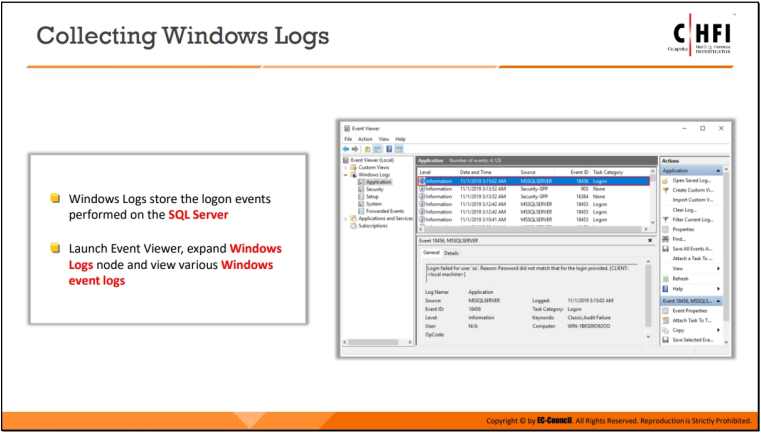
Để xem một hàng trên mỗi thuộc tính kế hoạch cho kế hoạch được chỉ định bởi núm điều khiển kế hoạch, truy vấn sau đây được sử dụng:

**select \* from sys.dm\_exec\_cached\_plans áp dụng chéo**

**sys.dm\_exec\_plan\_attribut(plan\_handle)**

Cần lưu ý rằng **plan\_handle** trong cú pháp xác định duy nhất một kế hoạch truy vấn cho một lô đã được thực thi và kế hoạch của nó nằm trong bộ đệm kế hoạch.

## Thu thập nhật ký windows

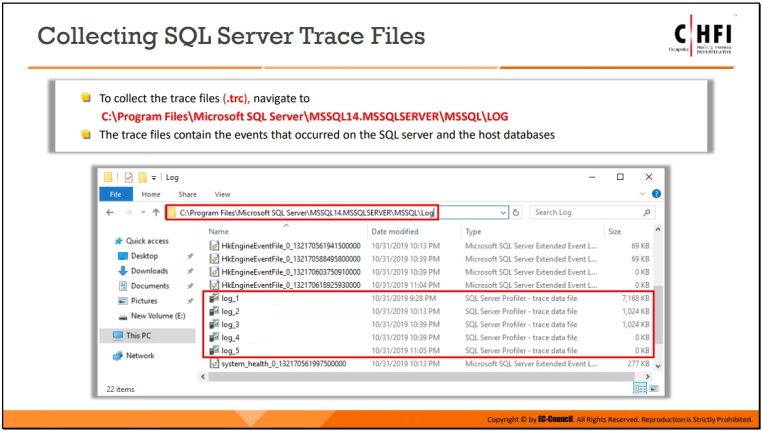


Nhật ký sự kiện Windows là các tệp văn bản đơn giản ở định dạng XML (EVTX) được sử dụng bởi Windows Vista và các phiên bản mới hơn. Windows chứa các loại nhật ký khác nhau, bao gồm nhật ký quản trị, hoạt động, phân tích, gỡ lỗi và ứng dụng.

Nhật ký Windows lưu trữ các sự kiện đăng nhập được thực hiện trên Máy chủ SQL. Trình xem sự kiện trong HĐH Windows cho phép người dùng xem nhật ký sự kiện trên máy cục bộ hoặc máy từ xa. Đối với điều này, hãy khởi chạy Trình xem sự kiện, mở rộng nút Nhật ký Windows và chọn loại nhật ký (ví dụ: Ứng dụng, Bảo mật, Thiết lập, Hệ thống hoặc Sự kiện được Chuyển tiếp) cần được xem.

Từ góc độ của một cuộc điều tra số, các tệp nhật ký sự kiện đóng một vai trò quan trọng vì chúng theo dõi tất cả “các sự kiện quan trọng” trên bất kỳ máy tính nào. Bất kỳ chương trình nào đang chạy trên máy tính đều đăng thông báo trong nhật ký sự kiện và đồng thời đăng thông báo trước khi kết thúc. Các sự kiện như truy cập hệ thống, OSlag và các sự cố về trình điều khiển hoặc phần cứng được lưu trong nhật ký sự kiện. Các nhà điều tra có thể sử dụng dữ liệu này để theo dõi những kẻ tấn công

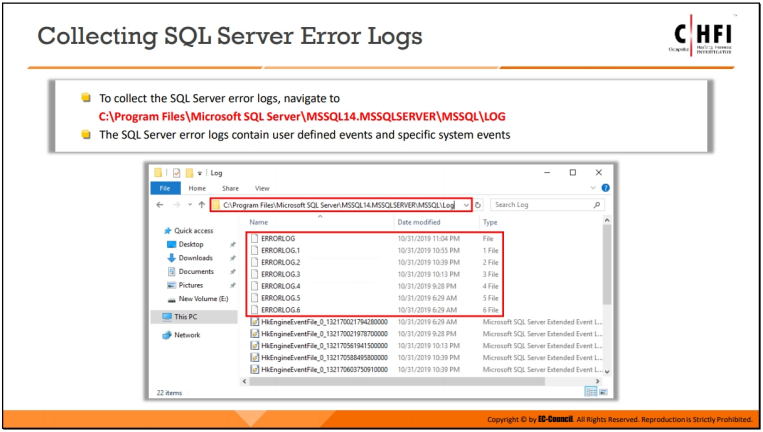
## Thu thập tệp theo dõi máy chủ SQL



Như đã thảo luận ở trên, các tệp theo dõi ghi lại tất cả các sự kiện xảy ra trên Máy chủ SQL và cơ sở dữ liệu có trong đó. Điều tra viên có thể sử dụng SQL Server Profiler để xem các tệp theo dõi. Để thu thập các tệp theo dõi, hãy điều hướng đến

**C:\ProgramFiles\MicrosoftSQLServer\MSSQL14.MSSQLSERVER\MSSQL\LOG**

## Thu thập nhật ký lỗi máy chủ SQL



Nhật ký lỗi máy chủ SQL ghi lại các sự kiện do người dùng xác định và hệ thống cụ thể. Nhật ký lỗi cũng chứa địa chỉ IP của các kết nối máy chủ-máy khách SQL. Tệp nhật ký lỗi mới được tạo khi xảy ra phiên bản SQL Server mới. Để thu thập nhật ký lỗi Máy chủ SQL, hãy điều hướng đến:

**C:\ProgramFiles\MicrosoftSQLServer\MSSQL14.MSSQLSERVER\MSSQL\LOG**

Điều tra viên có thể sử dụng SQL Server Management Studio hoặc bất kỳ trình soạn thảo văn bản nào để xem nhật ký lỗi. Cả tệp theo dõi và nhật ký lỗi đều là bằng chứng quan trọng để điều tra máy chủ SQL của quá trình giám định.