

**Mục tiêu học tập**

Cơ sở dữ liệu lưu trữ tất cả dữ liệu liên quan đến ứng dụng web và cho phép người dùng xem, truy cập, quản lý, và cập nhật các thông tin liên quan. Trong một số trường hợp, cơ sở dữ liệu hoặc ứng dụng web có thể chứa các lỗ hổng cho phép kẻ tấn công thao túng nội dung của cơ sở dữ liệu. Cơ sở dữ liệu pháp y giúp các nhà điều tra pháp y thu thập bằng chứng quan trọng, có thể dẫn đến truy tố thủ phạm trước tòa án. Một điều tra viên pháp y phải có kiến ​​thức vững chắc của các máy chủ đa cơ sở dữ liệu và các điều khoản hệ thống tệp của chúng. Ngoài ra, điều tra viên có thể kiểm tra các tệp nhật ký tương ứng của chúng và xác định nguyên nhân của các cuộc tấn công.

Mô-đun này phác thảo các nguyên tắc cơ bản của điều tra cơ sở dữ liệu và tóm tắt các hệ thống tệp của máy chủ MSSQL và MySQL. Hơn nữa, nó giải thích việc sử dụng các công cụ khác nhau để kiểm tra nhật ký tập tin và tìm kiếm các giao dịch gian lận.

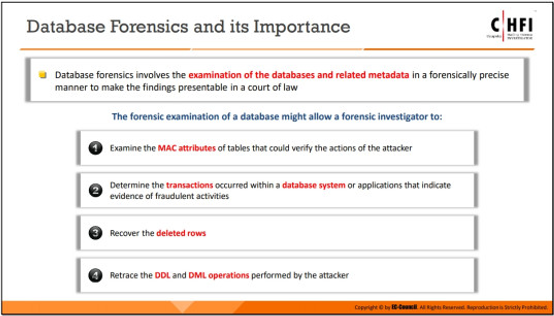
Vào cuối mô-đun này, bạn sẽ có thể:

* Hiểu về điều tra cơ sở dữ liệu và tầm quan trọng của nó
* Xác định kho lưu trữ dữ liệu và bằng chứng cơ sở dữ liệu trong máy chủ MSSQL
* Thu thập tệp chứng cứ trên máy chủ MSSQL
* Thực hiện pháp y MSSOL
* Hiểu kiến ​​trúc bên trong của MySQL và cấu trúc của thư mục dữ liệu
* Hiểu lược đồ thông tin và liệt kê các tiện ích MySQL để thực hiện phân tích pháp y
* Thực hiện pháp y MyS5QOL trên cơ sở dữ liệu ứng dụng web WordPress

**LO#01:Hiểu Cơ sở dữ liệu Forensics và tầm quan trọng của nó**

Điều tra cơ sở dữ liệu là một bộ phận của điều tra kỹ thuật số liên quan đến việc kiểm tra cơ sở dữ liệu và siêu dữ liệu liên quan được lưu trữ trong chúng theo cách chính xác về mặt pháp lý để xác định và truy tố thủ phạm của tội phạm liên quan đến vi phạm dữ liệu.

Phần này trình bày tổng quan về điều tra cơ sở dữ liệu và tầm quan trọng của nó.



**Cơ sở dữ liệu Forensics và tầm quan trọng của nó**

Hiện tại, nhiều ứng dụng sử dụng cơ sở dữ liệu hiệu suất cao để quản lý dữ liệu của họ. Trong khi các tổ chức đang triển khai các cơ chế bảo mật mạnh mẽ để bảo vệ cơ sở dữ liệu đa năng của họ, tin tặc đang nghĩ ra những cách tinh vi để tấn công chúng, do đó dẫn đến việc lộ dữ liệu nhạy cảm.

Cơ sở dữ liệu pháp y liên quan đến việc kiểm tra cơ sở dữ liệu và siêu dữ liệu liên quan của chúng. Các quy trình liên quan đến điều tra cơ sở dữ liệu tương tự như sau trong điều tra máy tính.

Cơ sở dữ liệu đóng vai trò là nguồn bằng chứng điện tử chính cho mọi tổ chức, bất kể kích thước và độ phức tạp của nó. Khi một sự cố bất ngờ xảy ra, một giám định pháp y sẽ tạo ra điều này bằng chứng tại tòa án, bất kể quy mô của cơ sở dữ liệu. Là một phần của cuộc điều tra, điều tra viên có thể kiểm tra khoảng thời gian sao để kiểm tra và xác nhận các hoạt động được thực hiện bởi người dùng/người dùng trên nội dung cơ sở dữ liệu. Họ cũng có thể phân tích các giao dịch trong giao dịch log data file (.ldf) để xác định xem có bất kỳ người dùng nào thực hiện các hoạt động gian lận trên cơ sở dữ liệu. Đa cơ sở lưu trữ máy chủ có thể chứa thông tin được lưu trong bộ nhớ cache trong RAM của chúng các nhà điều tra thậm chí có thể kiểm tra thông tin này bằng các kỹ thuật phân tích trực tiếp.

Việc kiểm tra pháp y cơ sở dữ liệu có thể cho phép điều tra viên:

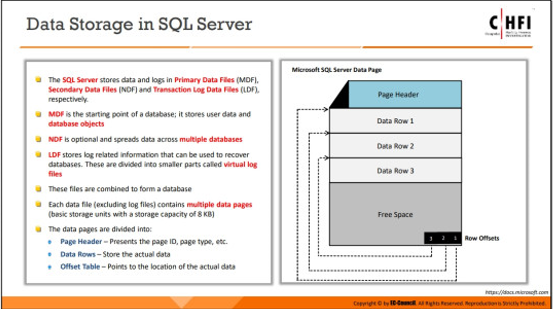
* Kiểm tra các thuộc tính MAC của các bảng có thể xác minh hành động của kẻ tấn công
* Xác định các giao dịch xảy ra trong một hệ thống cơ sở dữ liệu hoặc các ứng dụng chỉ ra bằng chứng về các hoạt động gian lận
* Khôi phục các hàng đã xóa
* Truy xuất các hoạt động DDL và DML do kẻ tấn công thực hiện

**LO#02: Xác định Kho lưu trữ Dữ liệu và Bằng chứng Cơ sở dữ liệu trong Máy chủ MSSQL**

SQL Server là một hệ thống quản lý cơ sở dữ liệu quan hệ được chấp nhận rộng rãi bởi nhiều các tổ chức để lưu trữ dữ liệu liên quan đến các ứng dụng của họ. Thỉs bao gồm dữ liệu nhạy cảm liên quan đến các ứng dụng web và tài khoản người dùng được liên kết với các ứng dụng web này.

Các kho lưu trữ bằng chứng cơ sở dữ liệu trong SQL Server là nguồn dữ liệu bằng chứng quan trọng cho điều tra viên pháp y. Dữ liệu Máy chủ SOQL được lưu trữ nguyên bản trong Máy chủ SQL và bên ngoài trong máy Windows lưu trữ máy chủ.

Phần này thảo luận về cấu trúc và vị trí lưu trữ đa dữ liệu trong Máy chủ MSSOL và nguồn bằng chứng có thể được tìm thấy trong đó.



Dữ liệu và Nhật ký trong Máy chủ SQL được lưu trữ trong ba tệp khác nhau:

**1. Tệp dữ liệu chính**

Tệp đdata chính (MDF) là điểm bắt đầu của cơ sở dữ liệu; nó trỏ đến các tệp khác trong kho dữ liệu. Mọi cơ sở dữ liệu đều có một tệp đa dữ liệu chính lưu trữ tất cả dữ liệu trong cơ sở dữ liệu đối tượng (bảng, lược đồ, chỉ mục, v.v.). Phần mở rộng tên tệp cho các tệp dữ liệu chính là .mdf.

**2. Tệp dữ liệu thứ cấp**

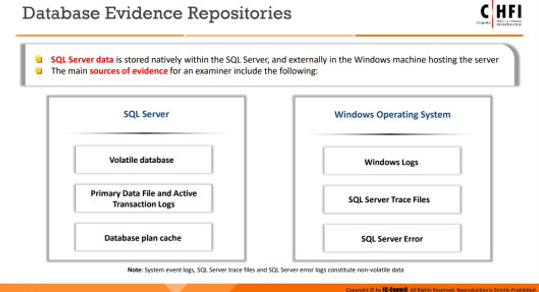
Các tệp dữ liệu thứ cấp (NDF) là tùy chọn. Cơ sở dữ liệu chỉ chứa một dữ liệu sơ cấp tệp, nhưng nó có thể chứa không/một/nhiều tệp đa số thứ cấp. Các tệp dữ liệu thứ cấp có thể được lưu trữ trên đĩa cứng, tách biệt với tệp dữ liệu chính. Phần mở rộng tên tệp đối với các tệp dữ liệu thứ cấp là .ndf.

**3. Tệp dữ liệu nhật ký giao dịch**

Các tệp dữ liệu nhật ký giao dịch (LDF} chứa thông tin nhật ký được liên kết với cơ sở dữ liệu. Tệp nhật ký giao dịch giúp điều tra viên pháp y kiểm tra các giao dịch xảy ra trong cơ sở dữ liệu và khôi phục dữ liệu đã xóa, nếu cần. Phần mở rộng tên tệp cho các tệp nhật ký giao dịch là .ldf và mỗi tệp được chia thành nhiều tệp nhật ký ảo.

Ba tệp này cùng nhau tạo thành một cơ sở dữ liệu và mỗi tệp dữ liệu chứa nhiều trang dữ liệu là những đơn vị lưu trữ cơ bản với dung lượng lưu trữ là 8 KB. Các trang dữ liệu được chia thành:

* **Page Header**: Trình bày ID trang, loại trang, v.v.
* **Hàng dữ liệu**: Lưu trữ dữ liệu thực tế
* **Offset Table**: Trỏ đến vị trí của dữ liệu thực tế



**Kho lưu trữ bằng chứng cơ sở dữ liệu**

Các nguồn cung cấp thông tin có giá trị đôi khi bị các nhà điều tra bỏ qua, vì chẳng hạn, trong các trường hợp sở hữu trí tuệ, đa cơ sở chứa dữ liệu liên quan đến tài chính là cơ sở chính mục tiêu cho những kẻ tấn công để làm hỏng cơ sở dữ liệu đdata. Trong những trường hợp như vậy, kho mã nguồn, kiến ​​thức hệ thống quản lý và hệ thống quản lý tài liệu có thể cung cấp thông tin chi tiết tốt hơn về điều tra viên liên quan đến một vi phạm bị nghi ngờ. Như vậy, Điều tra viên có thể giúp bị cáo chống lại nghĩa vụ không hợp lệ.

Cơ sở dữ liệu có thể được sử dụng để tạo phiên bản và xem xét vòng đời của tài liệu. Siêu dữ liệu mở rộng chẳng hạn như mô tả, từ khóa và nhận xét có thể cung cấp thông tin chi tiết về tài liệu mục đích. Nó tiết lộ thông tin như (những) người dùng đã truy cập hệ thống mục tiêu để tiết lộ dữ liệu nhạy cảm cũng như vị trí và thời điểm chúng được định tuyến.

**Vị trí của tệp để khôi phục bằng chứng**

Dữ liệu Máy chủ SQL được lưu trữ nguyên bản trong Máy chủ SOL và bên ngoài máy Windows lưu trữ máy chủ. Các nguồn bằng chứng chính cho người kiểm tra trong Máy chủ SQL là cơ sở dữ liệu dễ bay hơi, tệp dữ liệu chính và nhật ký giao dịch đang hoạt động và bộ đệm của sơ đồ cơ sở dữ liệu. Các các nguồn bằng chứng chính cho người kiểm tra trong máy Windows lưu trữ máy chủ là nhật ký Windows, tệp theo dõi máy chủ SOL và nhật ký lỗi máy chủ SQL. Nhật ký sự kiện hệ thống, SQL Server tệp theo dõi và nhật ký lỗi Máy chủ SQL tạo thành dữ liệu không bay hơi

Cùng với dữ liệu đa cơ sở dữ liệu không ổn định, nhật ký Windows và bộ nhớ cache gói cơ sở dữ liệu, các nhà điều tra có thể kiểm tra các tệp sau đây để hiểu sâu hơn về các hoạt động diễn ra trên cơ sở dữ liệu:

* **Cơ sở dữ liệu và tệp nhật ký**

\Wicrosoft SQL Server\MSSQL14.MSSOLSERVER\MSSQOL\DATA\\*.MDF \*.LDF

* **Trace file**

\\Microsoft SOL Server\MSSOL14.MSSOLSERVER \MSSOL\ LOG\LOG\_#.TRC

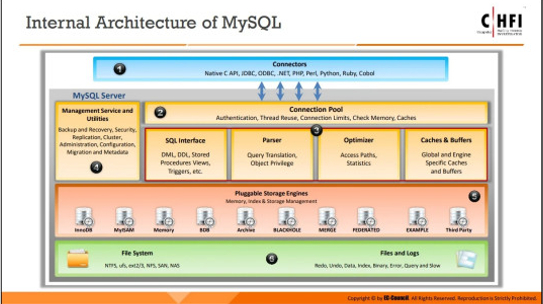
* **Nhật ký lỗi máy chủ SQL**

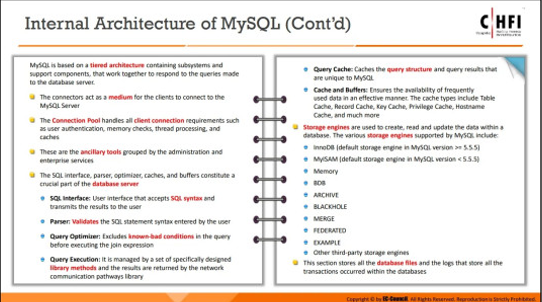
\\Microsoft SQL Server\MSSQL14.MSSOLSERVER\MSSOL\LOG\ERRORLOG

**LO#05: Hiểu nội bộ ärchitecture của mysql và § cấu trúc của**

Thư mục dữ liệu cơ sở dữ liệu MySOL là một cơ sở cơ sở nguồn mở được sử dụng rộng rãi mà Ís có sẵn miễn phí với phân phối lại không giới hạn, do đó cung cấp cho người dùng quyền truy cập đầy đủ vào mã nguồn. CáccCơ sở dữ liệu có thể chứa các công cụ lưu trữ có thể cắm khác nhau để phù hợp với ứng dụng. Nó hỗ trợ giao dịch với các công cụ lưu trữ InnoDB hoặc BDB tích hợp viết hoạt động cần thiết trong môi trường doanh nghiệp.

Kiến trúc bên trong của MySQL tuân theo cấu trúc phân cấp nhiều lớp, sử dụng một kết hợp các hệ thống con và hỗ trợ các thành phần tương tác với nhau để đọc, phân tích và thực hiện các truy vấn được thực hiện cho máy chủ cơ sở dữ liệu và trả về kết quả. Dữ liệu ngược lại, điều đó lưu trữ từng điều và bảng được xử lý bởi máy chủ. Cái này phần trình bày một cái nhìn tổng quan chi tiết về kiến trúc nội bộ của Mysol và cấu trúc của thư mục dữ liệu.





**Kiến trúc nội bộ của MySQL**

Kiến trúc của MySOL dựa trên kiến ​​trúc theo tầng; ít là sự kết hợp của các hệ thống con và hỗ trợ các thành phần tương tác với nhau để đọc, phân tích và thực thi các truy vấn được thực hiện cho máy chủ cơ sở dữ liệu để trả về các kết quả.

* Các trình kết nối hoạt động như một phương tiện để khách hàng kết nối với Máy chủ MySOL
* Nhóm kết nối xử lý tất cả các yêu cầu kết nối máy khách chẳng hạn như người dùng xác thực, kiểm tra bộ nhớ, xử lý luồng và bộ đệm
* Chúng bao gồm các công cụ phụ trợ được nhóm theo dịch vụ quản trị và doanh nghiệp
* Giao diện SQL, trình phân tích cú pháp, trình tối ưu hóa, bộ đệm và bộ đệm cùng nhau tạo thành một phần quan trọng của máy chủ cơ sở dữ liệu:
* **Giao diện SQL:** Lớp giao diện SQL hoạt động như một giao diện bằng cách chấp nhận SOL báo cáo và cung cấp kết quả cho người dùng. Mặc dù MySQL có rất nhiều các tùy chọn không tuân thủ ANSI, lớp hỗ trợ tiêu chuẩn ANSI SQL. Khi máy khách gửi yêu cầu đến máy chủ thông qua giao tiếp mạng đường dẫn, máy chủ sẽ tạo một luồng. Sau đó, máy chủ phân tích lệnh SQL và lưu trữ các phần trong một cấu trúc dữ liệu nội bộ.
* **Trình phân tích cú pháp:** lt xác thực các truy vấn SQL do người dùng nhập vào. lt xây dựng một cấu trúc truy vấn, điều này làm đen câu lệnh truy vấn (SQL) trong bộ nhớ dưới dạng cấu trúc cây. Cái này cấu trúc cây bao gồm một nhóm các bảng và tên trường được tham chiếu và tham gia điều kiện, trong số những người khác; chức năng chính của nó là kiểm tra tính chính xác của SQL nhà nước. Khi một câu lệnh SỐL được xác thực, trình phân tích cú pháp sẽ chuyển cấu trúc truy vấn đến bộ xử lý truy vấn, rồi đến bộ tối ưu hóa truy vấn.
* **Trình tối ưu hóa truy vấn:** Chức năng chính của trình tối ưu hóa truy vấn bao gồm xác thực sự tồn tại của các bảng và mức độ truy cập vào ứng dụng cho người dùng. trình tối ưu hóa sau đó trả về các lỗi (nếu có); sau đó, điều khiển được trả lại cho luồng người quản lý hoặc người nghe. Trình tối ưu hóa hoạt động trên chiến lược SELECT-PROJECT-JOIN cố gắng cơ cấu lại các truy vấn.
* **Thực thi truy vấn:** Một tập hợp các phương thức thư viện được thiết kế để thực hiện một truy vấn cụ thể kiểm soát việc thực hiện của nó và trả về kết quả từ mỗi phương thức thực hiện bằng cách sử dụng thư viện đường truyền thông mạng.
* **Bộ đệm truy vấn:** Bộ đệm truy vấn đóng vai trò quan trọng trong việc tối ưu hóa truy vấn và hệ thống con thực thi. Nó lưu trữ cấu trúc truy vấn và kết quả truy vấn.
* **Bộ nhớ cache và bộ đệm:** Chúng đảm bảo rằng dữ liệu thường được sử dụng được cung cấp trong một cách hiệu quả. Máy chủ cơ sở dữ liệu MySQL chứa nhiều loại bộ đệm khác nhau, bao gồm bộ đệm bảng, bộ đệm khóa, bộ đệm đặc quyền, bộ đệm tên máy chủ, bộ đệm bản ghi và các bộ đệm linh tinh (ví dụ: tham gia bộ đệm bộ đệm).

Công cụ lưu trữ được sử dụng để tạo, đọc và cập nhật dữ liệu trong cơ sở dữ liệu. MySOL hỗ trợ công cụ lưu trữ khác nhau, như được liệt kê dưới đây:

**1. InnoDB (công cụ lưu trữ mặc định trong phiên bản MySQL >= 5.5.5)**

* Thường dùng khi cần thực hiện giao dịch
* Hỗ trợ ACID truyền thống (Nguyên tử, Tính nhất quán, Cách ly, Độ bền)
* Giao dịch và ràng buộc khóa ngoại
* Cung cấp giới hạn lưu trữ là 64 TB cho mỗi bảng
* Cung cấp MVCC (kiểm soát đồng thời nhiều phiên bản)/Snapshot read
* Hỗ trợ khôi phục sự cố
* Dùng trong các hệ thống xử lý giao dịch trực tuyến

**2. MylSAM (công cụ lưu trữ mặc định trong phiên bản MySQL <5.5.5)**

* Cung cấp khả năng lưu trữ dữ liệu không giới hạn
* Đưa ra kỹ thuật nén dữ liệu
* Xử lý tải dữ liệu tốc độ cao
* Cho phép lưu trữ hiệu quả

**3. Memory**

* Một bảng bộ nhớ thực hiện cơ chế băm để truy xuất nhanh hơn
* dữ liệu thông dụng
* Cung cấp tính hợp lệ cho dữ liệu được lưu trữ trong bộ nhớ chỉ trong các phiên MySQL

**4. BDB**

* Viết tắt của cơ sở dữ liệu Berkeley
* Thay thế cho InnoDB
* Hỗ trợ các phương thức giao dịch bổ sung như CAM KẾT và ROLLBACK

**5. LƯU TRỮ**

* Cung cấp giới hạn lưu trữ không giới hạn ở định dạng nén
* Nổi tiếng với việc lưu trữ và truy xuất khối lượng lớn tài liệu lưu trữ hiếm khi được truy cập hoặc
* dữ liệu lịch sử
* Hỗ trợ nén đa dữ liệu tự động
* Cung cấp MVCC/Snapshot đọc
* Giới hạn hoạt động INSERT và SELECT

**6. LỖ ĐEN**

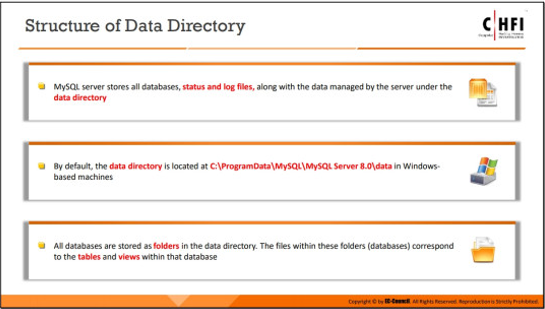
* Cho phép hệ thống ghi đa số; tuy nhiên, những dữ liệu này không bao giờ được lưu
* Ghi các câu lệnh SQL vào nhật ký khi bật tính năng ghi nhật ký nhị phân
* Cho phép quản trị viên đatabase tạm thời vô hiệu hóa tính năng đưa đata vào cơ sở dữ liệu bằng cách hoán đổi loại bảng

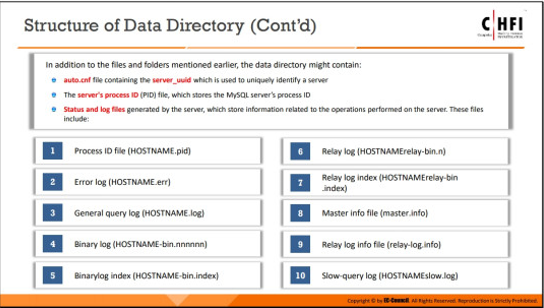
**7. HỢP NHẤT**

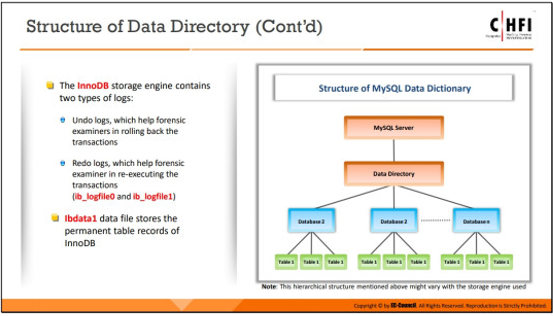
* Được xây dựng bằng cách sử dụng một loạt các bảng MylSAM (với bố cục bộ hoặc lược đồ}
* Đảm bảo rằng tất cả các bảng nằm trên cùng một hệ thống
* Chặn hoạt động thay thế
* Thực hiện các tùy chọn tìm kiếm và sắp xếp nhanh hơn
* Cho phép người dùng truy cập dữ liệu bằng các thao tác CHỌN, CẬP NHẬT, CHÈN và XÓA
* Được sử dụng rộng rãi ¡ trong các ứng dụng cơ sở dữ liệu rất lớn như kho dữ liệu

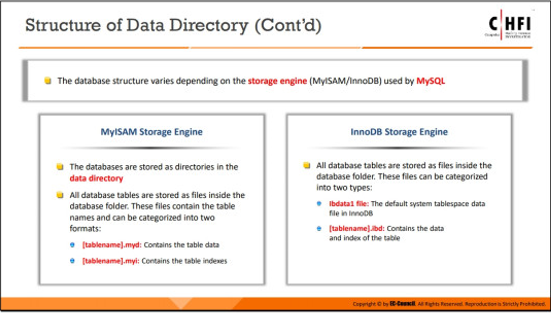
**8. LIÊN BANG**

* Tạo một tham chiếu bảng đơn từ một hoặc nhiều hệ thống cơ sở dữ liệu
* Do đó, nó tương tự như Merge, nhưng nó cho phép liên kết dữ liệu/bảng giữa các máy chủ cơ sở dữ liệu
* Cho phép dịch dữ liệu trong quá trình lưu trữ và truy xuất
* Hỗ trợ tất cả các thao tác SQL
* Không yêu cầu phần mềm trung gian để truy cập dữ liệu từ xa
* Được sử dụng rộng rãi trong môi trường siêu thị phân tán hoặc đa dạng









**Kết cấu của thư mục dữ liệu**

Thư mục dữ liệu MySQL chứa cơ sở dữ liệu, bảng và tệp trạng thái được quản lý bởi MySOL máy chủ. Các thư mục dữ liệu này được tổ chức theo cấu trúc dạng cây bằng cách tuân theo hệ thống phân cấp cấu trúc của hệ thống tệp Unix hoặc Windows.

Việc sắp xếp các thư mục dữ liệu trong MySOL như sau:

* Mỗi cơ sở dữ liệu tương ứng với một thư mục trong thư mục dữ liệu
* Các bảng, dạng xem và trình kích hoạt của cơ sở dữ liệu tương ứng với các tệp của cơ sở dữ liệu hư mục.
* Tất cả cơ sở dữ liệu được lưu trữ dưới dạng các thư mục trong thư mục đata
* Các cấu trúc lưu trữ khác nhau tùy theo việc triển khai cơ sở dữ liệu phân cấp.

Đường dẫn mặc định đến dữ liệu MySQL directoy cho các máy chạy Windows-based C:\ProgramData\MySOL\MySQL Server 8.0\data.

Các tệp trạng thái và nhật ký được lưu trữ trong một thư mục dữ liệu bao gồm:

**1. Tệp ID tiến trình (HOSTNAME.pid):** Chứa ID tiến trình được tạo khi máy chủ khởi động

**2. Nhật ký lỗi (HOSTNAME.err)}:** chứa thông tin liên quan đến khởi động và

sự kiện tắt máy cũng như các lỗi

**3. Nhật ký truy vấn chung (HOSTNAME.log):** Nó chứa các nhật ký liên quan đến kết nối máy khách và các hoạt động

**4. Nhật ký nhị phân (HOSTNAME-bin.nnnnnn):** Ít chứa các sự kiện mô tả các thay đổi mà xảy ra trong cơ sở dữ liệu

**5. Chỉ mục nhật ký nhị phân (HOSTNAME-bin.index):** Nó chứa danh sách tất cả các tệp nhật ký nhị phân hiện tại có sẵn trong thư mục dữ liệu

**6. \_Relay log (HOSTNAMErelay-bin.n):** Nó chứa các sự kiện mô tả những thay đổi mà xảy ra trong cơ sở dữ liệu

**7. Chỉ mục nhật ký chuyển tiếp (HOSTNAMErelay-bin.index):** tt chứa danh sách tất cả các tệp nhật ký chuyển tiếp hiện có sẵn trong thư mục dữ liệu

**8. Tệp thông tin chính (master.info):** Nó được tạo bởi một máy chủ nô lệ sao chép có chứa các tham số cần thiết được sử dụng để kết nối với nô lệ chính

**9. Tệp thông tin nhật ký chuyển tiếp (relay-log.info):** Nó được tạo bởi một máy chủ nô lệ sao chép có chứa trạng thái xử lý nhật ký chuyển tiếp

**10. Nhật ký truy vấn chậm (HOSTNAMEslow.log):** Một tệp văn bản chứa các câu lệnh yêu cầu thời gian xử lý lâu hơn

Ngoài các tệp và thư mục đã đề cập trước đó, thư mục dữ liệu có thể chứa:

* Tệp auto.cnf chứa server\_uuid được sử dụng xác định duy nhất một máy chủ
* Tệp ID tiến trình (PID) của máy chủ lưu trữ ID tiến trình của máy chủ MySOL

Cấu trúc cơ sở dữ liệu sau khi theo các công cụ lưu trữ được sử dụng bởi MySQL. Sau đây là hai công cụ lưu trữ phổ biến nhất trong MySOL:

**1. Công cụ lưu trữ MylSAM**

Trong một hệ thống tệp không được phân vùng, công cụ lưu trữ MylSAM lưu trữ từng bảng MylISAM trong

hai tập tin. Các tệp chứa tên bắt đầu bằng tên bảng và có phần mở rộng

để chỉ ra loại tập tin; phần mở rộng tệp bao gồm .MYI và .MYD.

* **[tablename].myi:** Tệp này lưu chỉ mục tệp
* **[tablename].myd:** Tệp này lưu dữ liệu của bảng

**2. Công cụ lưu trữ InnoDB**

Nội dung bảng của InnoDB được biểu diễn bằng các không gian bảng; chúng có hai loại:

* **Ibdata1 file:** Tệp dữ liệu vùng bảng hệ thống mặc định trong InnoDB. Tập tin này lưu trữ Ibdata1 bản ghi bảng cố định của InnoDB.
* [tablename].ibd: Nó chứa data và chỉ mục của bảng

Công cụ lưu trữ InnoDB chứa hai loại nhật ký:

* **Undo logs**: Những nhật ký này giúp người kiểm tra pháp y khôi phục các giao dịch
* **Redo logs**: Các nhật ký này giúp giám định pháp y thực hiện lại các giao dịch (ib\_logfile0 và ib\_logfile1)