

Hội nghị quốc tế lần thứ tư về hệ thống tự trị và tự trị

Thực thi cấu hình bảo mật cơ sở dữ liệu dựa trên chính sách thông qua khả năng tự trị

Ghassan 'Gus' Jabbour

Trường CNTT & Kỹ thuật Volgenau, Đại học George Mason, Fairfax, VA 22030, Hoa Kỳ

Daniel A. Menasce ́

Khoa Khoa học Máy tính, MS 4A5, Đại học George Mason Fairfax, VA 22030, Hoa Kỳ

[menasce@gmu.edu](mailto:menasce@gmu.edu)

# Trừu tượng

*Sự nhấn mạnh đáng kể gần đây đã được đặt vào việc củng cố cơ sở dữ liệu và kiểm toán thường xuyên các hệ thống như vậy bởi các kiểm toán viên độc lập và các Cán bộ An ninh Hệ thống Thông tin được chứng nhận (ISSO). Các trung tâm dữ liệu lưu trữ dữ liệu nhạy cảm và các hệ thống quan trọng, đặc biệt là các trung tâm thuộc các cơ quan chính phủ, đã chịu áp lực rất lớn để bảo mật cơ sở dữ liệu của họ tuân thủ một số nguyên tắc bảo mật. Các yêu cầu như vậy bắt buộc mỗi hệ thống phải vượt qua một cuộc quét bảo mật nghiêm ngặt trước khi nó được coi là phù hợp để đi vào chế độ hoạt động và nó phải chịu sự kiểm tra thường xuyên sau đó. Điều này đến lượt nó đã gây áp lực rất lớn lên các nhà quản lý cơ sở dữ liệu, trong nhiều trường hợp, đã bị choáng ngợp bởi các nhiệm vụ cài đặt, bảo trì đúng cách và tìm ra hệ thống của họ theo cách cung cấp sự phù hợp tối ưu. Tuy nhiên, nó đang trở nên cực kỳ thách thức, tốn thời gian và tốn nhiều tài nguyên để giải quyết các nhu cầu bảo mật trong ngân sách và thời gian chặt chẽ. Do đó, sẽ rất thuận lợi khi triển khai các tính năng tự chủ vào các hệ thống cơ sở dữ liệu để giải quyết một số khía cạnh của vấn đề này. Bài viết này trình bày một khuôn khổ nhúng các khả năng au-tonomic vào các hệ thống cơ sở dữ liệu để cung cấp các tính năng tự bảo vệ trong trường hợp thay đổi trái phép, vô tình hoặc cố ý trong các thông số bảo mật. Điều này đạt được bằng cách nhúng vào cơ sở dữ liệu khả năng so sánh từng cấu hình bảo mật, tham số, thay đổi, nỗ lực (hoặc yêu cầu) với chính sách bảo mật được xác định trước được nhúng trước khi cho phép hoặc từ chối thay đổi. Bài báo trình bày cách khung đề xuất có thể được triển khai trong cơ sở dữ liệu Oracle 10g Release 2.*

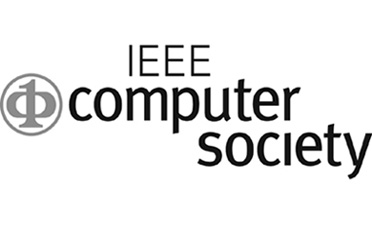
# Giới thiệu

Điện toán tự trị là một phân ngành của khoa học máy tính liên quan đến việc thiết kế các hệ thống tự quản lý, tức là, với các hệ thống tự tối ưu hóa, tự cấu hình, tự phục hồi và tự bảo vệ [1]. Bài viết này đề cập đến khía cạnh tự bảo vệ của điện toán tự trị vì nó áp dụng cho bảo mật cơ sở dữ liệu. Để đạt được điều đó, sự nhấn mạnh đáng kể đã được đặt trong vài năm qua về việc củng cố cơ sở dữ liệu theo các hướng dẫn bảo mật do chủ sở hữu hệ thống thiết lập. Khái niệm nâng cao nhận thức về bảo mật hệ thống máy tính, đặc biệt là những hệ thống được coi là nhiệm vụ quan trọng, đã thể hiện rõ ràng hơn trong bối cảnh các cuộc tấn công độc hại gia tăng và mối đe dọa tiềm tàng của khủng bố chống lại các mục tiêu máy tính quan trọng, đặc biệt là các mục tiêu của chính phủ. Do đó, với mối quan tâm ngày càng tăng về các mối đe dọa an ninh và vi phạm an ninh tiềm ẩn có thể liên quan đến khủng bố hoặc các loại tấn công khác, chủ sở hữu hệ thống, đặc biệt là các cơ quan chính phủ, đã áp đặt các hướng dẫn bảo mật nghiêm ngặt cho tất cả các khía cạnh của hệ thống của họ theo yêu cầu của Đạo luật Quản lý An ninh Thông tin Liên bang Hoa Kỳ (FISMA) năm 2002 [2]. Chủ sở hữu hệ thống đã được yêu cầu đưa ra các yêu cầu rất cứng nhắc để giữ cho hệ thống của họ tuân thủ đầy đủ các chính sách bảo mật nghiêm ngặt và quét hệ thống của họ thường xuyên để đảm bảo rằng không có cấu hình bảo mật nào bị thay đổi. Yêu cầu bảo mật nghiêm ngặt này đã được nhấn mạnh bởi một số luật, quy định, chỉ thị và ấn phẩm của chính phủ. Theo Chỉ thị của Tổng thống về An ninh Nội địa Hoa Kỳ / HSPD-7, tất cả các cơ quan được yêu cầu xác định và cung cấp "các biện pháp bảo mật thông tin tương xứng với rủi ro và mức độ thiệt hại do truy cập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi hoặc phá hủy thông tin trái phép" và các tài nguyên thông tin phù hợp với FISMA năm 2002 [3].

Những tiến bộ gần đây trong cơ sở dữ liệu tự trị và tự trị



0-7695-3093-1/08 $25.00 © 2008 IEEE DOI 10.1109/ICAS.2008.49



188

hệ thống quản lý cơ sở dữ liệu (ADBMS) đã tập trung vào quản lý tự động các tài nguyên để đạt được hiệu suất tối ưu [4], cung cấp cơ sở dữ liệu tự động [5], lựa chọn tài nguyên để tối ưu hóa và điều chỉnh cơ sở dữ liệu [6, 7], quyết định và quản lý dựa trên chính sách [8], tự định cỡ cơ sở dữ liệu phân cụm và nhóm đệm [9, 10], cách ly các cuộc tấn công vào dữ liệu và phục hồi từ các giao dịch độc hại [11, 12] và kiểm soát truy cập dựa trên vai trò [13, 14]. Nhưng, vì tính bảo mật của cơ sở dữ liệu và hệ thống thông tin là một vấn đề về tính bảo mật, tính toàn vẹn và tính sẵn có của dữ liệu được lưu trữ trong các hệ thống này [11, 12, 13], hầu hết các nỗ lực nghiên cứu an toàn đã tập trung vào việc bảo mật dữ liệu bằng cách kiểm soát và phát hiện bất kỳ truy cập trái phép nào vào nó hoặc bằng cách khôi phục bất kỳ dữ liệu bị mất nào trong trường hợp có chiến thuật độc hại. Trong nhiều năm, trọng tâm chính của sự chú ý là nghiên cứu, phát triển và triển khai các công nghệ như tường lửa, phát hiện xâm nhập và mạng riêng ảo. Tương đối ít đã được thực hiện để giải quyết tính bảo mật của các ứng dụng và hệ thống quản lý cơ sở dữ liệu truy cập hoặc lưu trữ dữ liệu [15].

Tuy nhiên, những yêu cầu đầy thách thức này đã thúc đẩy các nhà cung cấp cơ sở dữ liệu cũng như các công ty xây dựng các công cụ quét và giám sát cơ sở dữ liệu để kiểm tra các cách cải thiện tính bảo mật của cơ sở dữ liệu và tạo ra các ứng dụng phần mềm phát hiện các hoạt động đáng ngờ có thể dẫn đến truy cập trái phép vào cơ sở dữ liệu và có thể liên quan đến trạng thái của nó. Do đó, một số công cụ và công nghệ phần mềm đã có sẵn trên thị trường để giải quyết các vấn đề bảo mật cơ sở dữ liệu bằng cách cung cấp các cơ chế điều tra cấu hình của cơ sở dữ liệu và báo cáo các rủi ro và mối đe dọa tiềm ẩn cho chủ sở hữu dựa trên các nguyên tắc bảo mật nhất định. Các cách tiếp cận như vậy nhấn mạnh khía cạnh mon-itoring bằng cách kết nối với cơ sở dữ liệu và liên tục theo dõi nó cho bất kỳ thay đổi nào chủ yếu là trạng thái của các dịch vụ / quy trình hỗ trợ tính khả dụng của nó (ví dụ: listener, instance, firewall, v.v.). Một số công cụ cũng giám sát các thay đổi trong cài đặt cấu hình của cơ sở dữ liệu. Tuy nhiên, các công cụ hiện tại không giải quyết được thách thức của việc thực sự bảo mật cơ sở dữ liệu vì các công cụ giám sát có thể bị vô hiệu hóa bất cứ lúc nào bởi những người trong cuộc như kỹ sư hệ thống và mạng, nhân viên trung tâm điều hành mạng (NOC) hoặc người quản lý cơ sở dữ liệu. Cho dù ý định vô hiệu hóa các công cụ là tốt và cho dù lý do để vô hiệu hóa chúng có chính đáng đến đâu, thực tế vẫn là trong thời gian không có mon-itoring, cơ sở dữ liệu dễ bị truy cập trái phép không bị phát hiện và nguy cơ tiềm ẩn làm tổn hại đến nó hoặc làm thép dữ liệu của nó.

Một số công cụ hiện có giám sát mạng và hệ thống cơ sở dữ liệu, thu thập thông tin và tạo cảnh báo. Chúng cũng có khả năng cung cấp thông tin thu thập được vào các công cụ thống kê và phân tích đưa ra khuyến nghị cho chủ sở hữu hệ thống hoặc quản trị viên cơ sở dữ liệu về cách giải quyết vấn đề. Tuy nhiên, phần còn lại phụ thuộc vào

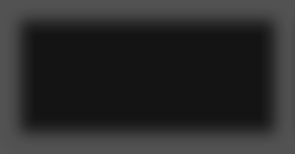
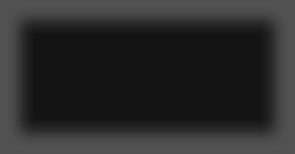
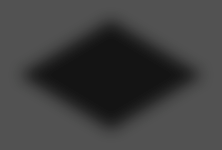
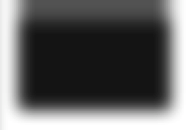
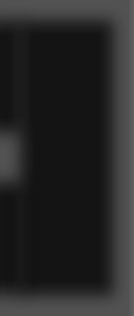
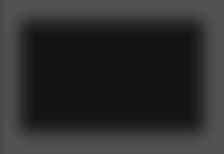
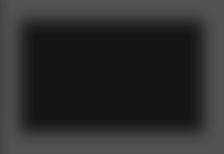
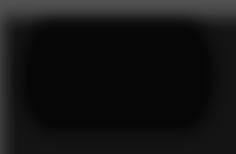
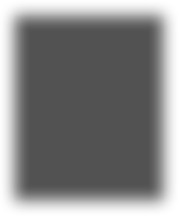
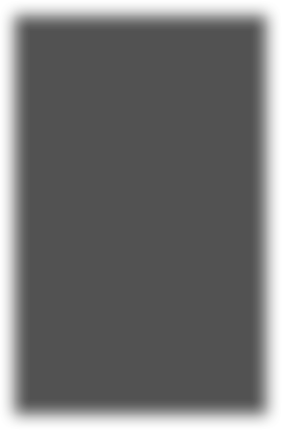
sự can thiệp của con người để thực hiện các biện pháp khắc phục thích hợp. Ngoài ra, hiệu quả của các công cụ này hoàn toàn phụ thuộc vào sự không gián đoạn tuyệt đối của việc giao tiếp với cơ sở dữ liệu. Việc gián đoạn giao tiếp dẫn đến gián đoạn trong việc giám sát và bảo vệ cơ sở dữ liệu.

Bài viết này trình bày một khuôn khổ giải quyết những thiếu sót của các công cụ này bằng cách sử dụng khái niệm nhúng chính sách vào chính cơ sở dữ liệu và cho phép các chính sách này chặn mọi nỗ lực thỏa hiệp trạng thái của cơ sở dữ liệu hoặc thay đổi cấu hình của nó theo cách mâu thuẫn với những gì đã được chủ sở hữu hệ thống thiết lập và đưa vào chính sách. Các chính sách này có thể được thiết lập ở các cấp độ granu-larity khác nhau theo cách mà chủ sở hữu hệ thống có thể chọn gọi các chính sách chi tiết thô để theo dõi và kiểm soát toàn bộ hành vi của cơ sở dữ liệu thông qua việc sử dụng cài đặt toàn cục hoặc gọi các chính sách chi tiết ảnh hưởng đến các khía cạnh cụ thể hoặc cài đặt cấu hình. Nhưng nguyên tắc cốt lõi tuyệt đối trong khuôn khổ của chúng tôi là khái niệm rằng các chính sách bảo mật, cũng như tất cả các đối tượng cơ sở dữ liệu và logic thực thi chúng, được coi là một phần không thể tách rời và không thể tách rời của cơ sở dữ liệu mà chúng có nghĩa là bảo vệ. Chúng được nhúng vào cơ sở dữ liệu và được bảo vệ khỏi bị truy cập bởi bất kỳ người dùng hoặc thực thể nào khác ngoài người sở hữu hệ thống. Thậm chí sau đó, khung cung cấp cho chủ sở hữu hệ thống khả năng thiết lập mật khẩu tổng hợp trong đó mỗi phần của mật khẩu thuộc sở hữu của một thành viên khác nhau trong nhóm chủ sở hữu hệ thống để tăng cường bảo mật.

# Khung dựa trên chính sách để bảo mật cơ sở dữ liệu

Có quyền truy cập đặc quyền vào cơ sở dữ liệu ngụ ý có quyền tác động hoặc thay đổi các khía cạnh nền tảng của cấu hình của nó, do đó thay đổi hành vi dự định của nó. Quản trị viên cơ sở dữ liệu thường có đặc quyền như vậy vì họ thường được giao nhiệm vụ quản lý cấu hình cơ sở dữ liệu và có thể hình dung là một mối đe dọa như đã được thể hiện bởi một số vi phạm bảo mật cơ sở dữ liệu trong vài năm qua [16, 17, 18, 19]. Cho dù cố ý hay không, quản trị viên cơ sở dữ liệu hoặc người dùng thành thạo có thể thay đổi cấu hình bảo mật theo cách có thể dẫn đến truy cập trái phép và xâm phạm cơ sở dữ liệu. Một ví dụ sẽ là cấp quyền truy cập đặc quyền cho người dùng không có đặc quyền hoặc chỉ đơn giản là lạm dụng quyền truy cập đặc quyền của anh ấy / cô ấy. Một ex- ample khác là một trong đó liên quan đến quét bảo mật hoặc kiểm toán cơ sở dữ liệu. Kiểm toán viên độc lập thường được thuê để thực hiện quét bảo mật cơ sở dữ liệu và họ làm việc với DBA để đưa cơ sở dữ liệu đến điểm đủ cứng để vượt qua quá trình quét. Tuy nhiên, quản trị viên cơ sở dữ liệu có thể tạm thời (hoặc vĩnh viễn) đặt một số hoặc tất cả các tham số cấu hình trở lại cài đặt ban đầu của chúng để đạt được các mục tiêu nhất định mà họ nghĩ là hợp lý. Một

### Hình 1. Kiến trúc của cơ sở dữ liệu tự bảo vệ.



Cơ sở dữ liệu đích

Hệ thống

Chủ nhân

Người dùng

Chính sách hành động

(2)

Yêu cầu thay đổi

(3)

(1)

Xây dựng chính sách

Tài nguyên

Giám sát

(4)

Chính sách

Chính sách thay đổi chính sách

Dữ liệu

DBA

Hacker người dùng điện

Không

(5)

(8)

Chủ sở hữu hệ thống cảnh báo

(7)

Có

(9)

Thông báo cho người dùng

(10)

(6)

Cơ quan thực thi chính sách

Thay đổi trình xác minh yêu cầu

Cập nhật bảng/chế độ xem hệ thống

Ghi lại bảng biên bản kiểm tra

DBMS SQL

Trình biên dịch

Ví dụ, kịch bản cơ bản nhưng nguy hiểm là thay đổi tham số hạn chế sử dụng cùng một mật khẩu sau khi hết hạn. DBA có thể dễ dàng đặt tham số đó thành unlim-ited, thay đổi mật khẩu thành cùng một mật khẩu và sau đó đặt tham số đó trở lại mức được cho là. Bằng cách đó, DBA sẽ vi phạm quy tắc áp dụng cho việc sử dụng lại cùng một mật khẩu nhiều lần (xem phần 2.3) để biết ví dụ chi tiết về tình huống này). Trong bài viết này, chúng tôi mô tả một cách tiếp cận dựa trên chính sách để thực thi các hình tượng cơ sở dữ liệu ngay cả đối với những người có quyền truy cập đặc quyền. Chúng tôi không ủng hộ việc giảm thiểu vai trò của DBA hoặc hạn chế quyền truy cập của họ. Tuy nhiên, chúng tôi ủng hộ rằng mỗi ac- tion được xác minh và phê duyệt bởi chủ sở hữu hệ thống nhúng, các chính sách cấu hình được xác định trước trước khi nó được áp dụng cho cơ sở dữ liệu.

Thủ tục được lưu trữ

## Kiến trúc của Framework

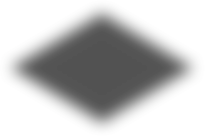
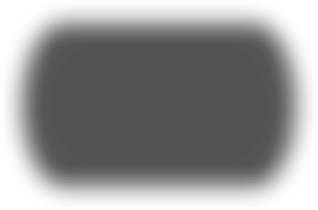
Không giống như các khung bảo mật cơ sở dữ liệu tồn tại ngày nay, chủ yếu phát hiện các vấn đề sắp xảy ra, tạo cảnh báo và tạo báo cáo, giải pháp của chúng tôi, là một thành phần không thể tách rời của cơ sở dữ liệu mà nó có nghĩa là để bảo vệ, tự giảm thiểu mọi rủi ro được phát hiện mà không cần phải chờ sự can thiệp của con người. Để minh họa khái niệm không liên kết này-

Tự bảo vệ bị phá vỡ, chúng tôi trình bày một cái nhìn tổng quan về kiến trúc của khung đề xuất. Lưu ý rằng tất cả các chính sách và thành phần xác minh nằm trong cơ sở dữ liệu là đối tượng được bảo vệ.

Trong kiến trúc này (xem Hình 1), chủ sở hữu hệ thống xây dựng các chính sách để hỗ trợ các mục tiêu nhất định (bước 1). Các chính sách này được lưu trữ trong cùng một cơ sở dữ liệu đang được bảo vệ (cơ sở dữ liệu tar-get) và được sử dụng để xác minh các yêu cầu (hoặc nỗ lực) thay đổi cấu hình cơ sở dữ liệu và thực thi các nhiệm vụ chính trị. Khi người dùng thành thạo hoặc tin tặc bắt đầu nỗ lực thay đổi cấu hình bảo mật (bước 2), nhiệm vụ lại sẽ trải qua quá trình xác minh trước khi có thể được xử lý. Bước này được thực hiện bởi các thủ tục lưu trữ cơ sở dữ liệu có logic tích hợp để kiểm tra yêu cầu đối với các chính sách (bước 3 &; 4). Nếu yêu cầu tuân thủ các chính sách đã đặt chi phối phạm vi áp dụng của yêu cầu (bước 5), thì yêu cầu sẽ được áp dụng. Sau đó, các bảng/dạng xem hệ thống cơ sở dữ liệu được cập nhật để phản ánh sự thay đổi (bước 6) và biên bản kiểm tra được ghi lại (bước 7). Nếu không, nhiệm vụ lại sẽ bị từ chối và chủ sở hữu hệ thống được cảnh báo (bước 8), người dùng được thông báo (bước 9) và dấu vết kiểm tra được ghi lại (bước 10).

Hình 2 cho thấy cách quản lý cơ sở dữ liệu truyền thống

cấu hình bởi quản trị viên cơ sở dữ liệu hoặc bất kỳ người dùng privi-leged nào. DBA đăng nhập vào cơ sở dữ liệu với quyền truy cập đặc quyền và thực hiện các lệnh SQL làm thay đổi cấu hình khẩu phần.



Người dùng/DBA

Yêu cầu thay đổi

KHÔNG

Cho phép?

CÓ

Cập nhật

Hoàn thành thành công

Yêu cầu

Bị từ chối

Thông báo cho người dùng

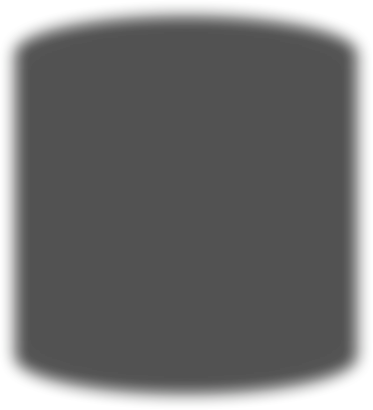
Ghi lại bảng biên bản kiểm tra

Chủ sở hữu hệ thống cảnh báo

Cập nhật bảng/chế độ xem hệ thống cơ sở dữ liệu

Từ chối thay đổi

Kiểm tra chính sách bảo mật



Cơ sở dữ liệu đích

Bảng hệ thống / Chế độ xem

(2)

Cập nhật chế độ xem / bảng hệ thống

(1)

Thực hiện thay đổi

Bảng biên bản kiểm tra

(3)

Phản hồi

DBMS

Trình biên dịch SQL



DBA

Hacker người dùng điện

### Hình 2. Cách tiếp cận truyền thống để quản lý cấu hình cơ sở dữ liệu.

Hình 3 cho thấy sơ đồ của các quy trình liên quan đến việc cung cấp khả năng tự bảo vệ không bị gián đoạn thông qua việc nhúng các khả năng tự chủ vào cơ sở dữ liệu.

## Tích hợp chính sách

Như đã đề cập trước đó, khuôn khổ của chúng tôi được xây dựng dựa trên sự không thể thiếu rằng tất cả các chính sách phải là một phần không thể thiếu của cơ sở dữ liệu mà chúng có nghĩa là để bảo vệ theo cách khiến chúng liên quan trực tiếp đến sự tồn tại của nó. Lưu trữ chúng trong một ứng dụng hoặc cơ sở dữ liệu bên ngoài hoặc thậm chí trong một phiên bản cơ sở dữ liệu khác trên cùng một máy chủ với cơ sở dữ liệu đích, gây ra rủi ro cô lập các chính sách khỏi cơ sở dữ liệu đích và do đó, tạo cơ hội truy cập và xâm phạm cơ sở dữ liệu mà không có bất kỳ dòng de-fense nào. Trong khuôn khổ của chúng tôi, các chính sách được đưa vào các bảng cơ sở dữ liệu vật lý, nơi chúng được lưu trữ và quản lý bởi chủ sở hữu hệ thống. Các bảng này thuộc sở hữu của chính cơ sở dữ liệu và không thể truy cập được đối với các ứng dụng, máy chủ ứng dụng hoặc thậm chí là người dùng thành thạo. Chúng tôi chuẩn hóa việc trình bày các chính sách thành hai bảng chính, đó là TIÊU ĐỀ CHÍNH SÁCH và NHIỆM VỤ CHÍNH SÁCH như thể hiện trong Bảng 1 và 2 be- thấp.

## Đại diện chính sách

Điện toán dựa trên chính sách là một trong một số kỹ thuật được sử dụng để thực hiện các khả năng tự trị trong hệ thống máy tính. Trong bài viết này, chúng tôi áp dụng việc sử dụng các chính sách để áp dụng các khả năng tự trị vào cơ sở dữ liệu. Chúng tôi cho phép chủ sở hữu hệ thống tạo các chính sách dành riêng cho cấu hình cơ sở dữ liệu để quyết định hành vi thời gian chạy thực tế của cơ sở dữ liệu. Các chính sách này kiểm soát và quyết định thay đổi nào thấp và thay đổi nào không. Điều này dựa trên cơ sở dữ liệu

### Hình 3. Lưu đồ của phương pháp tự bảo vệ không bị gián đoạn.

Nhận thức được trạng thái hoạt động của nó có thể tự bảo vệ nó chống lại đầu vào từ nhiều nguồn môi trường khác nhau như người dùng, mã độc hoặc hệ thống phần mềm bên ngoài. Các cơ chế dựa trên chính sách cũng rất hữu ích trong việc thực thi Thỏa thuận mức dịch vụ (SLA), đặc biệt là những cơ chế liên quan đến tính khả dụng và hiệu suất cơ sở dữ liệu quan trọng.

Nói chung, các chính sách cung cấp khả năng kiểm soát

**Bảng 2. NHIỆM VỤ CHÍNH SÁCH**

|  |  |
| --- | --- |
| **NHIỆM VỤ CHÍNH SÁCH** |  |
| ID ỦY NHIỆM | Mã định danh duy nhất của loại chính sách - khóa chính |
| ID CHÍNH SÁCH | Mã định danh duy nhất của chính sách - khóa ngoại |
| PHIÊN BẢN CSDL CHÍNH SÁCH | Tên phiên bản của CSDL cần giám sát |
| THÔNG SỐ CHÍNH SÁCH | Tham số DB là một phần của cấu hình bảo mật tổng thể |
| GIÁ TRỊ THAM SỐ CHÍNH SÁCH | Một giá trị được chỉ định bởi chủ sở hữu hệ thống để được thực thi bởi chính sách |
| CỘT CSDL CHÍNH SÁCH | Cột trong bảng CSDL tham chiếu đến tham số cấu hình |
| CHÍNH SÁCH GIÁ TRỊ DB | Giá trị của cột CSDL tham chiếu đến một tham số cấu hình |
| XÁC MINH THAM SỐ CHÍNH SÁCH | Lệnh DB chọn giá trị của tham số đang được điều tra |
| THAM SỐ CHÍNH SÁCH HỢP LỆ | Một cơ chế để đảm bảo rằng yêu cầu sửa đổi tham số cấu hình DB là hợp lệ |
| TRUY VẤN CHÍNH SÁCH | Một lệnh SQL được sử dụng để giám sát các tài nguyên / hành vi nhất định của DB |
| ĐIỀU KIỆN TRUY VẤN CHÍNH SÁCH | Một điều kiện do chủ sở hữu hệ thống đặt ra để thực thi cấu hình CSDL nhất định cũng như để duy trì  và dự báo mức sử dụng tài nguyên |
| HÀNH ĐỘNG DỰA TRÊN CHÍNH SÁCH | Một hành động mà chính sách đưa ra dựa trên thông tin mà chính sách sở hữu và thông tin mà chính sách thu thập. |
| THỰC THI HÀNH ĐỘNG CHÍNH SÁCH | Chỉ định quy trình được lưu trữ cần được thực hiện để thực hiện hành động cần thiết |

**Bảng 1. TIÊU ĐỀ CHÍNH SÁCH**

|  |  |
| --- | --- |
| **TIÊU ĐỀ CHÍNH SÁCH** |  |
| ID CHÍNH SÁCH | Giá trị nhận dạng duy nhất của chính sách |
| TÊN CHÍNH SÁCH | Tên của chính sách |
| CHỦ HỢP ĐỒNG | Chủ hợp đồng |
| LOẠI CHÍNH SÁCH | Mục tiêu của chính sách như nó  liên quan đến việc bảo mật DB |
| NGÀY TẠO CHÍNH SÁCH | Ngày chính sách được tạo |
| NGÀY SỬA ĐỔI CHÍNH SÁCH | Ngày chính sách được sửa đổi |
| NGÀY HỢP ĐỒNG CÓ HIỆU LỰC | Ngày chính sách có hiệu lực |
| KÍCH HOẠT CHÍNH SÁCH | Chuyển sang BẬT chính sách hoặc  TẮT mà không cần phải xóa nó |
| CƠ SỞ DỮ LIỆU ĐÍCH | Tên của DB chính sách  Áp dụng cho |

Ai có thể làm gì, khi nào, ở đâu và như thế nào. Nhưng việc sử dụng các chính sách cũng có thể được khai thác để dự đoán lý do thực hiện một hành động nhất định, tức là tại sao. Dựa trên các chi tiết cụ thể của hành động, hệ thống có thể thu thập và hình thành thông tin tình báo sẽ là cơ sở để suy luận động cơ đằng sau hành động.

Mục đích của việc sử dụng các chính sách chủ yếu là để thực thi các yêu cầu và ràng buộc của chủ sở hữu sys-tem lên một hệ thống. Một chính sách có thể được coi là một phương tiện khai báo để thể hiện các chỉ thị được thực hiện bởi hệ thống lưu trữ các chính sách này, trong trường hợp này là một công cụ cơ sở dữ liệu. Trong khuôn khổ này, chúng tôi thực hiện các chính sách vào một hệ thống cơ sở dữ liệu với mục đích làm cho cơ sở dữ liệu thực hiện các hành động cụ thể để đáp ứng với các nỗ lực thay đổi trạng thái hoặc cài đặt cấu hình của nó. Do đó, việc tạo ra và thực thi các chính sách đòi hỏi phải thiết lập các quy tắc viện dẫn các hành động nhất định được thực hiện trong các điều kiện nhất định.

Để hỗ trợ khung dựa trên chính sách của chúng tôi, chúng tôi liệt kê bốn loại chính sách mà chúng tôi nhúng vào cơ sở dữ liệu Oracle 10g để chứng minh tính hiệu quả của phương pháp tiếp cận. Dưới đây là ví dụ về các chính sách này. Trong khi xác định pol-icy, chủ sở hữu hệ thống có thể nhập một thẻ đại diện được đại diện bởi \* để chỉ ra rằng một thuật ngữ chính sách nhất định có thể lấy làm đầu vào bất kỳ giá trị nào trong không gian của nó. Họ cũng có thể sử dụng N / A được đại diện bởi # để chỉ ra rằng thuật ngữ này không áp dụng cho kịch bản mà họ quan tâm.

Các chính sách thường được tạo bởi chủ sở hữu hệ thống cho một miền hoặc khu vực áp dụng cụ thể mà chính sách có xu hướng chi phối. Khu vực áp dụng đó được chỉ định bởi loại chính sách. Ví dụ: các chính sách loại một và hai (được định nghĩa bên dưới) nhằm chi phối các lĩnh vực thực thi cấu hình bảo mật trọn đời mật khẩu và giám sát cơ sở dữ liệu, tương ứng, trong khi các chính sách loại ba và bốn chi phối các thay đổi đối với chính sách bảo mật. Bốn loại chính sách được minh họa dưới đây. Các loại chính sách khác cũng có thể được thêm vào tùy thuộc vào nhu cầu.

**Loại 1. Chính sách xác minh và kiểm soát hành động của người dùng** Vai trò của chính sách này là xác minh và kiểm soát hành động của người dùng đặc quyền, chẳng hạn như quản trị viên cơ sở dữ liệu và người dùng thành thạo. Quá trình xác thực được thực hiện như một phản hồi cho đầu vào của người dùng như hình dưới đây. DBA gọi một quy trình được lưu trữ cụ thể để thay đổi thời gian tồn tại của mật khẩu và chọn các giá trị của các tham số mà họ dự định thay đổi. Các giá trị này sau đó được xác minh theo chính sách chi phối khả năng áp dụng của chúng. Như thể hiện trong ví dụ

1.1 (xem Bảng 3), chính sách nêu rõ rằng thời gian tồn tại của mật khẩu được đặt thành 60 ngày và không thể thay đổi. Nó cũng lưu trữ lệnh SQL được sử dụng để xác minh thay đổi và hành động mà nó thực hiện tùy thuộc vào việc thay đổi được chứng minh hay bị từ chối.

### Bảng 3. Ví dụ 1.1

[loại] Thực thi cấu hình bảo mật trọn đời mật khẩu

[tên] Thời gian sống của mật khẩu [tham số] Thời gian sống của mật khẩu [tham số] 60 (ngày)

[xác minh] CHỌN GIỚI HẠN TỪ CẤU HÌNH DBA

TRONG ĐÓ TÊN TÀI NGUYÊN = THỜI GIAN TỒN TẠI CỦA MẬT KHẨU VÀ HỒ SƠ = MẶC ĐỊNH;

[xác nhận] nếu đầu vào = KHÔNG GIỚI HẠN hoặc đầu vào =*/*60

[hành độngrejec] Cảnh báo cho chủ sở hữu hệ thống về nỗ lực không thành công, thông báo cho người dùng về thay đổi tham số không được phép và ghi lại hành động trong biên bản kiểm tra để điều tra thêm

[hành động] Thực thi mật khẩu Life Proc

Trong ví dụ 1.2 (xem Bảng 4), chính sách thực thi chế độ nhật ký lưu trữ của cơ sở dữ liệu. Nỗ lực thay đổi chế độ đó bị từ chối vì chính sách chỉ chấp nhận chế độ nhật ký lưu trữ là TRUE hoặc ARCHIVELOG.

### Bảng 4. Ví dụ 1.2

[loại] thực thi chính sách chế độ lưu trữ DB

[tên] Chế độ nhật ký lưu trữ [tham số] Nhật ký lưu trữ bắt đầu [tham số] THẬT [dbcolumn] Chế độ nhật ký [dbvalue] Lưu trữĐăng nhập

[xác minh] CHỌN CHẾ ĐỘ NHẬT KÝ

TỪ SYS. CƠ SỞ DỮ LIỆU V $;

[xác nhận] nếu CHẾ ĐỘ ĐĂNG NHẬP = NOARCHIVELOG

[hành độngrejec] cảnh báo chủ sở hữu hệ thống về nỗ lực thất bại, thông báo

người dùng thay đổi thông số không được phép và ghi lại hành động trong biên bản kiểm tra để điều tra thêm

[hành động] Thực thi ENF Archive Log Proc

Thuật ngữ [actionexec] của chính sách xác định thủ tục lưu trữ cơ sở dữ liệu sẽ được thực thi. Trong trường hợp ví dụ 1.2, quy trình được lưu trữ sẽ thực hiện một tập hợp các lệnh và / hoặc quy trình để gửi email cho chủ sở hữu hệ thống, bật lên một cửa sổ thông báo để thông báo cho người dùng về kết quả và cuối cùng để ghi lại hành động trong biên bản kiểm tra.

**Loại 2. Chính sách giám sát tài nguyên cơ sở dữ liệu** Vai trò của chính sách này là chủ động giám sát các nguồn tái tạo cơ sở dữ liệu, chẳng hạn như các phiên hoạt động, nhằm mục đích ngăn chặn trước các tình huống có thể làm cạn kiệt máy chủ cơ sở dữ liệu của các tài nguyên quan trọng. Chính sách trong ví dụ 2.1 (xem Bảng 5) hỗ trợ các quy trình được lưu trữ được chỉ định trong việc giám sát và chấm dứt tất cả các phiên mở nhưng không hoạt động. Chính sách nêu rõ rằng thời gian đăng nhập không được quá 24 giờ.

### Bảng 5. Ví dụ 2.1

[loại] Giám sát cơ sở dữ liệu của các phiên không hoạt động

[tên] Giám sát các phiên không hoạt động

[truy vấn] CHỌN TÊN NGƯỜI DÙNG, SID, NỐI TIẾP #, thành char (THỜI GIAN ĐĂNG NHẬP, 'Ngày HH24: MI')

thời gian đăng nhập,

đến char (sysdate, 'Day HH24: MI')

thời gian hiện tại TỪ V$SESSION TRONG ĐÓ STATUS = 'INACTIVE';

[điều kiện] nếu thời gian đăng nhập = thời gian hiện tại + 24

[hành độngrejec] Giết phiên

[hành động] Thực hiện kill session proc

Chính sách trong ví dụ 2.2 (xem Bảng 6) hoạt động tương tự như chính sách trước. Tuy nhiên, nó giám sát CPU mỗi phiên thay vì các phiên không hoạt động. Nó lưu trữ truy vấn được sử dụng để giám sát CPU và các điều kiện phải được đáp ứng và hành động cần thực hiện trong trường hợp không. Mệnh đề điều kiện trong ví dụ 2.2 có thể được nới lỏng một chút bằng cách thay đổi nó thành như sau: nếu CPU MỖI PHIÊN > 70000 hoặc  CPU MỖI PHIÊN < 50000 . Điều này cung cấp cho DBA một số tính linh hoạt trong việc thay đổi cấu hình mà không ảnh hưởng hoặc gây hại cho cơ sở dữ liệu.

### Bảng 6. Ví dụ 2.2

[loại] giám sát cơ sở dữ liệu CPU mỗi phiên

[tên] Giám sát CPU mỗi phiên

[truy vấn] CHỌN TÊN TÀI NGUYÊN,

GIỚI HẠN TỪ CẤU HÌNH DBA TRONG ĐÓ PROFILE = APPUSER VÀ

TÊN TÀI NGUYÊN = CPU MỖI PHIÊN;

[điều kiện] nếu CPU MỖI PHIÊN =*/*60000

[hành độngrejec] cảnh báo chủ sở hữu hệ thống về nỗ lực thất bại,

Thông báo cho người dùng về thay đổi tham số không được phép và ghi lại hành động trong biên bản kiểm tra để điều tra thêm

[hành động] thực thi màn hình CPU proc

**Loại 3. Chính sách thay đổi chính sách bảo mật** Vai trò của chính sách trong ví dụ 3.1 là cho phép chủ sở hữu hệ thống thay đổi các điều kiện được đặt trong chính chính sách bảo mật (xem Bảng 7). So sánh chính sách này với ví dụ 2.1 chỉ ra rằng thời gian đăng nhập đã được đặt thành 12 giờ thay vì 24.

**Loại 4. Chính sách thay đổi tham số chính sách bảo mật Chính sách của** ví dụ 4.1 (xem Bảng 8) cho phép chủ sở hữu hệ thống thực hiện thay đổi đối với giá trị tham số bảo mật của chính chính sách. So sánh chính sách này với một kỳ thi 1.2, chúng tôi thấy rằng chế độ lưu trữ của cơ sở dữ liệu có

### Bảng 7. Ví dụ 3.1

[loại] Thay đổi chính sách giám sát tài nguyên cơ sở dữ liệu [tên] Giám sát tài nguyên thay đổi - Phiên không hoạt động [tham số] #

[giới hạn] #

[xác minh] #

[truy vấn] CHỌN TÊN NGƯỜI DÙNG, SID, NỐI TIẾP #, thành char (THỜI GIAN ĐĂNG NHẬP, 'Ngày HH24: MI')

thời gian đăng nhập,

đến char(sysdate,'Day HH24:MI') thời gian hiện tại FROM V$SESSION

TRONG ĐÓ TRẠNG THÁI = 'KHÔNG HOẠT ĐỘNG';

[điều kiện] Nếu thời gian đăng nhập = thời gian hiện tại + 12

[hành độngrejec] Giết phiên

[hành động] Thực hiện kill session proc

[hiệu quả] ngay lập tức, tức là ngày hệ thống hiện tại

đã thay đổi để cho phép nó ở chế độ nhật ký không lưu trữ.

### Bảng 8. Ví dụ 4.1

[loại] Thay đổi chính sách chế độ lưu trữ cơ sở dữ liệu

[tên] Chế độ nhật ký lưu trữ [tham số] Nhật ký lưu trữ bắt đầu [tham số] SAI [dbcolumn] Chế độ nhật ký [dbvalue] noarchivelog

[hiệu quả] ngay lập tức, tức là ngày hệ thống hiện tại

Có bốn tính năng chính trong cách tiếp cận của chúng tôi giúp nó hiệu quả, có thể mở rộng, linh hoạt và có thể mở rộng. Đầu tiên, chủ sở hữu sys-tem có thể viết nhiều chính sách cần thiết để quản lý một loạt các cấu hình bảo mật cơ sở dữ liệu có khả năng áp dụng toàn cầu hoặc cụ thể. Thứ hai, cấu trúc để xác định một chính sách không bị giới hạn mà có thể được mở rộng để đáp ứng bất kỳ phạm vi áp dụng nào. Thứ ba, thực tế là các chính sách ngắn gọn, có mục tiêu và đơn giản làm cho nhiệm vụ tạo ra chúng trở nên dễ dàng. Cuối cùng, tiền đề của khung này có thể mở rộng ở chỗ nó có thể được áp dụng cho các nguồn điện khác, nơi giám sát hành vi hệ thống hoặc bảo vệ cấu hình hệ thống là điều cần thiết.

# Kịch bản thực hiện

Phần này trình bày một số kịch bản triển khai trong đó khung dựa trên chính sách được sử dụng để tự động thực thi cấu hình bảo mật trong cơ sở dữ liệu, do đó vô hiệu hóa chúng để tự bảo vệ. Để chứng minh khả năng sử dụng của khung đề xuất, chúng tôi xem xét chính sách giám sát các phiên không hoạt động như được trình bày trong Bảng 5.

Đảm bảo rằng mã ứng dụng phần mềm đóng tất cả các phiên mà nó mở sau khi chúng không còn cần thiết nữa là vi-

tal cho hiệu suất cơ sở dữ liệu tối ưu. Tuy nhiên, điều này không xảy ra thường xuyên, đặc biệt là trong một môi trường có áp lực phải giao hàng đúng hạn và nơi các chế độ xem lại mã chính thức không phải là một thực tế phổ biến. Điều này thường dẫn đến tăng số phiên không hoạt động đến mức làm cạn kiệt tài nguyên cơ sở dữ liệu. Mặc dù các tham số cấu hình như thời gian chờ kết nối, maxi- mum và các kết nối tối thiểu được phép có thể được đặt đúng cách, các phiên không hoạt động vẫn có thể tồn tại. Tuy nhiên, điều này có thể dễ dàng được giảm thiểu bằng cách tạo và nhúng chính sách để giám sát tất cả các phiên hoạt động. Cách tiếp cận của chúng tôi làm phong phú cơ sở dữ liệu với các khả năng tự chủ dựa trên chính sách cho phép nó khắc phục vấn đề đó bằng cách tự động thực thi các nhiệm vụ chính sách.

Để thực hiện và thực thi chính sách, một quy trình lưu trữ cơ sở dữ liệu thực thi truy vấn SQL được cung cấp bởi chính sách vài giờ một lần (hoặc theo chỉ định của DBA hoặc chủ sở hữu hệ thống) để xác định thời lượng của mỗi phiên không hoạt động. Nếu điều kiện của chính sách được đáp ứng, thì một thủ tục được lưu trữ khác được thực hiện để giết các phiên vi phạm. Điều này đảm bảo rằng tài nguyên cơ sở dữ liệu không bị cạn kiệt, không có bất kỳ sự can thiệp nào của con người.

Một kịch bản triển khai khác cực kỳ không phù hợp với tính bảo mật của bất kỳ cơ sở dữ liệu nào là thay đổi mật khẩu lược đồ cơ sở dữ liệu hiện có thành một mật khẩu khác trong sáu mươi ngày. Quy tắc này thường được thực thi bởi một hoặc nhiều tham số cấu hình cơ sở dữ liệu. Ví dụ, trong trường hợp cơ sở dữ liệu Oracle, các tham số mật khẩu được đặt trong bảng hệ thống DBA PROFILE.

Các thông số như THỜI GIAN SỬ DỤNG MẬT KHẨU, THỜI GIAN SỬ DỤNG LẠI MẬT KHẨU và THỜI GIAN ÂN HẠN MẬT KHẨU

Kiểm soát các khía cạnh nhất định của mật khẩu cơ sở dữ liệu. Tuy nhiên, vấn đề là các tham số này có thể bị thao túng để cho phép sử dụng cùng một mật khẩu nhiều lần. Bằng cách thực hiện chính sách thời gian sử dụng lại mật khẩu được hiển thị trong Bảng 9, chủ sở hữu hệ thống có thể yên tâm rằng ngay cả DBA cũng không thể sử dụng lại mật khẩu cũ sau khi hết hạn.

Chúng tôi thu hút sự chú ý của người đọc đến thực tế là điều khoản hành động chỉ đơn giản là bắt đầu thông báo cho người dùng về thay đổi tham số không được phép, cảnh báo chủ sở hữu hệ thống về nỗ lực không thành công và bắt đầu ghi lại dấu vết kiểm toán. Không có hành động nào khác được thực hiện.

Cuối cùng, chúng tôi giải quyết kịch bản liên quan đến vấn đề leo thang đặc quyền gián tiếp như nhận DBA privi- leges từ các đặc quyền khác như CREATE ANY TRIG- GER, CREATE ANY VIEW và EXECUTE ANY PRO-

NHƯỢNG BỘ. Trong Oracle 10g Release 2, một tài khoản cơ sở dữ liệu như MDSYS, không phải là DBA, có thể được tận dụng để đạt được các đặc quyền DBA. Điều này có thể được thực hiện thông qua việc tiêm các lệnh SQL vào các trình kích hoạt thuộc sở hữu của MDSYS. Ngoài ra, theo mặc định, trong Oracle 10g Release 2, người dùng duy nhất được cấp đặc quyền CREATE ANY View là SYS.

### Bảng 9. Thực thi chính sách thời gian sử dụng lại mật khẩu.

[loại] Thực thi bảo mật thời gian sử dụng lại mật khẩu

cấu hình

[tên] Thời gian sử dụng lại mật khẩu

[tham số] Thời gian sử dụng lại mật khẩu

[tham số] 20 (lần trước khi mật khẩu có thể được sử dụng lại)

[xác minh] CHỌN GIỚI HẠN TỪ CẤU HÌNH DBA TRONG ĐÓ TÊN TÀI NGUYÊN =

THỜI GIAN SỬ DỤNG LẠI MẬT KHẨU VÀ HỒ SƠ = MẶC ĐỊNH;

[xác nhận] nếu đầu vào = KHÔNG GIỚI HẠN hoặc đầu vào =*/*60

[hành độngrejec] Cảnh báo cho chủ sở hữu hệ thống về nỗ lực không thành công, thông báo cho người dùng về thay đổi tham số bị cấm và ghi lại hành động trong biên bản kiểm tra để điều tra thêm

[hành động] Thực thi mật khẩu Life Proc

Nhưng, nếu một người có thể khai thác một thủ tục dễ bị tổn thương, anh ta / cô ta có thể đạt được các đặc quyền DBA. Chủ đề này đã được minh họa rõ ràng trong tài liệu [20]. Một hacker sẽ cần phải trải qua hai hoặc ba bước đơn giản trước khi anh ta có thể có được quyền riêng tư DBA. Ý tưởng ở dạng đơn giản nhất, trong trường hợp CREATE ANY VIEW, là tìm một thủ tục dễ bị tổn thương do SYS sở hữu và tiêm vào đó một lệnh SQL để cấp đặc quyền DBA cho một người dùng nhất định. Việc tiêm SQL, có thể ở dạng một hàm với một câu lệnh grant đơn giản như cấp dba cho người dùng;, có thể được ngăn chặn bằng cách sử dụng phương pháp tiếp cận dựa trên chính sách của chúng tôi. Để làm điều đó, chủ sở hữu hệ thống tạo trước một chính sách để ngăn chặn việc cấp bất kỳ đặc quyền nào cho bất kỳ người dùng nào trừ khi tên của người dùng đó cùng với các đặc quyền đã thỏa thuận được liệt kê cụ thể trong chính sách. Nói cách khác, DBA phải thảo luận về việc tạo ra một người dùng mới và tập hợp các đặc quyền được cấp cho nó với chủ sở hữu sys-tem. Chủ sở hữu hệ thống lần lượt sẽ sửa đổi chính sách để chấp nhận tài khoản người dùng mới đó và bộ đặc quyền đã thỏa thuận. Bất kỳ nỗ lực nào để cấp đặc quyền, ngoài những đặc quyền được liệt kê trong chính sách, thông qua việc sử dụng SQL injec- tion sẽ không được phép. Xem chính sách trong Bảng 10.

Khi các điều khoản chính sách mới được thêm vào (như trường hợp trong pol-

băng giá ở trên), các cột bảng tương ứng được tự động thêm vào bảng cơ sở dữ liệu ỦY THÁC CHÍNH SÁCH. Cũng cần lưu ý rằng các quy trình được lưu trữ của chúng tôi không cho phép người dùng nhập giá trị vào các biến. Thay vào đó, các thủ tục trình bày cho người dùng một tập hợp các giá trị để lựa chọn. Điều này rất quan trọng vì nó loại bỏ mọi khả năng người dùng đưa các biến thể vào đầu vào dự kiến.

# Công việc liên quan

Việc sử dụng các chính sách đã được áp dụng cho các lĩnh vực như mạng và quản lý mạng [21, 22, 23, 24,

### Bảng 10. Chặn chính sách leo thang đặc quyền gián tiếp.

[loại] Tạo lược đồ CSDL và các đặc quyền được phép [tên] Tạo lược đồ và đặc quyền mới [lược đồ] Người dùng mới

[Vai trò] grant create session cho NewUser, grant select on

schema.table cho NewUser;

[mặc địnhTBS] Người dùng [tạm thời] Temp [quotaType] Vô hạn [hạn ngạch] Người dùng

[hành động] Thực thi Tạo người dùng proc

25, 26], chất lượng kiến trúc dịch vụ và hệ thống quản lý [27, 28], lập trình [29, 30], nhân lực bảo mật [31], hệ thống phân tán dựa trên tác nhân [32], phân bổ mem- ory [33], phân phối nội dung [34], định tuyến [35],

kiểm soát nhập học [36, 37, 38] và tính toán tự động [39, 40]. Tuy nhiên, mối quan tâm của bài viết này là việc áp dụng các chính sách để bảo mật cơ sở dữ liệu. Nhiều công cụ quét và giám sát phần mềm thoát ra trên thị trường hiện nay. Các công cụ như AuditPro for Databases [41], AppDe- tective [42], E-Trust Policy Compliance [43], NGSSQL- Crack [44], Oscanner [45], Symantec Enterprise Security Manager for Databases [46], NeXpose [47], NGSSquirrel for Oracle [48], Appsentry for Oracle [49], ISS Database Scanner [50], SQLdict [51] và NGSSquirrel for SQL [48] đều có một yếu tố chung: tất cả đều tự động hóa và hợp lý hóa việc xác định các lỗ hổng ngoài việc định vị, báo cáo, và thậm chí giúp khắc phục các lỗ hổng bảo mật được phát hiện. Chúng chạy độc lập với cơ sở dữ liệu và nhanh chóng tạo báo cáo chi tiết với tất cả thông tin cần thiết để định cấu hình chính xác và bảo mật cơ sở dữ liệu. Mặc dù các công cụ như vậy có rất nhiều thứ để cung cấp, nhưng thiếu sót lớn của chúng là chúng chạy hoàn toàn độc lập với cơ sở dữ liệu. Việc không cư trú và chạy trên các hệ thống độc lập với cơ sở dữ liệu làm cho các công cụ này dễ bị tổn thương và không đủ để bảo vệ cơ sở dữ liệu.

Một cách tiếp cận khác để bảo mật cơ sở dữ liệu đã được Sentrigo cung cấp thông qua việc cung cấp một nền tảng kiểm toán và giám sát thời gian thực được gọi là Hedgehog [52]. Hedge- hog không giám sát cơ sở dữ liệu thông qua kiểm tra trực tiếp (chặn) các cuộc gọi hệ thống giữa cơ sở dữ liệu và ứng dụng hoặc phân tích tệp nhật ký. Thay vào đó, nó lấy mẫu bộ nhớ dùng chung của cơ sở dữ liệu trong thời gian thực. Mặc dù công nghệ này là gần nhất với cách tiếp cận của chúng tôi, chúng tôi tin rằng cách tiếp cận của chúng tôi linh hoạt hơn vì nó cho phép người dùng tạo ra bất kỳ loại chính sách nào họ muốn. Nó cũng cung cấp cho người dùng khả năng thiết lập các điều kiện chính sách và sửa đổi chúng khi có nhu cầu. Ngoài ra, trong khi Hedgehog có thể được sử dụng để ghi lại các sự kiện, đưa ra cảnh báo và chấm dứt phiên, cách tiếp cận của chúng tôi

chặn các sự kiện trái phép mà không phải đột ngột chấm dứt các phiên. Tóm lại, chủ sở hữu hệ thống kiểm soát việc xây dựng và tùy chỉnh các chính sách của họ để phù hợp nhất với mô hình kinh doanh và nhu cầu kinh doanh của họ. Cách tiếp cận mà chúng tôi trình bày là đóng gói đầy đủ và tích hợp cơ chế bảo vệ vào cốt lõi của cơ sở dữ liệu cần được bảo vệ.

Cách tiếp cận của Ou khác với khái niệm moni- tor tham chiếu bảo mật [53] vì chúng tôi cung cấp khả năng tính toán tự động. Cấu trúc liên kết của Mô hình tham chiếu đặt thành phần "màn hình tham chiếu" như một en-tity riêng biệt với thành phần "tài nguyên". Trên thực tế, mô hình al- thấp để thực hiện một màn hình tham chiếu cho nhiều tài nguyên và nhiều màn hình tham chiếu cho các tài nguyên mul-tiple. Điều này trái ngược trực tiếp với cách tiếp cận được đề xuất của chúng tôi, làm cho việc thực hiện cơ chế thực thi bảo mật (tương tự như màn hình tham chiếu) trở thành một phần không thể tách rời và không thể tách rời của hệ thống (hoặc tài nguyên) mà nó đang bảo vệ.

# Kết luận và công việc trong tương lai

Bài viết này trình bày một cách tiếp cận sáng tạo để đưa các khả năng tự chủ vào các hệ thống cơ sở dữ liệu trong or-der để cho phép tự bảo vệ. Nền tảng của ap-proach của chúng tôi là tích hợp đầy đủ các chính sách bảo mật vào cơ sở dữ liệu mà chúng nhằm bảo vệ. Bằng cách đó, chúng tôi nhúng vào các khả năng tự chủ của cơ sở dữ liệu để cung cấp cho nó một cơ chế tự bảo vệ vượt trội, về hiệu quả của nó, khung bảo mật cơ sở dữ liệu hiện có- hoạt động. Bài viết này tập trung vào cách tiếp cận và các khía cạnh chính sách. Một bài báo đi kèm sẽ trình bày chi tiết cơ chế cho phép cơ sở dữ liệu có khả năng tự bảo vệ thông qua việc sử dụng các quy trình được lưu trữ cơ sở dữ liệu hoạt động như công cụ cho phép xác minh yêu cầu, biên soạn lệnh, bảo vệ cơ sở dữ liệu và thông báo cho chủ sở hữu hệ thống và người dùng.

# Tham khảo

1. Menasce', D.A. và J.O. Kephart, "Autonomic Comput- ing," Giới thiệu khách mời. IEEE Internet Comput- ing, 2007. 11(1).
2. FISMA,"Đạo luật Quản lý An ninh Thông tin Liên bang năm 2002. FISMA," Tiêu đề III của Đạo luật Chính phủ điện tử được Quốc hội thứ 107 thông qua và được hát thành luật bởi persi-dent, 44 U.S.C. 3541, et seq., 2002.
3. Chi nhánh Hành pháp Hoa Kỳ, Bộ Nội địa Secu- rity, Chỉ thị của Tổng thống An ninh Nội địa / HSPD-7. [www.whitehouse.gov,](http://www.whitehouse.gov/) 2003.
4. Martin, P., S. Elnaffar và T. Wasserman, "Mô hình khối lượng công việc cho các hệ thống quản lý cơ sở dữ liệu tự trị". IEEE, 2006.
5. Chen, J., G. Soundararajan và C. Amza, "Tự động cung cấp cơ sở dữ liệu phụ trợ trong các máy chủ web nội dung động". IEEE, 2006: trang 231-242.
6. Bruno, N. và S. Chaudhuri, "Điều chỉnh cơ sở dữ liệu vật lý tự động: Cách tiếp cận dựa trên thư giãn". SIG- MOD, ACM, 2005.
7. Oh, JS và S.H. Lee, "Lựa chọn tài nguyên để điều chỉnh cơ sở dữ liệu tự động". Proc. 21st Intl. Conf. on Data Engineering (ICDE' 05), IEEE, 2005.
8. Boughton, H., et al., "Workload Class Importance Pol- icy in Autonomic Database Management Systems". GS. Hội thảo quốc tế IEEE lần thứ 7 về chính sách cho hệ thống và mạng phân tán (POLICY'06), 2006.
9. Taton, C., et al., "Tự định cỡ cơ sở dữ liệu cụm". Proc. Symp. World of Wireless, Mobile and Multimedia, IEEE, 2006.
10. Tian, W., P. Martin và W. Powley, "Kỹ thuật tự động định cỡ nhiều vùng đệm trong DB2". Đại học Queens, 2001.
11. Ammann, P., S. Jajodia và P. Liu, "Phục hồi từ các giao dịch ma thuật". IEEE Tr. Kiến thức và Dữ liệu En- gineering, 2002. 14(5).
12. Liu, P., "Dais: Hệ thống cách ly tấn công thời gian thực cho cơ sở dữ liệu thương mại". GS. 17th Annual Computer Se- curity Applications Conf., 2001.
13. Bertino, E. và R. Sandhu, "Bảo mật cơ sở dữ liệu - Nhận thức, phương pháp tiếp cận và thách thức". IEEE Tr. Máy tính đáng tin cậy và an toàn, 2005. 2(1).
14. Jeong, M.-A., J.-J. Kim và Y. Won, "Một hệ thống bảo mật cơ sở dữ liệu linh hoạt sử dụng nhiều chính sách kiểm soát truy cập". Proc. 4th Intnl. Conf. Điện toán song song và phân tán, Ứng dụng và Công nghệ, 2003. PD- CAT'2003, 2003.
15. Kern, A., et al., "Mô hình Meta cho các ủy quyền trong hệ thống bảo mật ứng dụng và tích hợp chúng vào quản trị RBAC". ACM, SACMAT, 2004.
16. Conry-Murray, A., "Mối đe dọa từ bên trong". [www.networkcomputing.com,](http://www.networkcomputing.com/) 2005.
17. Stanley, N., DBA Dnaffles Data - Mối đe dọa bên trong tiếp tục. [www.it-analysis.com,](http://www.it-analysis.com/) 2007.
18. Stiennon, R., DBA của bạn có bàn tay của anh ấy / cô ấy trong cày. [www.zdnet.com,](http://www.zdnet.com/) 2007.
19. CNNMoney, vi phạm an ninh ngân hàng có thể là lớn nhất. CNNMoney.com, 2005.
20. Litchfield, D., *The Oracle Hacker's Handbook: Hacking and Defending Oracle*. 2007.
21. Bao, J.Q., L. Guo và W.C. Lee, "Mạng đặc biệt: Phân bổ nguồn lực dựa trên chính sách trong mạng an toàn công cộng không dây để quản lý hiện trường sự cố". Proc. 2006 Wkshp. Các vấn đề về độ tin cậy trong mạng Ad-hoc không dây và mạng cảm biến DIWANS '06, 2006.
22. Itani, W., A. Kayssi và A. Chehab, "T1-B: hội nghị chuyên đề an ninh mạng và máy tính: Giao thức bảo mật dựa trên chính sách doanh nghiệp để bảo vệ các đối tượng mạng cơ sở dữ liệu quan hệ". Proc. 2006 Intl. Conf. Truyền thông không dây và Điện toán di động IWCMC '06, 2006.
23. Wright, M.J., "Sử dụng các chính sách để quản lý mạng hiệu quả," *Intl. J. Network Management*, 1999.
24. Kim, G., J. Kim và J. Na, "Thiết kế và thực hiện điểm quyết định chính sách trong mạng lưới dựa trên chính sách". GS. Hội nghị quốc tế ACIS thường niên lần thứ 4 về Khoa học Máy tính và Thông tin (ICIS05), 2005.
25. Perez, GM, et al., "Quản lý mạng dựa trên chính sách năng động cho một môi trường liên minh an toàn". Tạp chí Truyền thông IEEE 2006.
26. Olaussen, E. và A. Karlsen, "Một khung ưu tiên và ưu tiên dựa trên chính sách cho các mạng IP quân sự". Hội nghị Truyền thông Quân sự, MILCOM 2004. IEEE, 2004.
27. Rudack, M., et al., "Bản đồ chất lượng dịch vụ dựa trên chính sách trong các hệ thống phân tán". Hội nghị chuyên đề quản lý và vận hành mạng, NOMS 2002, IEEE / IFIP, 2002.
28. Flegkas, P., P. Trimintzios và G. Pavlou, "Một hệ thống quản lý chất lượng dịch vụ dựa trên chính sách cho các mạng IP Diff- Serv". Mạng IEEE, 2002.
29. Montanari, R., G. Tonti và C. Stefanelli, "Tách biệt mối quan tâm dựa trên chính sách đối với người quản lý di động mã động". Proc. 27th Annual Intl. Computer Software and Applications Conf., COMPSAC 2003, 2003.
30. McDaniel, P., "Về bối cảnh trong chính sách ủy quyền". Triệu chứng ACM thứ 8. Mô hình và công nghệ kiểm soát truy cập, 2003.
31. Bhatti, R., K. Moidu và A. Ghafoor, "Tích hợp và trao đổi dữ liệu chăm sóc sức khỏe: Quản lý bảo mật dựa trên chính sách cho cơ sở dữ liệu chăm sóc sức khỏe liên kết (hoặc RHIO)". Proc. Intl. Wkshp. Thông tin chăm sóc sức khỏe và quản lý bí quyết (HIKM '06), 2006.
32. Tripathi, A., D. Kulkarni và T. Ahmed, "Cấu hình và quản lý theo hướng chính sách của các hệ thống phân tán dựa trên tác nhân". 4th Intl. Wkshp. Software En- gineering for Large-Scale Multi-Agent Systems (SEL- MAS'05), 2005.
33. Alexandrescu, A. và E. Berger, "Phân bổ Mem-ory dựa trên chính sách: Tinh chỉnh quản lý bộ nhớ của bạn", Tạp chí C / C ++ của Tiến sĩ Dobb, 2005.
34. Kawarasaki, M. và R. Atarashi, "Quản lý phân phối lều dựa trên chính sách sử dụng siêu dữ liệu". Proc. IEEE 2004 Intl. Symp. Applications and the Internet Work- shops (SAINTW'04), 2004.
35. Chau, C.-k., "Định tuyến dựa trên chính sách với các ưu tiên không nghiêm ngặt". SIGCOMM 2006, 2006.
36. Verdi, FL, M. Magalhaes và E.R.M. Madeira, "Kiểm soát nhập học dựa trên chính sách trong mạng quang GMPLS". Proc. First Intl. Conf. Mạng băng thông rộng (BROAD- NETS04), 2004.
37. Yan, Y., et al., "A policy-based admission control algo- rithm for UMTS end to end QoS provision". 2nd Intl. Conf. Công nghệ di động, Ứng dụng và Hệ thống, 2005.
38. Ramirez, SL, et al., "Đánh giá hiệu suất của các thuật toán kiểm soát nhập học dựa trên chính sách cho môi trường quản lý tài nguyên Ra-dio chung". Hội nghị Electrotechni-cal, MELECON 2006. IEEE Địa Trung Hải, 2006.
39. Badr, N., A. Taleb-Bendiab, và D. Reilly, "Dịch vụ kiểm soát tự trị dựa trên chính sách". GS. 5th IEEE Intl. Wkshp. Chính sách cho các hệ thống và mạng phân tán (POLICY'04), 2004.
40. Chan, H. và T. Kwok, "Một hệ thống quản lý dựa trên chính sách với khả năng lựa chọn và tạo chính sách tự động bằng cách sử dụng kỹ thuật phân tách giá trị đơn lẻ". Proc. 7th Intl. Wkshp. Chính sách cho các hệ thống và mạng phân phối (POLICY'06), 2006.
41. AuditPro, Mạng Thông minh (I) Pvt. Ltd. [www.niiconsulting.com.](http://www.niiconsulting.com/)
42. AppDetectivePro, Bảo mật ứng dụng, Inc. [www.appsecinc.com/products/appdetective/.](http://www.appsecinc.com/products/appdetective/)
43. Tin tưởng điện tử Chính sách Tuân thủ. Ser- phó chiến lược, Inc., www.ebusiness- Chính sách security.com/eTrust compliance.htm.
44. NGSSQLCrack, Phần mềm bảo mật thế hệ tiếp theo,. [www.ngssoftware.com/products/database-security/ngs- sqlcrack.php](http://www.ngssoftware.com/products/database-security/ngs-) .
45. Karlsson, P., OScanner cho Oracle, 2004.
46. Symantec Xí nghiệp An ninh Man- agerł cho Cơ sở dữ liệu,. Symantec, [www.symantec.com/region/can/eng/product/esm/databases.](http://www.symantec.com/region/can/eng/product/esm/databases)
47. NeXposeł, Rapid7. [www.rapid7.com.](http://www.rapid7.com/)
48. NGSSQuirreL, Phần mềm bảo mật thế hệ tiếp theo. [www.ngssoftware.com/products/database-security/ngs-](http://www.ngssoftware.com/products/database-security/ngs-) squirrel-oracle.php.
49. Appsentry, Tích hợp Công ty. [www.integrigy.com/products.](http://www.integrigy.com/products)
50. ISS, Máy quét cơ sở dữ liệu ISS. Internet Security Systems, Inc., www.iss.net/about/index.html.
51. SQLdict, ntsecurity. [www.ntsecurity.nu/toolbox/sqldict/.](http://www.ntsecurity.nu/toolbox/sqldict/)
52. Nhím, Sentrigo. [www.sentrigo.com/.](http://www.sentrigo.com/)
53. Anderson, J.P., Computer Security Technology Planning Study, ESD-TR-73, Vol. II, October 1972.