

KHẮC PHỤC SỰ CỐ CÁC VẤN ĐỀ ĐĂNG NHẬP

Brien M. Posey

Quản trị mạng - Việc đăng nhập vào máy tính là một hành động quá đỗi thường xuyên trong ngày đến nỗi người ta không hề nghĩ đó là một quá trình. Tuy vậy vẫn có nhiều vấn đề có thể và đôi khi xảy ra khi người dùng đăng nhập vào Windows. Bài viết này chúng tôi sẽ giới thiệu một số nguyên nhân gây ra lỗi trong quá trình đăng nhập trong môi trường Active Directory.

Trước khi bắt đầu

Trước khi bắt đầu, chúng tôi muốn đề cập nhanh một số vấn đề nhằm cung cấp cho các bạn các thông tin hữu ích, tuy nhiên sẽ tránh nói về các nguyên nhân gây ra lỗi đăng nhập. Thừa nhận rằng trước khi bắt đầu quá trình khắc phục sự cố, bạn đã kiểm tra và bảo đảm rằng người dùng truy cập đúng một khẩu và mật khẩu của người dùng không bị hết hạn, bên cạnh đó không có bất cứ vấn đề về truyền thông cơ bản nào giữa máy trạm và domain controller.

Clock hệ thống

Có thể dường như khác kỳ cục nhưng clock của máy trạm có thể là nguyên nhân gây ra lỗi đăng nhập. Vì nếu clock khác hơn 5 phút so với thời gian trên các domain controller của bạn thì đăng nhập sẽ bị lỗi.

Bắt đầu quá trình thẩm định, người dùng nhập vào username và password của họ. Sau đó máy trạm sẽ gửi Kerberos Authentication Server Request đến Key Distribution Server. Kerberos Authentication Server Request sẽ gồm một số thông tin như:

Nhận dạng người dùng.

Tên của dịch vụ mà người dùng yêu cầu (trong trường hợp này nó chính là Ticket Getting Service).

Thẩm định được mã hóa với khóa chủ của người dùng. Khóa chủ của người dùng này được phân phối bởi việc mã hóa mật khẩu của người dùng bằng hàm một chiều.

Khi Key Distribution Server nhận được yêu cầu, nó sẽ tra cứu tài khoản Active Directory của người dùng. Sau đó sẽ tính toán khóa chủ của họ và sử dụng nó để giải mã thẩm định (cũng được biết đến như dữ liệu tiền thẩm định).

Khi máy trạm của người dùng đã tạo dữ liệu tiền thẩm định, nó đặt một tem thời gian bên trong file mã hóa. Khi Key Distribution Server mã hóa file này, nó sẽ so sánh tem thời gian này với thời gian hiện hành trên clock của chính nó. Nếu tem thời gian này và thời gian hiện hành khác nhau

không đến 5 phút thì Kerberos Authentication Server Request được thừa nhận hợp lệ, khi đó quá trình thẩm định sẽ tiếp tục. Còn nếu tem thời gian và thời gian hiện hành khác nhau hơn 5 phút thì Kerberos thừa nhận rằng yêu cầu là một replay của gói đã được capture trước đó và vì vậy từ chối yêu cầu đăng nhập. Khi xảy ra điều này, thông báo dưới đây sẽ được hiển thị:

Hệ thống không thể đăng nhập do lỗi sau: Có sự khác biệt về thời gian giữa máy chủ và khách. Xin vui lòng thực hiện đăng nhập lại hoặc liên hệ với quản trị viên hệ thống.

Giải pháp để giải quyết vấn đề này rất đơn giản; chỉ cần thiết lập clock của máy trạm phù hợp với clock của domain controller.

Các lỗi Global Catalog Server

Một nguyên nhân khác của các vấn đề đăng nhập là lỗi global catalog server. Global catalog server là một domain controller được cấu hình để thực hiện vài trò của nó. Các máy chủ này gồm có trình diễn tìm kiếm các đối tượng trong các miền của toàn bộ forest.

Khi forest mới bắt đầu được tạo, domain controller đầu tiên mà bạn đưa vào hoạt động sẽ tự động được cấu hình thực hiện vai trò như global catalog server. Tuy nhiên vấn đề ở đây là, máy chủ có thể trở thành một lỗi, vì Windows không tự động chỉ định các domain controller khác để thực hiện vai trò global catalog server. Nếu global catalog server xuất hiện lỗi thì lúc này chỉ có các quản trị viên miền mới có khả năng đăng nhập vào Active Directory.

Nắm được tầm quan trọng của máy chủ global, bạn cần phải thực hiện các biện pháp nhằm ngăn chặn lỗi cho chúng. Một may mắn ở đây là bạn có thể chỉ định bất kỳ hoặc tất cả các domain controller của mình thực hiện vai trò global catalog server. Cũng nên lưu ý rằng bạn chỉ phải cấu hình tất cả các domain controller để thực hiện vài trò global catalog server nếu forest của bạn gồm có miền đơn. Việc có nhiều global catalog server là một giải pháp tốt hơn cả cho các forest đa miền, tuy nhiên việc chỉ ra các domain controller nào sẽ thực hiện vai trò của các global catalog server nào lại là một vấn đề cần phải lưu ý.

Nếu global catalog server của bạn đã bị lỗi và không ai có thể đăng nhập, khi đó cách tốt nhất mà bạn có thể thực hiện là quay trở về trạng thái thiết thực global catalog server. Có một cách cho phép người dùng có thể đăng nhập thậm chí khi global catalog server gặp lỗi, tuy nhiên lại có những rủi ro bảo mật liên quan đến vấn đề này.

Nếu Active Directory đang hoạt động trong chế độ nguyên bản, thì máy chủ global sẽ chịu trách nhiệm kiểm tra các thành viên trong nhóm phổ dụng của người dùng. Nếu bạn cho phép người dùng đăng nhập trong suốt quá trình lỗi thì các thành viên nhóm phổ dụng sẽ không được kiểm tra. Nếu đã gán các hạn chế cụ thể cho các thành viên của nhóm phổ dụng nào đó thì các hạn chế này sẽ không có hiệu lực cho tới khi global catalog server hoạt động trở lại.

Nếu quyết định rằng bạn phải cho phép người dùng đăng nhập thì bạn phải edit registry trên mỗi domain controller. Lưu ý rằng việc edit registry là rất nguy hiểm, nếu mắc phải một lỗi nào đó thì có thể sẽ làm nguy hại cho hệ điều hành Windows. Chính vì vậy hãy tạo một backup toàn bộ hệ thống trước khi bạn thực hiện các soạn thảo này.

Mở Registry Editor và điều hướng đến HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa.

Tạo một giá trị DWORD mới có tên IgnoreGCFailures, và thiết lập giá trị bằng 1. Bạn phải khởi động lại domain controller sau khi thực hiện thay đổi này.

Lỗi DNS Server

Nếu bạn bất ngờ phát hiện thấy rằng không có user nào đăng nhập trong mạng và các domain controller và các global catalog server của bạn vẫn đang làm việc thì khi đó có thể do lỗi DNS

server. Active Directory hoàn toàn phụ thuộc vào các dịch vụ DNS.

Máy chủ DNS có chứa các bản ghi cấu hình chủ cho mỗi máy tính trong mạng. Các máy tính trong mạng của bạn sử dụng các bản ghi cấu hình này để so sánh tên máy tính với địa chỉ IP. Nếu lỗi của máy chủ DNS xuất hiện thì hoạt động host name này cũng sẽ bị lỗi và ảnh hưởng đến quá trình đăng nhập.

Có hai vấn đề ở đây bạn cần biết về các lỗi DNS có liên quan đến vấn đề khắc phục các vấn đề đăng nhập. Đầu tiên là các lỗi đăng nhập có thể không xảy ra ngay lập tức. Hệ điều hành Windows sẽ giữ một cache DNS gồm có các kết quả của các truy vấn DNS trước đó. Cache này tránh cho các máy trạm làm lộn các máy chủ DNS bởi các truy vấn về tên cho các đối tượng liên tiếp xuất hiện.

Trong nhiều trường hợp, các máy trạm sẽ lưu các địa chỉ IP của các domain controller và global catalog server. Tuy nhiên, các mục trong cache DNS thực hiện thao tác hết hạn và sẽ cần được refresh. Bạn sẽ thấy được các vấn đề đăng nhập khi các bản ghi host đã lưu bắt đầu hết hạn.

Một thứ khác mà bạn cần biết về các lỗi máy chủ DNS là có khá nhiều triệu chứng khác bên cạnh các lỗi đăng nhập. Trừ khi các máy tính trên mạng của bạn được cấu hình sử dụng máy chủ DNS cấp thứ trong sự kiện DNS server chính bị lỗi thì toàn bộ môi trường Active Directory sẽ ngừng hẳn lại. Mặc dù có những ngoại lệ xong nhìn chung sự thiếu DNS server trong mạng Active Directory thường liên quan đến việc làm ngắt quãng sự truyền thông.

Kết luận

Mặc dù chúng tôi đã thảo luận một số nguyên nhân chính gây ra các lỗi đăng nhập trong các mạng Active Directory nhưng một phần quan trọng của quá trình khắc phục sự cố chính là xem xét vấn đề này như lan rộng như thế nào. Cho ví dụ, nếu chỉ một host nào đó trong một mạng lớn đang có các vấn đề đăng nhập thì bạn có thể loại trừ các lỗi DNS hoặc global catalog. Nếu một lỗi DNS hoặc một lỗi global catalog xuất hiện thì vấn đề sẽ phải rộng hơn rất nhiều. Nếu bị cách ly trong một máy đơn lẻ thì vấn đề có thể chỉ liên quan đến cấu hình, kết nối của máy hoặc tài khoản của người dùng.