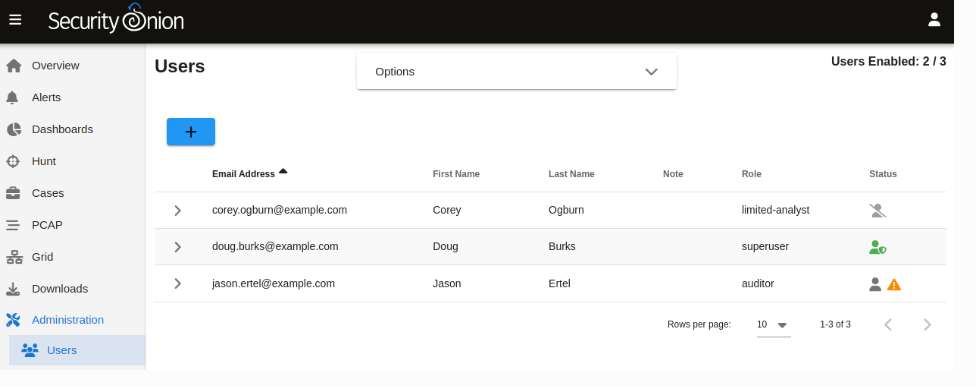
**Nội dung**

**+ Administator**

[Security Onion Console (SOC)](https://docs.securityonion.net/en/2.4/soc.html" \l "soc) bao gồm phần Quản trị cho phép bạn quản trị Người dùng, Thành viên lưới và Cấu hình.

## **Người dùng**

Trang Người dùng hiển thị tất cả tài khoản người dùng đã được tạo cho lưới.



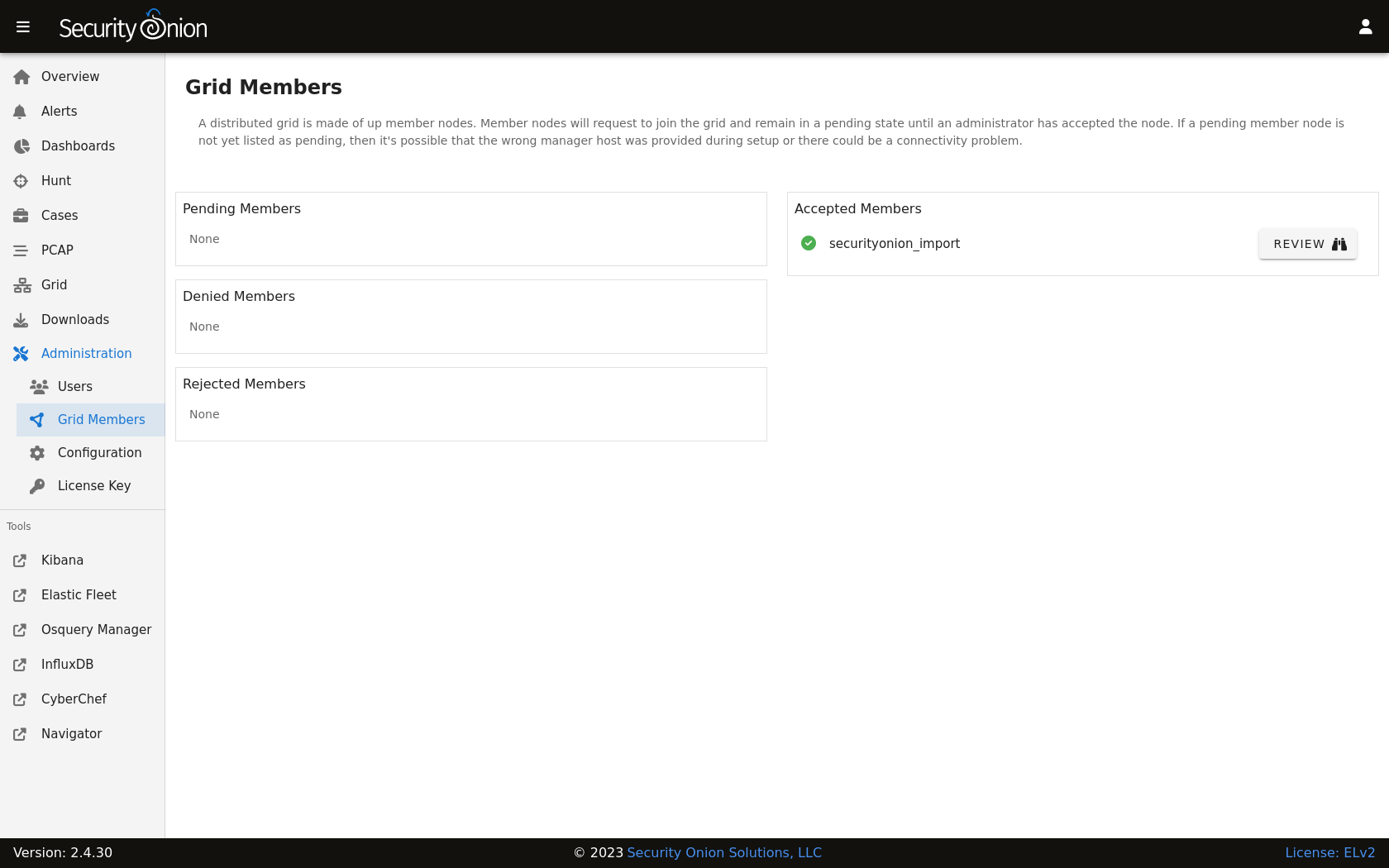
Cột Vai trò liệt kê các vai trò được gán cho người dùng như được xác định trong phần [Kiểm soát truy cập dựa trên vai trò (RBAC)](https://docs.securityonion.net/en/2.4/rbac.html" \l "rbac) .

Cột Trạng thái sẽ hiển thị các biểu tượng khác nhau tùy theo trạng thái của tài khoản. Trong ảnh chụp màn hình ở trên:

* tài khoản đầu tiên bị vô hiệu hóa
* tài khoản thứ hai đã được bật và đã bật TOTP [MFA](https://docs.securityonion.net/en/2.4/mfa.html" \l "mfa)
* tài khoản thứ ba đã được kích hoạt nhưng chưa kích hoạt TOTP [MFA](https://docs.securityonion.net/en/2.4/mfa.html" \l "mfa) và chưa thay đổi mật khẩu

## **Thành viên lưới**

Trang Thành viên lưới hiển thị các nút đã cố gắng tham gia vào lưới và liệu chúng có được quản trị viên chấp nhận vào lưới hay không.

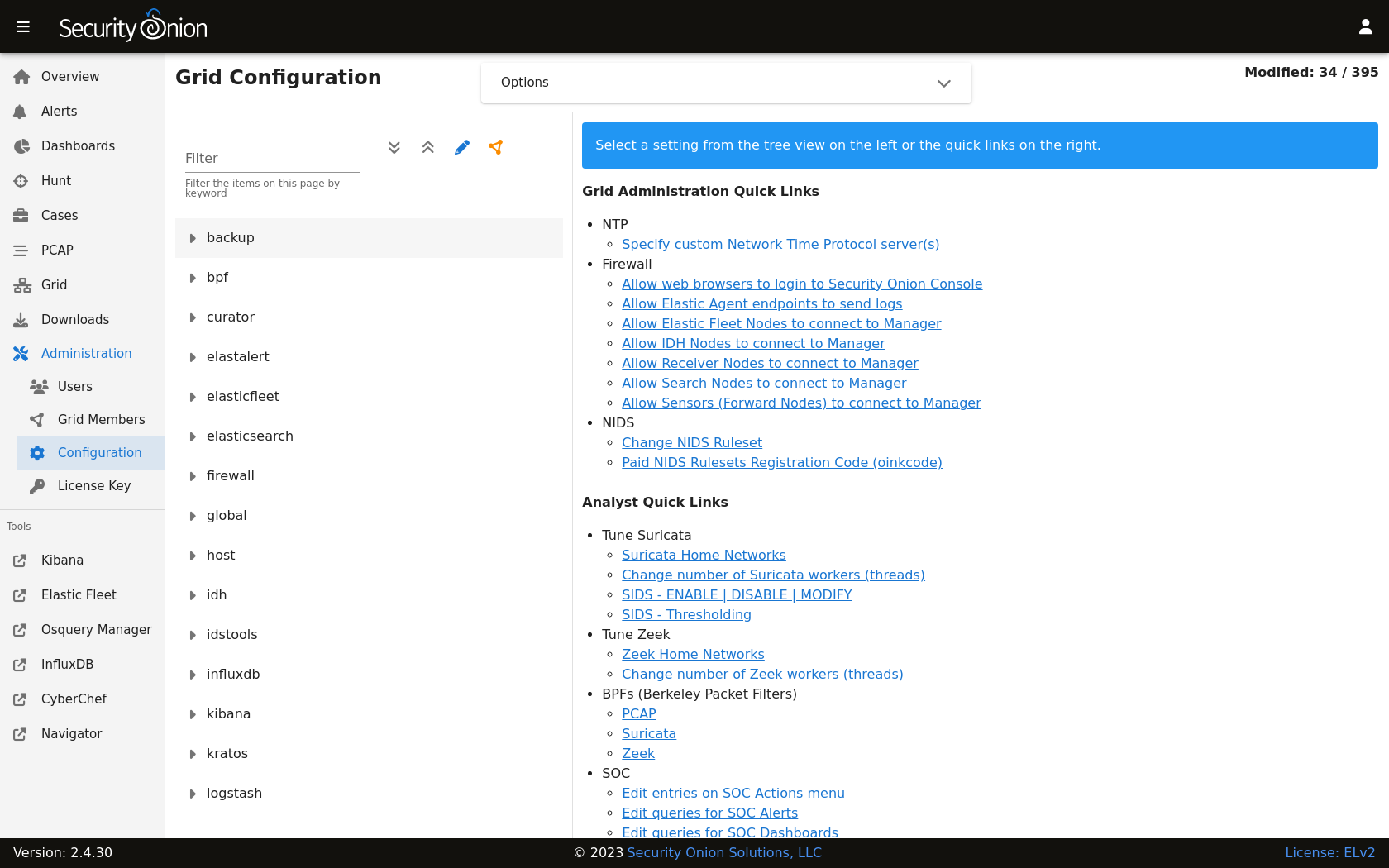
[](https://docs.securityonion.net/en/2.4/_images/60_gridmembers.png)

Thành viên không được chấp nhận được hiển thị ở phía bên trái và được chia thành ba phần: Thành viên đang chờ xử lý, Thành viên bị từ chối và Thành viên bị từ chối. Khi bạn chấp nhận một thành viên, thành viên đó sẽ chuyển sang bên phải bên dưới Thành viên được chấp nhận.

Đối với các thành viên được chấp nhận, bạn có thể nhấp vào nút ĐÁNH GIÁ để hiển thị thông tin bổ sung về thành viên lưới. Nếu bạn muốn xóa thành viên, bạn có thể nhấp vào nút XÓA và xem lại xác nhận.

## **Cấu hình**

Trang Cấu hình cho phép bạn định cấu hình các thành phần khác nhau của lưới.

[](https://docs.securityonion.net/en/2.4/_images/61_config.png)

Các tùy chọn cấu hình phổ biến nhất được hiển thị trong các liên kết nhanh ở bên phải. Ở phía bên trái, bạn có thể nhấp vào một thành phần trong chế độ xem dạng cây để đi sâu vào thành phần đó và hiển thị tất cả các cài đặt có sẵn cho thành phần đó. Sau đó, bạn có thể nhấp vào cài đặt để hiển thị cài đặt hiện tại hoặc sửa đổi cài đặt đó nếu cần. Nếu mắc lỗi, bạn có thể dễ dàng quay lại giá trị mặc định. Nếu dấu chấm hỏi màu xanh xuất hiện trên trang cài đặt, bạn có thể nhấp vào dấu chấm hỏi đó để đi tới tài liệu về thành phần đó.

Nếu bạn không chắc chắn cài đặt cụ thể có thể thuộc về thành phần nào, bạn có thể sử dụng Bộ lọc ở đầu danh sách để tìm cài đặt cụ thể. Ở bên phải trường Bộ lọc là các nút thực hiện các chức năng sau:

* mở rộng tất cả cài đặt
* thu gọn tất cả cài đặt
* hiển thị cài đặt đã được sửa đổi từ giá trị mặc định
* hiển thị cài đặt có giá trị duy nhất được chỉ định cho một hoặc nhiều nút trong lưới

CyberChef là một ứng dụng web đơn giản, trực quan để thực hiện tất cả các hoạt động “mạng” trong trình duyệt web. Các hoạt động này bao gồm mã hóa đơn giản như XOR hoặc Base64, mã hóa phức tạp hơn như AES, DES và Blowfish, tạo nhị phân và hexdumps, nén và giải nén dữ liệu, tính toán băm và tổng kiểm tra, phân tích cú pháp IPv6 và X.509, thay đổi mã hóa ký tự, v.v. .

Công cụ này được thiết kế để cho phép cả nhà phân tích kỹ thuật và phi kỹ thuật thao tác dữ liệu theo những cách phức tạp mà không cần phải xử lý các công cụ hoặc thuật toán phức tạp.

CyberChef là một công cụ mã nguồn mở và trực tuyến được sử dụng trong lĩnh vực an ninh mạng và phân tích dữ liệu. Nó cung cấp một giao diện dễ sử dụng cho việc thực hiện các phép biến đổi, mã hóa, giải mã và xử lý dữ liệu theo nhiều định dạng khác nhau.

Với CyberChef, người dùng có thể thực hiện nhiều tác vụ xử lý dữ liệu, bao gồm:

Mã hóa và giải mã: CyberChef hỗ trợ nhiều thuật toán mã hóa và giải mã như Base64, Hex, URL, ROT13, XOR, AES và nhiều hơn nữa. Người dùng có thể mã hóa và giải mã các chuỗi dữ liệu dễ dàng chỉ bằng một vài cú nhấp chuột.

Xử lý dữ liệu: CyberChef cung cấp các công cụ xử lý dữ liệu linh hoạt như tách chuỗi, ghép chuỗi, cắt, lọc và định dạng lại dữ liệu. Điều này cho phép người dùng thực hiện các tác vụ phức tạp như phân tích log, xử lý dữ liệu đầu vào và đầu ra từ các công cụ khác nhau.

Phân tích định dạng: CyberChef hỗ trợ phân tích các định dạng dữ liệu phổ biến như JSON, XML, CSV và nhiều hơn nữa. Người dùng có thể chuyển đổi dữ liệu từ một định dạng sang định dạng khác và thực hiCyberChef là một công cụ mã nguồn mở và trực tuyến được sử dụng trong lĩnh vực an ninh mạng và phân tích dữ liệu. Nó cung cấp một giao diện dễ sử dụng cho việc thực hiện các phép biến đổi, mã hóa, giải mã và xử lý dữ liệu theo nhiều định dạng khác nhau.

Với CyberChef, người dùng có thể thực hiện nhiều tác vụ xử lý dữ liệu, bao gồm:

Mã hóa và giải mã: CyberChef hỗ trợ nhiều thuật toán mã hóa và giải mã như Base64, Hex, URL, ROT13, XOR, AES và nhiều hơn nữa. Người dùng có thể mã hóa và giải mã các chuỗi dữ liệu dễ dàng chỉ bằng một vài cú nhấp chuột.

Xử lý dữ liệu: CyberChef cung cấp các công cụ xử lý dữ liệu linh hoạt như tách chuỗi, ghép chuỗi, cắt, lọc và định dạng lại dữ liệu. Điều này cho phép người dùng thực hiện các tác vụ phức tạp như phân tích log, xử lý dữ liệu đầu vào và đầu ra từ các công cụ khác nhau.

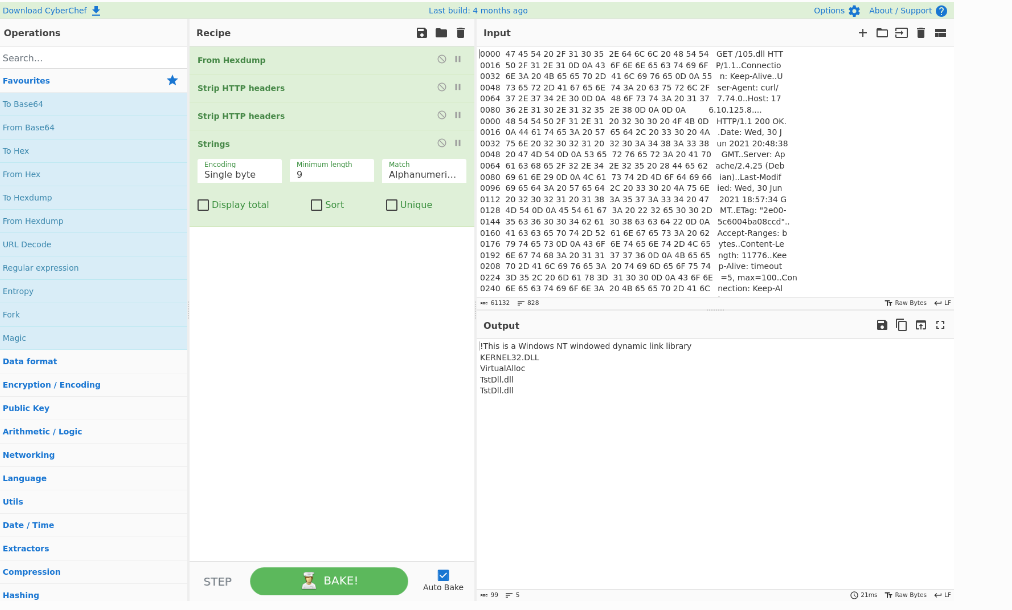
Phân tích định dạng: CyberChef hỗ trợ phân tích các định dạng dữ liệu phổ biến như JSON, XML, CSV và nhiều hơn nữa. Người dùng có thể chuyển đổi dữ liệu từ một định dạng sang định dạng khác và thực hiện các thao tác phân tích dữ liệu cơ bản.

Xử lý chuỗi ký tự: CyberChef cung cấp các công cụ để thực hiện các phép biến đổi và xử lý chuỗi ký tự như tìm kiếm, thay thế, mã hóa, giải mã và nhiều hơn nữa. Điều này rất hữu ích trong việc xử lý và phân tích các chuỗi dữ liệu như địa chỉ email, địa chỉ IP, địa chỉ URL và thông tin nhận dạng khác.

CyberChef là một công cụ mạnh mẽ và linh hoạt, được sử dụng rộng rãi trong cộng đồng an ninh mạng và phân tích dữ liệu để thực hiện các tác vụ xử lý dữ liệu và phân tích dữ liệu đơn giản đến phức tạp.

Có bốn lĩnh vực chính trong CyberChef:

1. Hộp nhập liệu ở trên cùng bên phải, nơi bạn có thể dán, nhập hoặc kéo văn bản hoặc tệp bạn muốn thao tác.
2. Hộp đầu ra ở phía dưới bên phải, nơi kết quả xử lý của bạn sẽ được hiển thị.
3. Danh sách thao tác ở phía bên trái, nơi bạn có thể tìm thấy tất cả các thao tác mà CyberChef có thể thực hiện trong danh sách được phân loại hoặc bằng cách tìm kiếm.
4. Khu vực công thức ở giữa, nơi bạn có thể kéo các thao tác bạn muốn sử dụng cũng như chỉ định các đối số và tùy chọn.



Elastic Fleet là một tính năng trong Elasticsearch, một hệ thống tìm kiếm và phân tích dữ liệu phân tán. Elastic Fleet giúp quản lý và điều khiển các đám mây Elasticsearch và các agent dữ liệu từ xa một cách dễ dàng và hiệu quả.

Với Elastic Fleet, bạn có thể triển khai, cấu hình và theo dõi các đám mây Elasticsearch từ một nơi duy nhất. Nó cung cấp các khả năng quản lý tập trung cho việc triển khai và quản lý quy mô lớn của các nút Elasticsearch trên các máy chủ từ xa hoặc trong môi trường đám mây.

Các tính năng và lợi ích chính của Elastic Fleet bao gồm:

Quản lý đám mây Elasticsearch: Elastic Fleet cho phép bạn triển khai và quản lý các đám mây Elasticsearch từ xa một cách dễ dàng thông qua giao diện điều khiển trực quan. Bạn có thể tạo, cấu hình và giám sát các cụm Elasticsearch từ xa mà không cần truy cập trực tiếp vào từng nút.

Quản lý agent dữ liệu: Elastic Fleet cho phép bạn quản lý các agent dữ liệu từ xa, bao gồm cài đặt, cấu hình và theo dõi các agent này. Các agent dữ liệu được sử dụng để thu thập và gửi dữ liệu vào Elasticsearch từ các nguồn khác nhau như máy chủ, máy tính cá nhân hoặc các hệ thống khác.

Tự động hóa và mở rộng linh hoạt: Elastic Fleet cung cấp khả năng tự động hóa cho việc triển khai và mở rộng các đám mây Elasticsearch và agent dữ liệu. Bạn có thể dễ dàng mở rộng hệ thống để đáp ứng yêu cầu tải và quy mô của môi trường dữ liệu của bạn.

Quản lý cấu hình: Elastic Fleet cho phép bạn quản lý cấu hình toàn diện cho các đám mây Elasticsearch và agent dữ liệu. Bạn có thể tạo và áp dụng các mẫu cấu hình, cung cấp các cài đặt chuẩn và tuỳ chỉnh cho từng đám mây Elasticsearch hoặc agent dữ liệu.

Tóm lại, Elastic Fleet là một tính năng quan trọng trong Elasticsearch giúp quản lý và điều khiển các đám mây Elasticsearch và agent dữ liệu từ xa một cách hiệu quả, đơn giản hóa việc triển khai và quản lý các hệ thống tìm kiếm và phân tích dữ liệu phức tạp.