Note splunk:

**What is Splunk Enterprise:**

- Là chương trình cho phép nghiên cứu, phân tích, giải lập các thiết bị sinh ra dữ liệu từ web, app, sensor, devices ..

- Sau khi chỉ định nguồn dữ liệu, splunk sẽ biểu thị luồng dữ liệu vè hiện thị ra các biểu đồ để từ đó có thể xem và nghiên cứu

**Các tính năng của splunk**

1. Indexing:

- Hiện thị các chỉ số về dữ liệu. Bao gồm các gói, các app custom, app server, web,db, network, sensor..

- Độ lớn của các chỉ số dựa trên key Spluck Enterprise

2. Data model

- là bản đồ ngữ nghĩa về cấu trúc phân cấp dựa trên 1 hoặc nhiều tập dữ liệu

- nó encode miền dữ liệu thành dạng, cần thiết cho việc tìm kiếm đặc biệt của các tập dữ liệu

- Có 1 số loại công cụ tìm kiếm đặc biết bởi splunk Enterprise được sinh ra các reports cho Pivot users. Data model đại diện cho các tập datasets trong tập dự liệu lớn của Splunk Enterprise

2. Pivot

- Đại diện cho table, chart, hoặc các data tượng trưng được tạo ra cho việc sử dụng Pivot Editor.

- Pivot Editor cho phép user map các attr được định nghĩa bởi đối tượng data model tới các table hoặc chart tương trưng mà không cần phải viết ra researches để sinh ra các biểu đồ

- Pivots có thể saves như các report và đưa tới trang chủ

3. Search

- là phương thức tiểu biểu mà user có thế lọc dữ liệu từ splunk

- Có thế viết các câu search để lấy events từ index, sử dụng các cấu lệnh thống kế để tính toán các metric và sinh ra các reports, tím kiếm các điều kiện của thể trên 1 cửa sổ, xác định các, xác định các mẫu trong tương lai, dự báo xu hướng tương lai …

- Các searches có thế saved dưới dạng các report và sử dụng cho nhưng biểu đồ

4. Alerts.

- báo đống được kích hoạt khi 1 điểu kiện nào đó được thỏa mãn kết quả search trong cả quá khứ lấn tương lai

- alearts có thế được cấu hình để thực hiện 1 số công việc như aleart tới 1 email được định trước, gửi 1 alearts tới RSS feed, chạy 1 số custom script như gửi 1 aleart event tới syslog

5. Reports

- Được lưu từ các searches và pivot

- có thể chạy reports từ các ad hoc basic

- lập trình các report để sinh ra aleart khi kết quả trùng với các điều kiện

- có thể add reports tới trang chủ như các biểu đồ

6. Dashboards

- tạo ra các panels chứa các modules như search boxes, fields, charts, tables, form ..

- thường được sử dụng để lưu các searches or pivots.

- có thể hiện thị kết quả của 1 searches cũng như các data từ real-time searches chạy trong background

Next: <https://docs.splunk.com/Documentation/Splunk/6.6.2/Overview/AboutSplunkEnterpriseusers>