**VIETNAM CYBERSPACE SECURITY TECHNOLOGY**

**JSC**

**🙜🙞🕮🙜🙞**



**BÁO CÁO**

**CÀI ĐẶT THU THẬP LOG**

**TỪ MÁY WINDOWS 7**

**TRÊN VMWARE WORKSTATION**

Người thực hiện: Mai Thành Thắng

Hà Nội, 9/2019

Mục Lục

[I. Thông tin chung 3](#_Toc19518249)

[1. Giới thiệu 3](#_Toc19518250)

[2. Source type và Data mode sử dụng 3](#_Toc19518251)

[3. Các bước thực hiện cấu hình, cài đặt 3](#_Toc19518252)

[II. Cài đặt cấu hình Splunk và Add-on 4](#_Toc19518253)

[1. Cài đặt Splunk Server 4](#_Toc19518254)

[2. Cài đặt Window 7 và Splunk Forwarder trên VMware Workstation. 5](#_Toc19518255)

[3. Cài đặt Add-on and app Data Model trên giao diện Splunk Server 8](#_Toc19518256)

[III. Cấu hình nhận log trên Splunk Server 11](#_Toc19518257)

[1. Mở cổng kết nối nhận dữ liệu 11](#_Toc19518258)

[2. Cấu hình nhận dữ liệu: 12](#_Toc19518259)

[IV. Seaching event trên Splunk sau Data mode 15](#_Toc19518260)

[V. Phân tích log trong search and report 17](#_Toc19518261)

# I. Thông tin chung

## 1. Giới thiệu

* Mô tả việc thu thập log trên hệ điều hành Win 7 cài đặt trên VMware WorkStation 15 .
* Phiên bản win 7 Ultimate và Splunk 7.3+
* Loại log thu thập: Winevent log: App, Security, Setup, System.

## 2. Source type và Data mode sử dụng

|  |  |  |
| --- | --- | --- |
| Sourcetype | Data model | **Ghi chú** |
| WindowEventlog | web | Sử dụng Data model Web có sẵn trong Window Event Logs Analysis |

## 3. Các bước thực hiện cấu hình, cài đặt

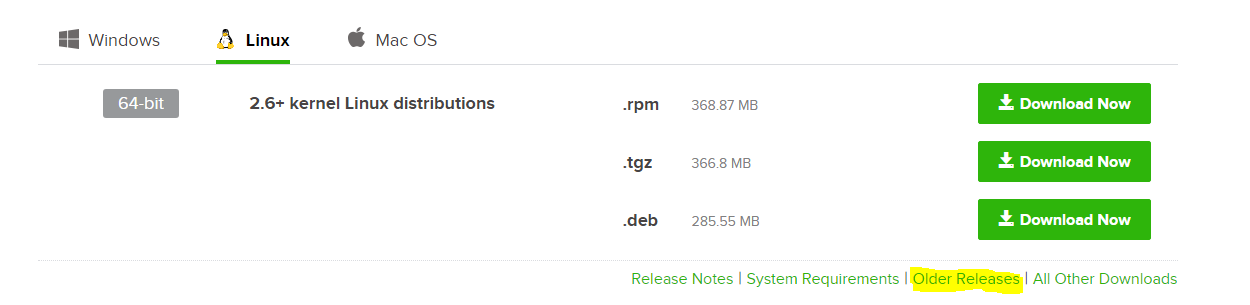
|  |  |  |
| --- | --- | --- |
| Bước thực hiện | Nội dung | Nơi cài đặt/cấu hình  (Agent, Server, SearchHead) |
| 1 | Cài đặt Splunk Server | Server |
| 2 | Cài đặt Win 7 trên VM | Agent |
| 3 | Cài đặt Splunk forwarder | Agent |
| 4 | Cài đặt add-on và app Data Model | Server |
| 5 | Cài đặt data input | Server |
| 6 | Searching dữ liệu indexed trên Splunk | SearchHead |
| 7 | Chuẩn hóa dữ liệu theo data model | SearchHead |
| 8 | Searching dữ liệu sau data model | SearchHead |

# II. Cài đặt cấu hình Splunk và Add-on

## Cài đặt Splunk Server

Để cài đặt Splunk Universal, thực hiện các bước sau:

* Kiểm tra cấu hình máy hiện tại
* Cài đặt một máy Ubuntu server. Link hướng dẫn: [Github](https://github.com/Thang1102/OnBoard/blob/master/install-ubuntu-server%20on%20VM-%C4%91%C3%A3%20chuy%E1%BB%83n%20%C4%91%E1%BB%95i.pdf)
* Dowload phiên bản Splunk Universal bạn muốn cài vào trong máy ảo Ubuntu server: ( lưu ý phần màu vàng là bạn có thể tải phiên bản khác cho hệ điều hành mà bạn muốn cài)



Hình II.1.1

* Khi bạn bấm vào **Download Now** Bạn có thể dùng tool **wget** để tải trực tiếp cho nhanh.



Hình II.1.2

* Sau khi tải về bạn copy tiến hành cài đặt theo hướng dẫn sau :

+ Ở đây mình tải file .tgz về máy Ubuntu

+ Dùng lệnh tar xvzf splunk\_package\_name.tgz -C /opt

+ sudo su và nhập pass của user root

+ Cd /opt/splunk/bin

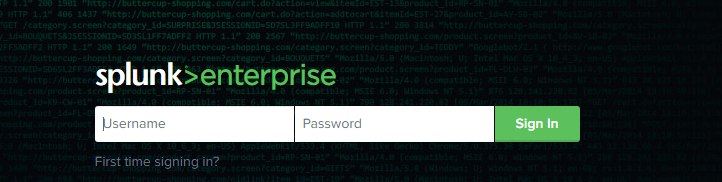
+ ./splunk –-accept-license

+ ./splunk enable boot-start

+ Lưu ý nhập username và pass của admin

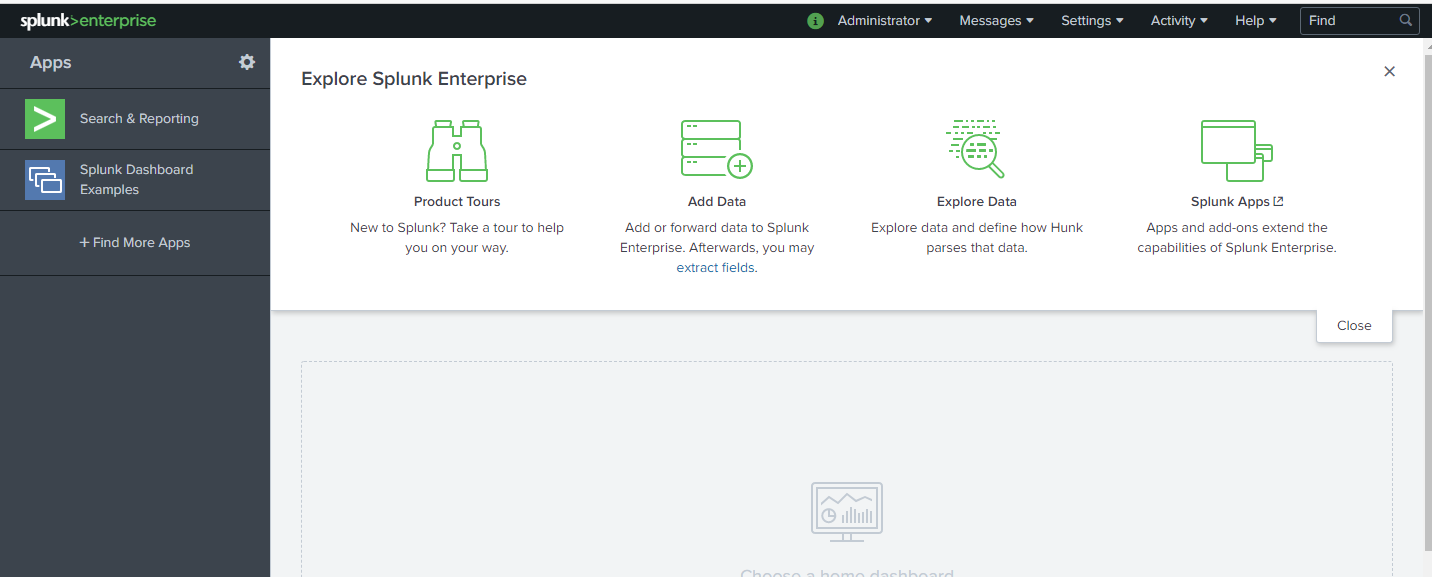
+ ./splunk restart

* Sau đó bạn vào web browser của bạn. Bạn nhâp: ip\_ubuntu\_server:8000



Hình II.1.3

* Nhập username và password admin bạn sẽ vào được giao diện sau

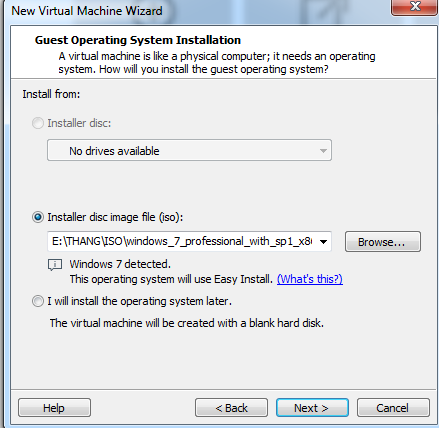


Hình II.1.4

Mục App là mình cài thêm app splunk Dashboard Examples nó mới có nếu không thì nó chưa có.

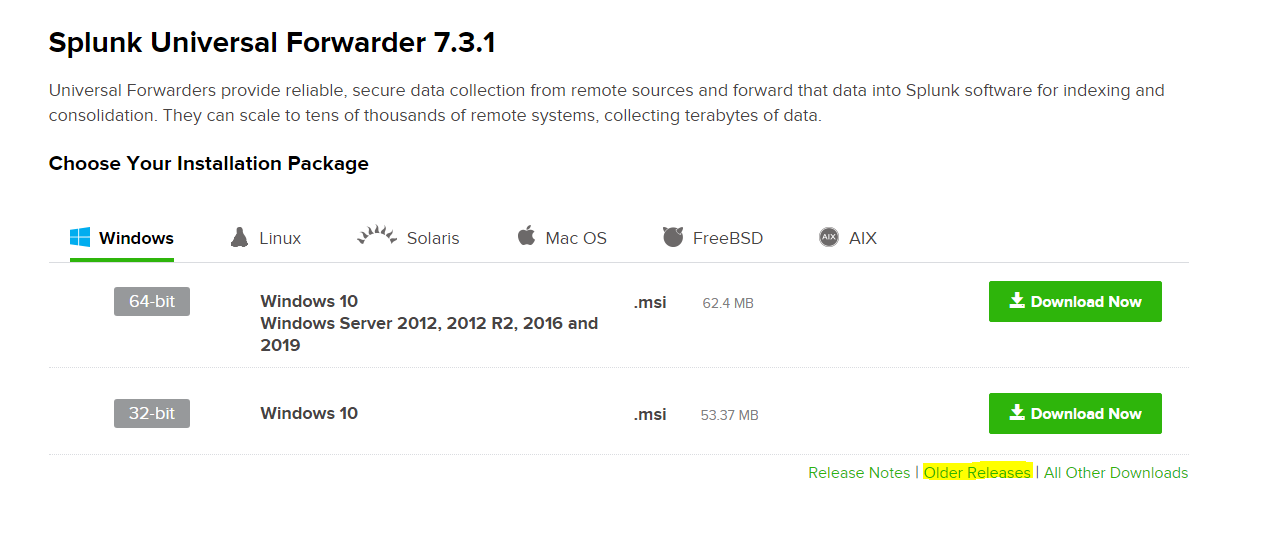
## Cài đặt Window 7 và Splunk Forwarder trên VMware Workstation.

* Cài đặt win 7 trên VM bạn chỉ khác với bước tạo Ubuntu server ở chọn đĩa



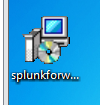
Hình II.2.1

* Sau đó bạn chạy cài nó lên như cài win 7 bình thường
* Bạn vào link download splunk forwarder chọn phiên bản phù hợp với hệ điều hành win 7 bạn cài trên VM



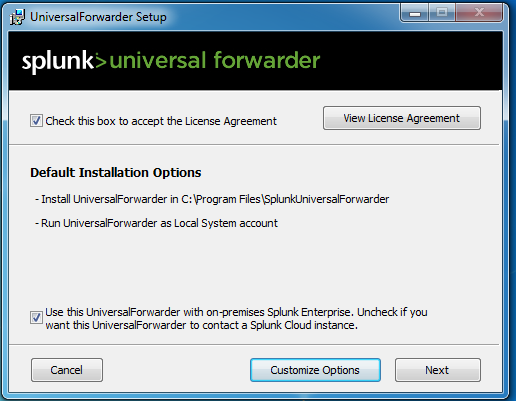
Hình II.2.2

* Lưu ý phần màu vàng bạn có thể chọn cho phần mềm cho loại window khác.
* Các bước cài đặt
* Phần mềm tải về mình copy ra desktop



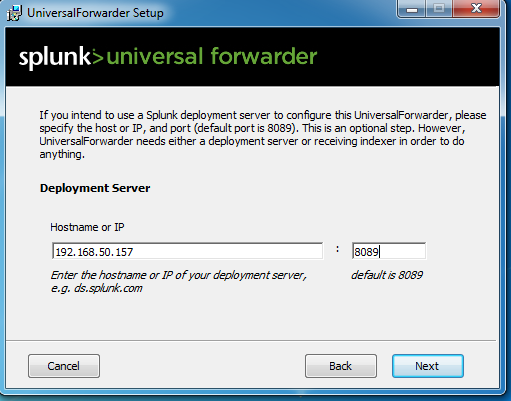
Hình II.2.3

* Chạy nó tích như hình và chọn **Next**



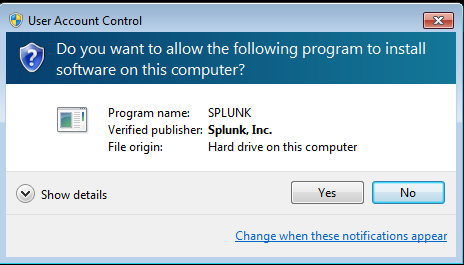
Hình II.2.4

* Tiếp theo cấu hình cổng manger port mặc định là 8098 và ip splunk server để thực hiện quá trình quét tìm kiếm các máy agent theo dõi bởi splunk( **Nên tắt firewall trên window để đảm bảo cài đặt khi bạn chưa biết câu hình mở port)**



Hình II.2.5

* Tiếp theo bạn tương tự như vậy bạn đổi cổng cài đặt là 9997 để gửi log lên server splunk -> **Install**
* Ra bảng như này bạn bấm **Yes**



Hình II.2.6

* Kiểm tra xem splunk forwarder đã chạy chưa bạn vào  gõ **service.msc**



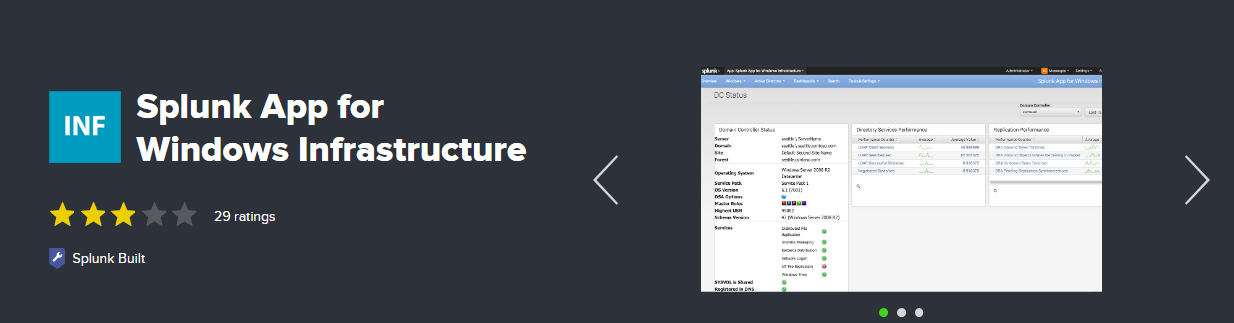
Hình II.2.7

## Cài đặt Add-on and app Data Model trên giao diện Splunk Server

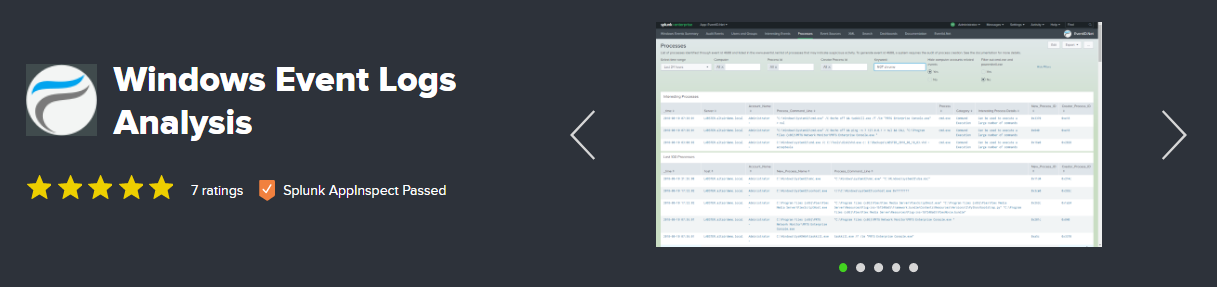
* Đầu tiên vào link : <https://splunkbase.splunk.com/>
* Chọn app tìm kiếm trên thanh tìm kiếm  
  

Hình II.3.1

* Nhập từ khóa: windows infrastructure và WMI
* Kết quả:



Hình II.3.2

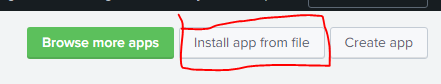


Hình II.3.3

* Tải về máy tiến hành cài 2 app này.
* Ở trang **HOME** và các trang tiếp chọn như hình:

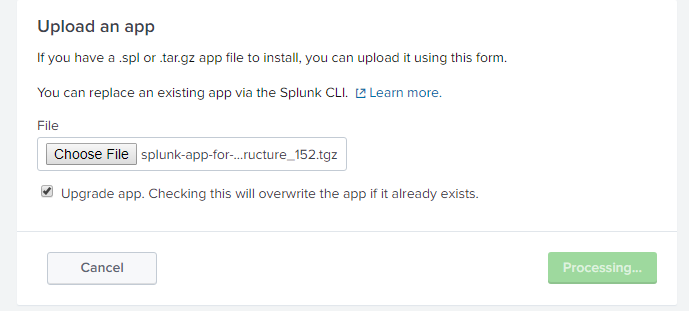


Hình II.3.4



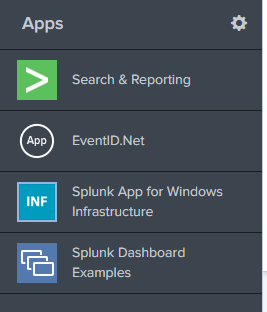
Hình II.3.5

* Sau đó lựa chọn app để cài. Đầu tiên là app: **windows infrastructure**
* Chọn splunk-app-for-windows-infrastructure\_152.tgz( ứng dụng cho cơ sở hạ tầng window)
* Sau khi cài xong nhớ khởi động lại**.**



Hình II.3.5

* Tương tự với app windows-event-logs-analysis làm tưng tự như vậy ta thu được kết quả ở trang **Home** như sau:



Hình II.3.6

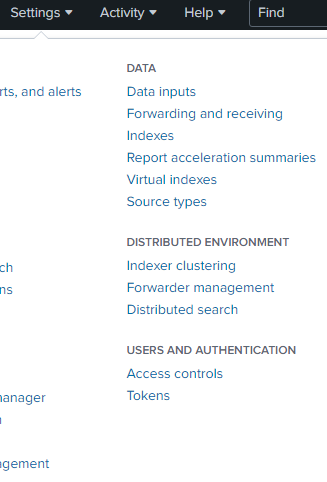
**NOTE: -** Ứng dụng splunk-app-for-windows-infrastructure cung cấp các ví dụ về đầu vào dữ liệu dựng sẵn, tìm kiếm, báo cáo và bảng điều khiển cho máy chủ Windows và quản lý máy tính để bàn. Bạn có thể theo dõi, quản lý và khắc phục sự cố hệ điều hành Windows, bao gồm các thành phần Active Directory, tất cả từ một nơi.

**-** The Windows Event Log Analysis app cung cấp giao diện trực quan cho nhật ký sự kiện Windows được thu thập bởi Splunk Universal Forwarder cho Windows (từ máy tính cục bộ hoặc được thu thập thông qua Chuyển tiếp Nhật ký Sự kiện Windows). Thông tin khắc phục sự cố có sẵn tại **www.eventid.net** chỉ bằng một cú nhấp chuột. Các số liệu thống kê khác nhau cho nhật ký sự kiện Windows được biên soạn và trình bày theo cách trực quan.

# III. Cấu hình nhận log trên Splunk Server

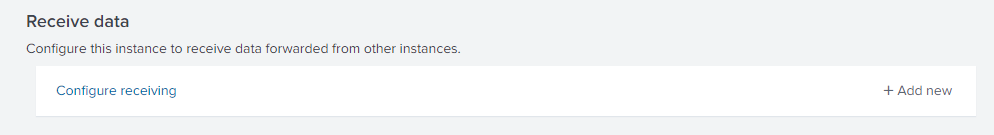
1. Mở cổng kết nối nhận dữ liệu**:**

* Mở cổng nhận dữ liệu từ forwarder. Vào Setting -> Forwarding and receving



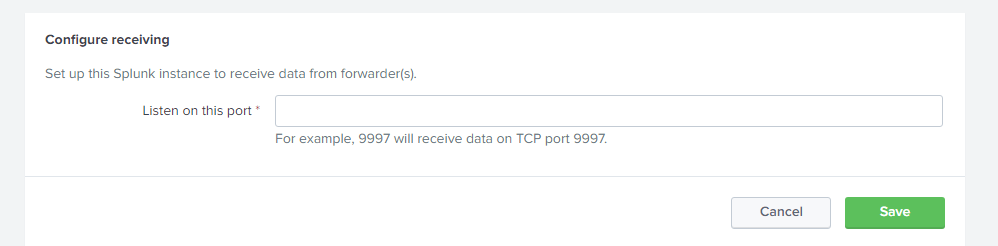
Hình III.1.1

* Chọn Recive Data -> Add new



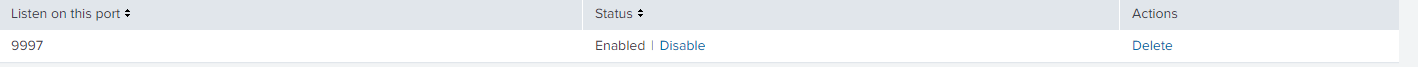
Hình III.1.2.

* Nhập cổng 9997 để nhận dữ liệu và bấm Save



Hình III.1.3

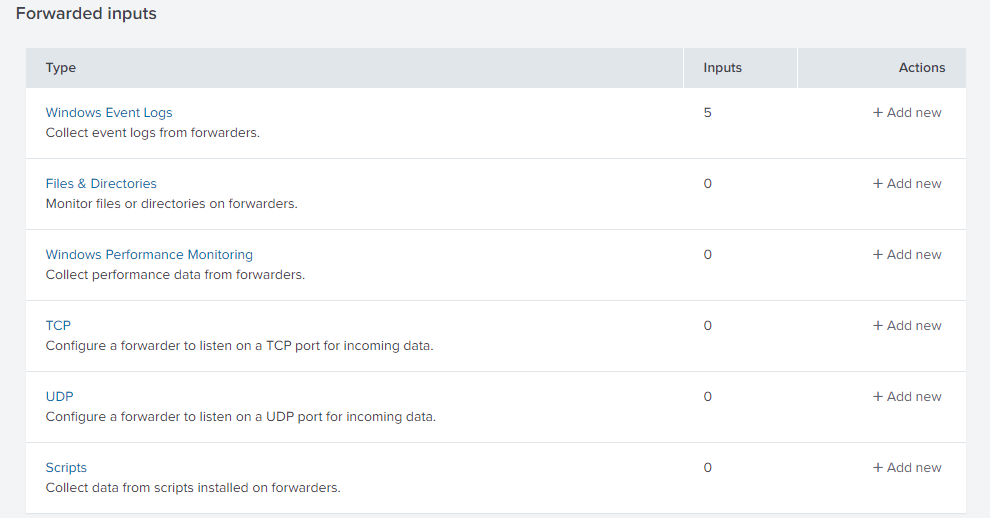
* Kết quả:



Hình III.1.4

## Cấu hình nhận dữ liệu:

* Setting -> data input
* Bạn xuống mục Forwarded Input chọn Windows Event Logs



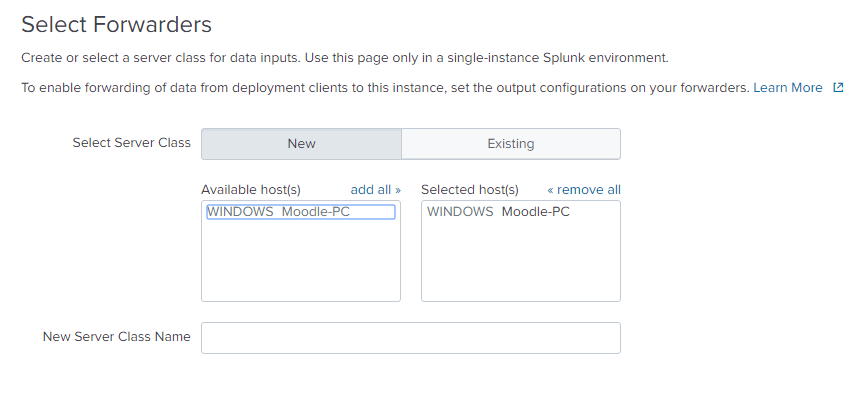
Hình III.2.1

* Tiếp theo bạn chọn như hình:



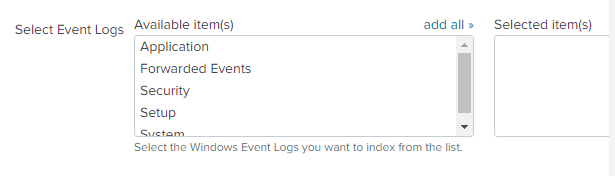
Hình III.2.2

* Bạn thấy như vậy. Bạn thấy tên máy window bạn lấy log



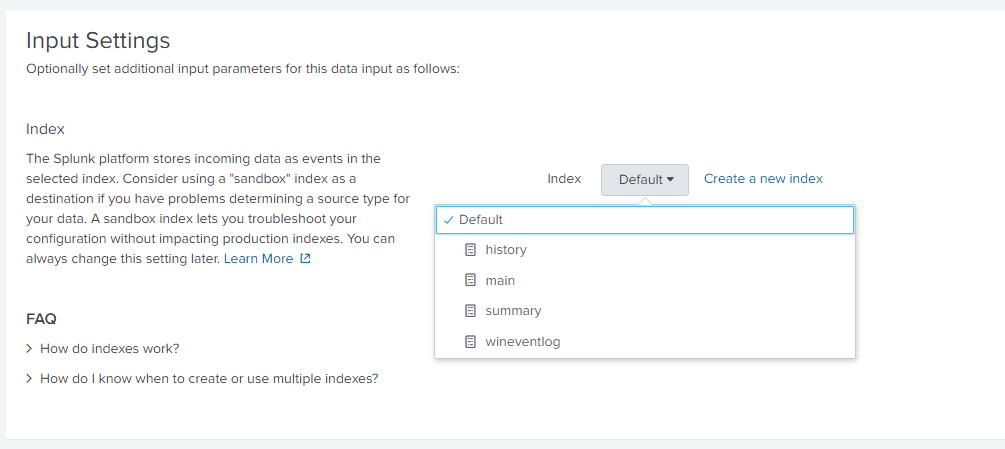
Hình III.2.3

* Bạn chọn máy đó và đặt class name cho nó.
* Bạn lựa chọn loại log cần lấy(ở đây mình lấy tất cả)



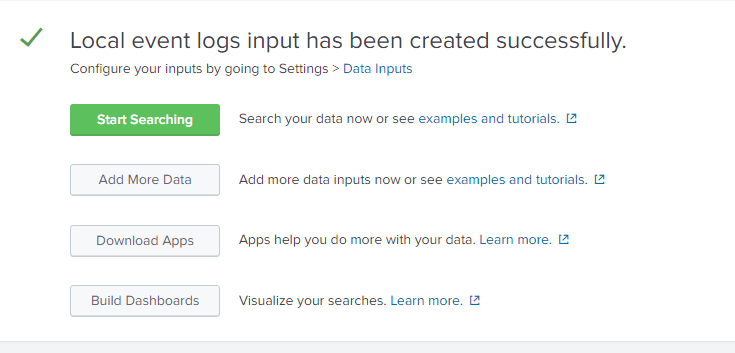
Hình III.2.4

* Trang tiếp Input setting mình chọn **windoweventlog**



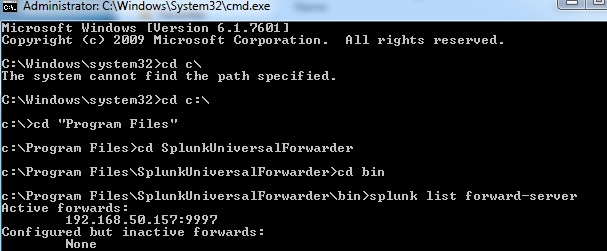
Hình III.2.5

* Bấm **review** kiểm tra gì mình đã làm nếu thấy ok và bấm **submit**
* Test thử search bấm **Start Searching**

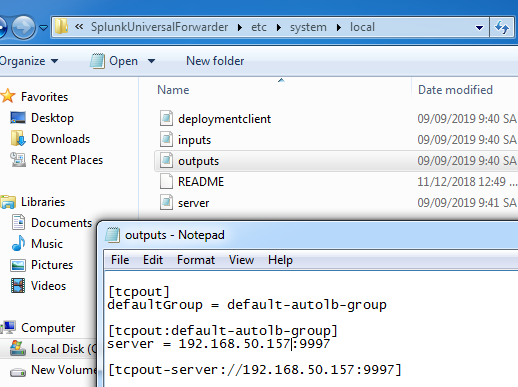


Hình III.2.6

**NOTE:**  Trường hợp xảy ra sự cố bạn cần kiểm tra cổng vào ra dữ liệu:



Hình III.2.7



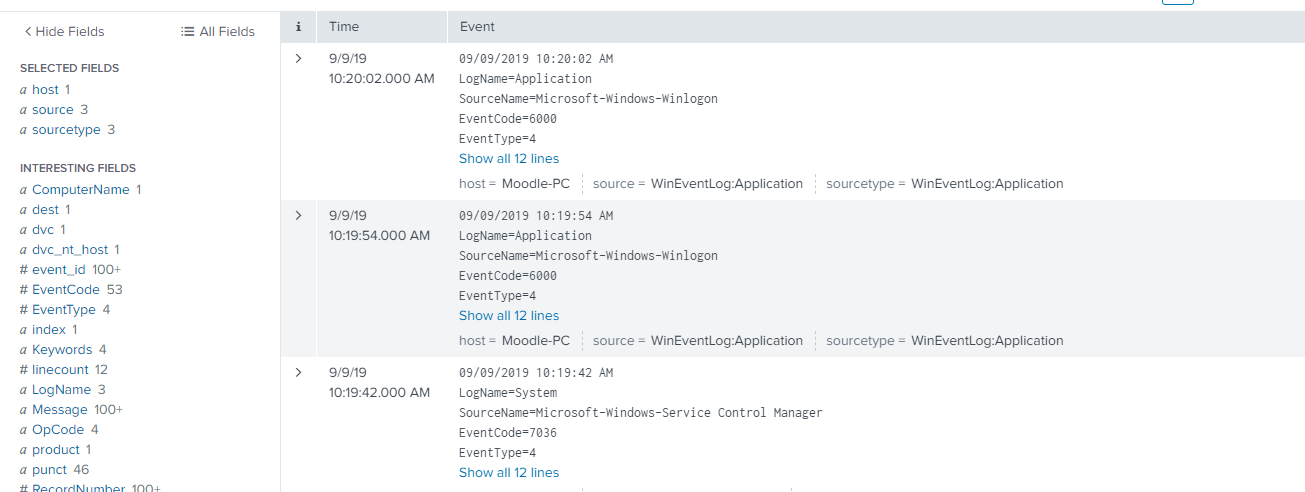
Hình III.2.8

* Lưu ý khi cài đặt nếu bạn để Input setting mục Index là default tất cả event sẽ được chuyển về index=main khi thực hiện tìm kiếm.

# IV. Seaching event trên Splunk sau Data mode

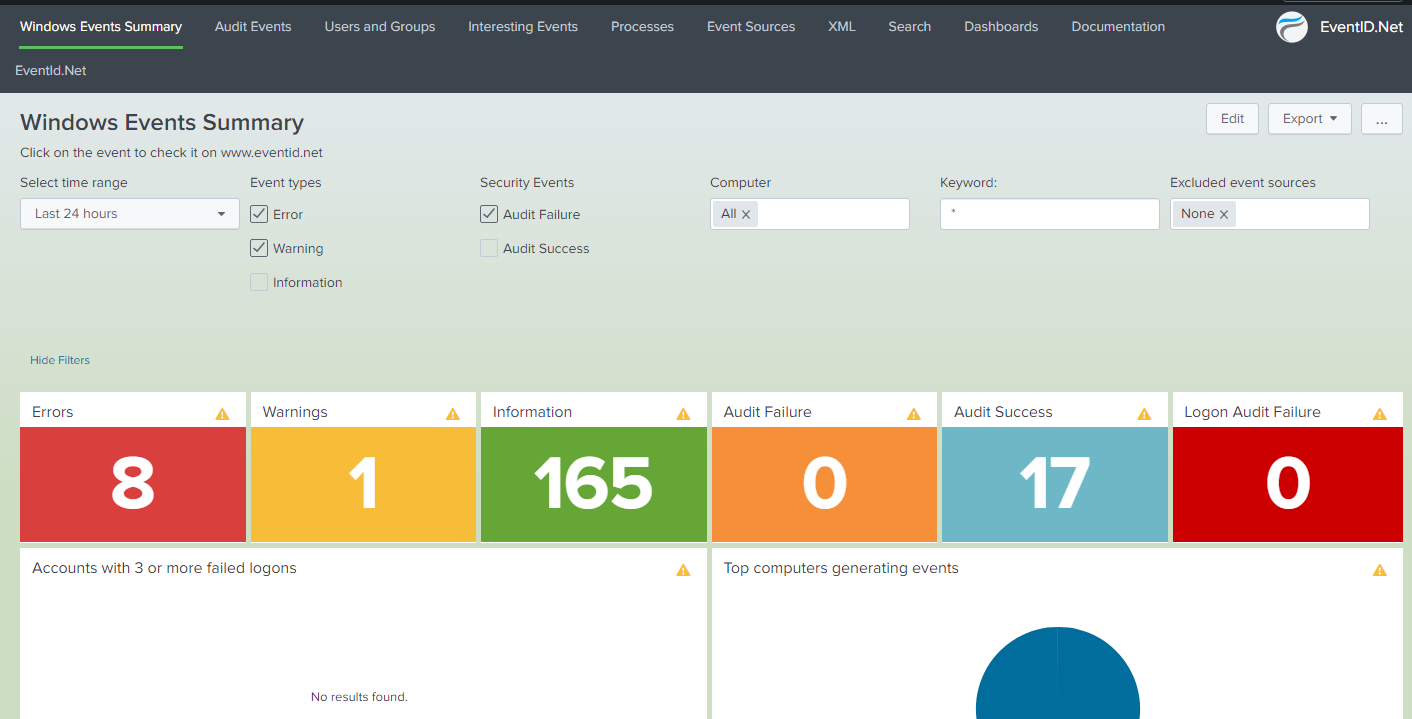
* Vào web brower truy cập <http://Splunk_server_ip:8000>
* Kiểm tra xem log đã được đẩy lên splunk chưa.

Search index = “winenventlog”



Hình IV.1

* Sau khi cấu hình và nhận event log thành công ta tiến hành phân tích sự kiện xảy ra trong hệ thống có thể sử dụng 2 app trên để thống kê báo cáo tình trạng của hệ thống mọi thời điểm một cách dễ nhất và nhanh gọn.
* Lưu ý app: **windows infrastructure** chuyêndùng cho WindowServer, còn **windows-event-logs-analysis(EventID.Net)** dùng chủ yếu cho việc phân tích sự kiện xảy ra trên máy trạm. Máy cá nhân.
* **Các dùng windows-event-logs-analysis phân tích log**
  + Giao diện của EventID.Net



Hình IV.1

**Phân tích task menu:**

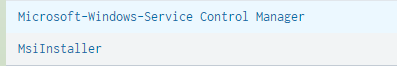
**- Windows events summary**: tổng hợp thông tin sự kiện xảy tra trong thời điểm nào đó của hệ thống hiển thị lên một dashboard.

**-** **Audit Event:** Kiểm toán, thống kê sự kiện liên quan đến account quá trình login, logout trên hệ thống

**- User and Group:** Hiện thị thông tin sự kiện về user và group hệ thông

**- Intereting Event:** Hiện thị sự kiện nổi bật của hệ thống

**- Process:** Thống kê tiến trình sự kiện khi thực hiện command trên giao diện dòng lệnh. Xác định sự kiện này thông qua id 4688

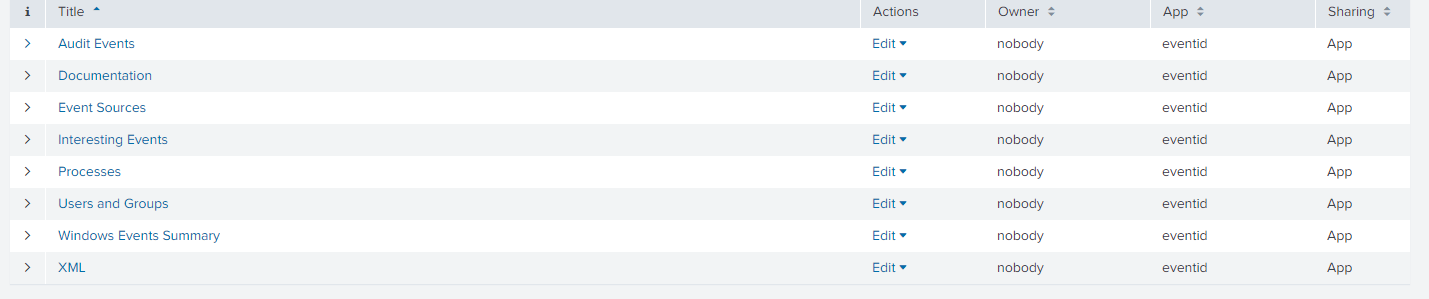
**- Event sources:** Sự kiện liên quan đến sources: 

Hình IV.2

**- XML:** Mục đích chính của **XML là** đơn giản hóa việc chia sẻ dữ liệu giữa các platform. Ở đây là đơn giản hóa việc nhận window eventlog lên splunk.

**- Search:**  Sự dụng tìm kiến hiển thị sự kiện cách thủ công có chức năng giống app **search & reporting**

**- Doashboards:**  Hiện thị danh sách các bảng điều kiển tự tạo sẵn ra khi cài app và thêm những cái của riêng bạn.

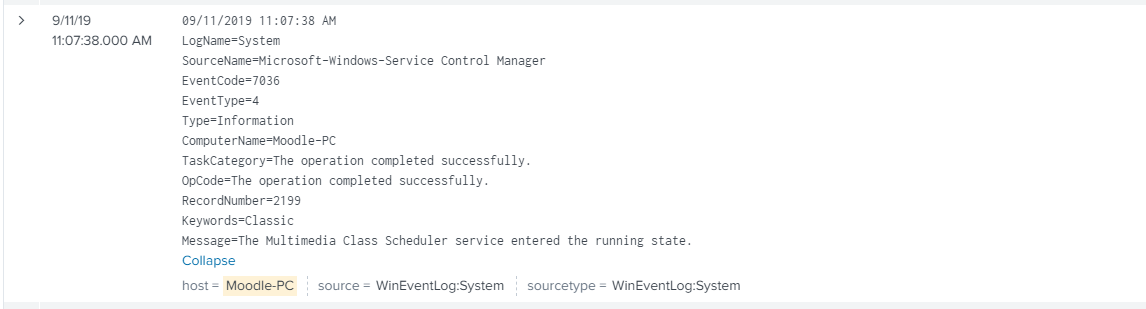


Hình IV.3

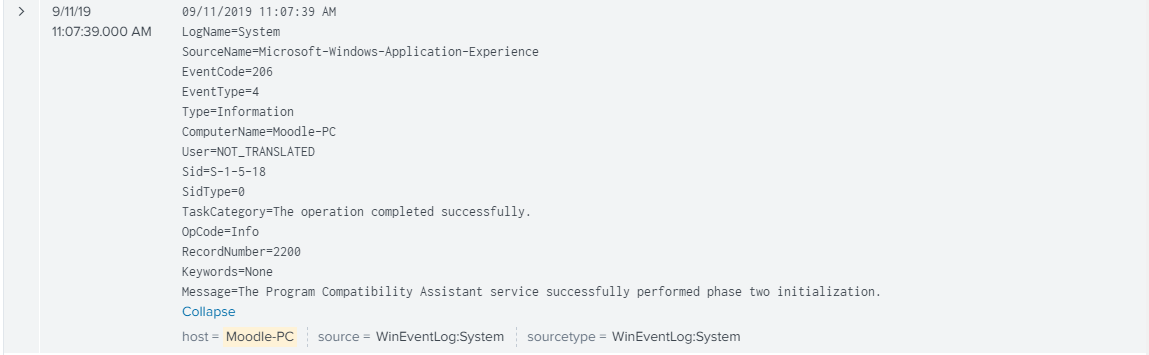
**- Document:**  Là thông tin tài liệu hướng dẫn sử dụng app và một số thông tin về app

# V. Phân tích log trong search and report

* Đây là trình cài đặt một app trên window từ bắt đầu cho đến hoàn thành hiện thị thông báo ra sao



Hình V.1



Hình V.2