

**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
1. Giới thiệu .....	3
2. Source type và Data mode sử dụng.....	3
3. Các bước thực hiện cấu hình, cài đặt .....	3
II. Cài đặt cấu hình Splunk và Add-on .....	4
1. Cài đặt Splunk Server .....	4
2. Cài đặt Window 7 và Splunk Forwarder trên VMware Workstation. ....	5
3. Cài đặt Add-on and app Data Model trên giao diện Splunk Server.....	8
III. Cấu hình nhận log trên Splunk Server .....	11
1. Mở cổng kết nối nhận dữ liệu .....	11
2. Cấu hình nhận dữ liệu: .....	12
IV. Seaching event trên Splunk sau Data mode.....	15
V. Phân tích log trong search and report.....	17

## 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

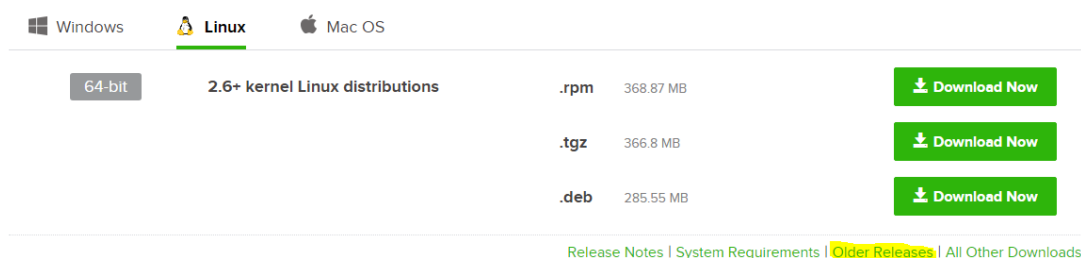
Bước thực hiện	Nội dung	Nơi cài đặt/cấu hình (Agent, Server, SearchHead)
1	Cài đặt Splunk Server	Server
2	Cài đặt Win 7 trên VM	Agent
3	Cài đặt Splunk forwarder	Agent
4	Cài đặt add-on và app Data Model	Server
5	Cài đặt data input	Server
6	Searching dữ liệu indexed trên Splunk	SearchHead
7	Chuẩn hóa dữ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

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

### 1. Cài đặt Splunk Server

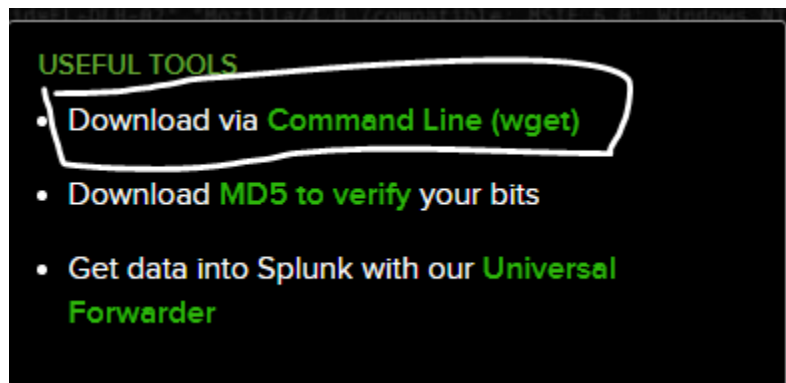
Để cài đặt Splunk Universal, thực hiện các bước sau:

- Kiểm tra cấu hình máy hiện tại
- Cài đặt một máy Ubuntu server. Link hướng dẫn: [Github](#)
- Download 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 xvfz 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
```

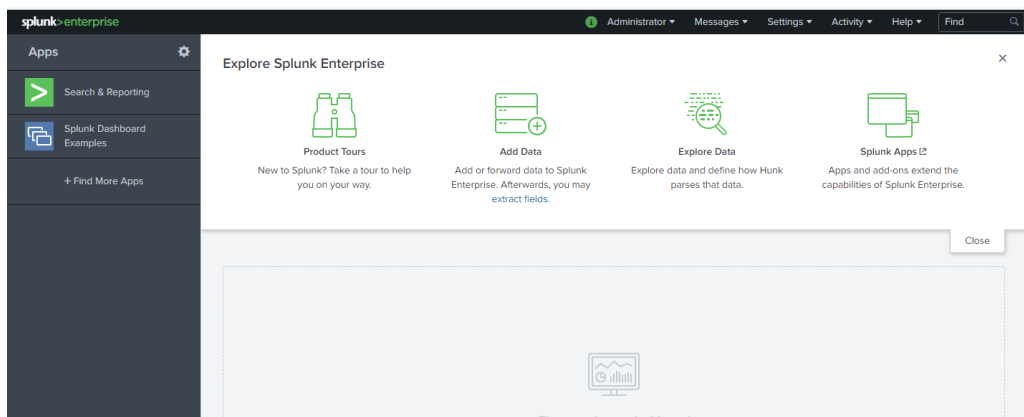
```
+ ./splunk restart
```

- Sau đó bạn vào web browser của bạn. Bạn nhập: ip\_ubuntu\_server:8000



Hình II.1.3

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

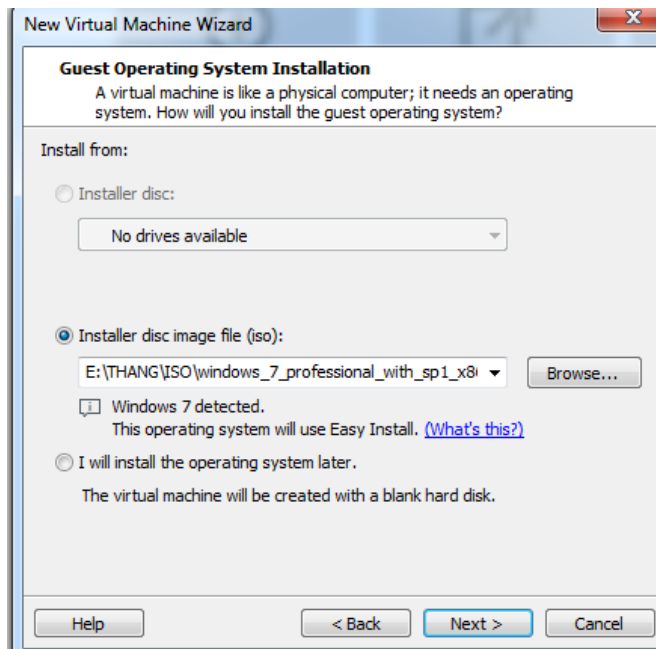


Hình II.1.4

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

## 2. 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

## Splunk Universal Forwarder 7.3.1

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

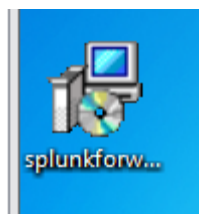
### Choose Your Installation Package

Windows	Linux	Solaris	Mac OS	FreeBSD	AIX
<p>64-bit</p> <p>Windows 10 Windows Server 2012, 2012 R2, 2016 and 2019</p> <p>.msi 62.4 MB</p> <p><a href="#">Download Now</a></p>					
<p>32-bit</p> <p>Windows 10</p> <p>.msi 53.37 MB</p> <p><a href="#">Download Now</a></p>					

[Release Notes](#) | [Older Releases](#) | [All Other Downloads](#)

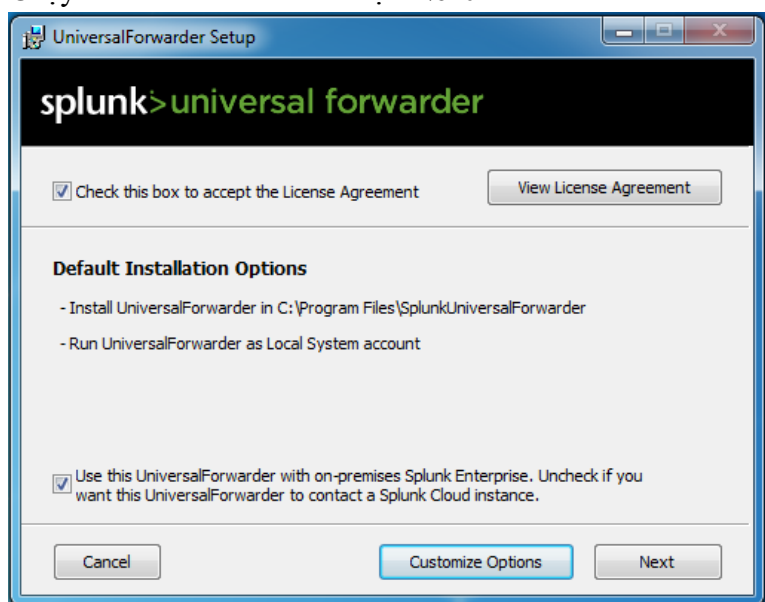
Hình II.2.2

- 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



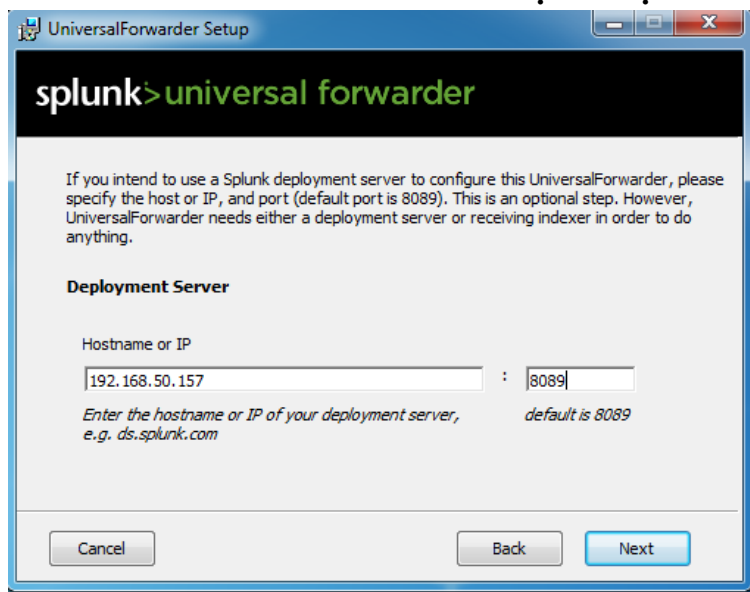
Hình II.2.3

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



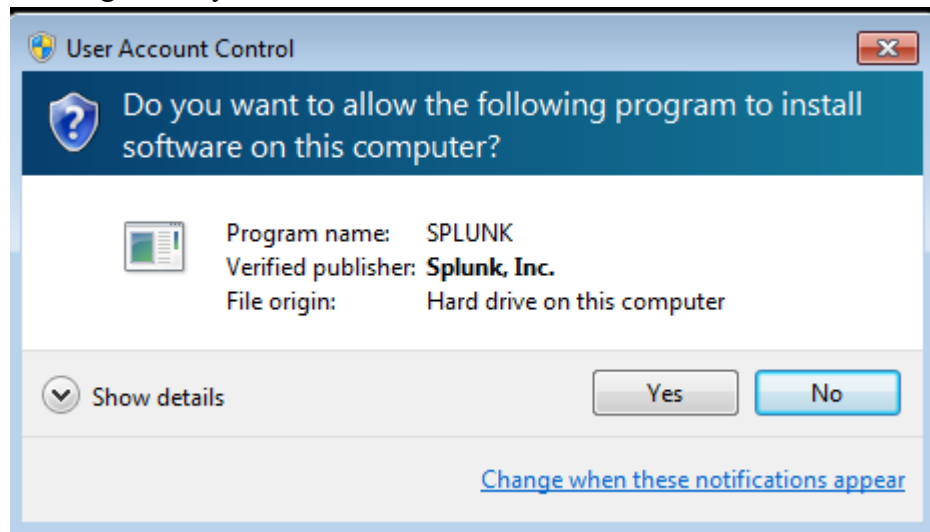
Hình II.2.4

- Tiếp theo cấu hình cổng manager 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 cấu hình mở port**)




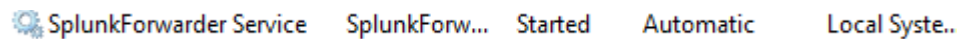
Hình II.2.5

- 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

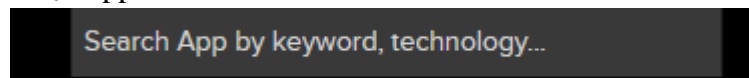
- Kiểm tra xem splunk forwarder đã chạy chưa bạn vào  gõ **service.msc**



Hình II.2.7

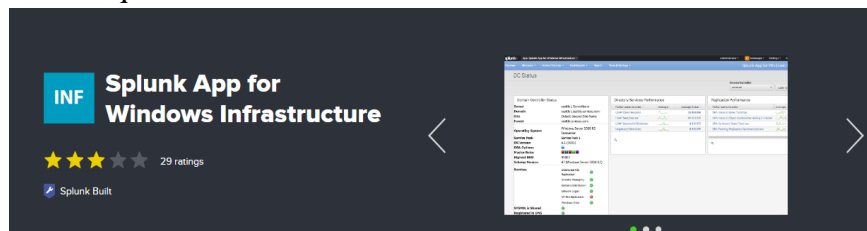
### 3. Cài đặt Add-on and app Data Model trên giao diện Splunk Server

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



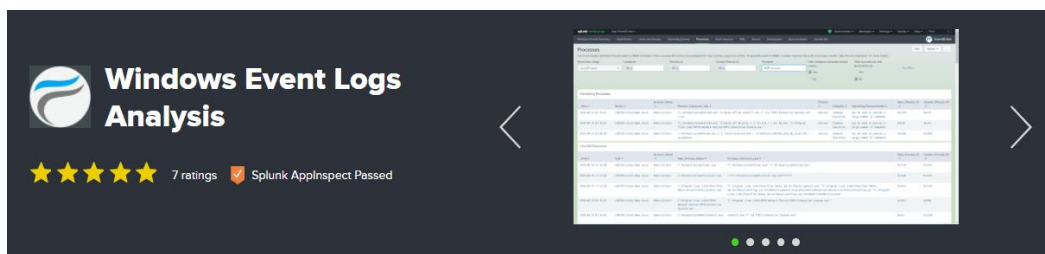
Hình II.3.1

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



Hình II.3.2



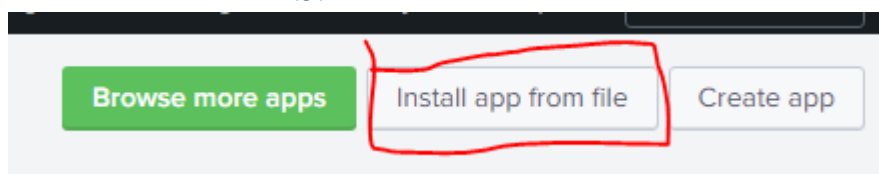


Hình II.3.3

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

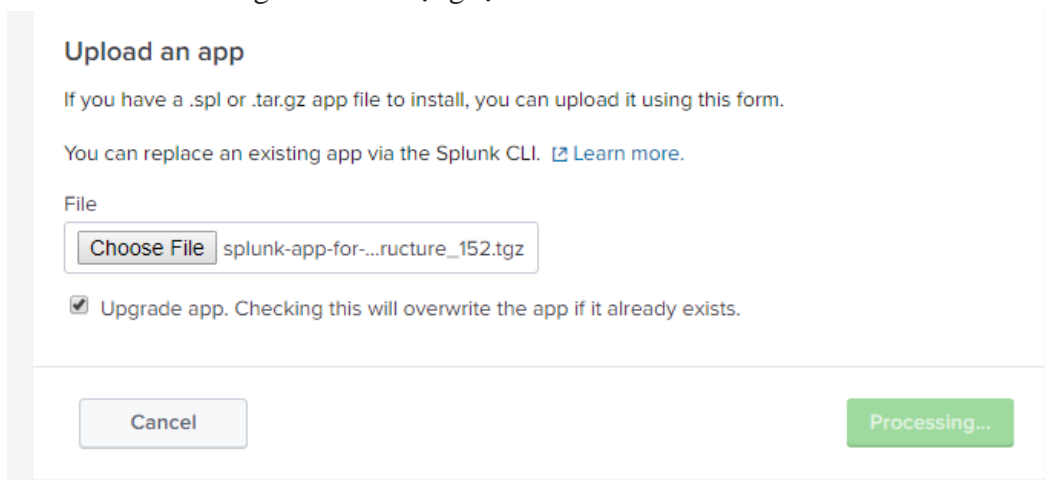


Hình II.3.4



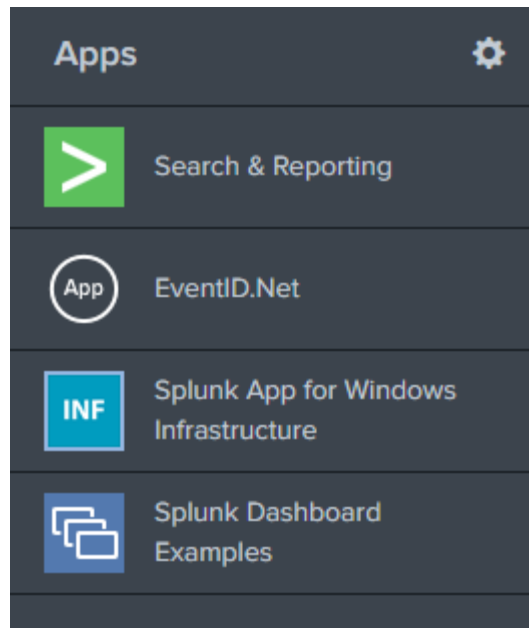
Hình II.3.5

- 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 tương tự như vậy ta thu được kết quả ở trang **Home** như sau:



Hình II.3.6

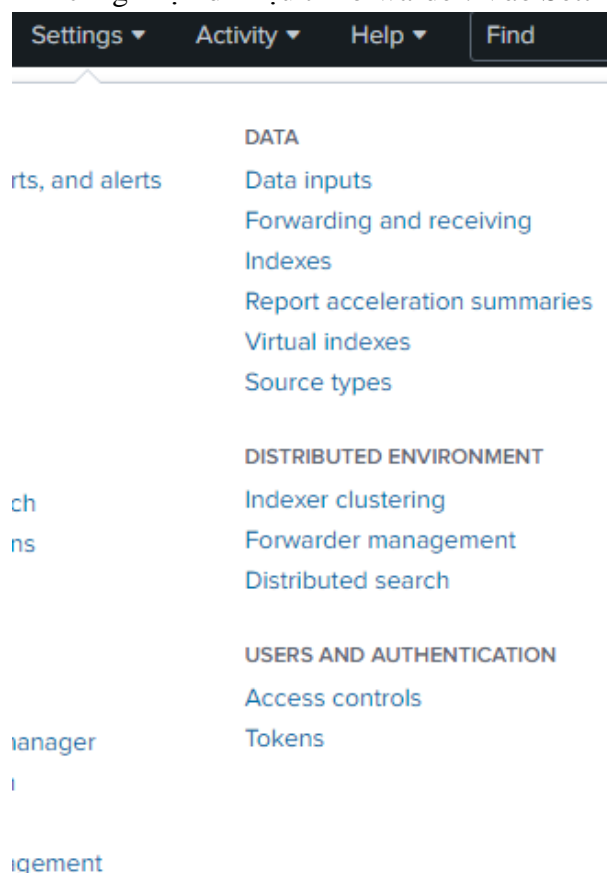
**NOTE: -** Ứng dụng splunk-app-for-windows-infrastructure cung cấp các ví dụ về đầu vào dữ liệu dựng sẵn, tìm kiếm, báo cáo và bảng điều khiển cho máy chủ Windows và quản lý máy tính để bàn. Bạn có thể theo dõi, quản lý và khắc phục sự cố hệ điều hành Windows, bao gồm các thành phần Active Directory,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

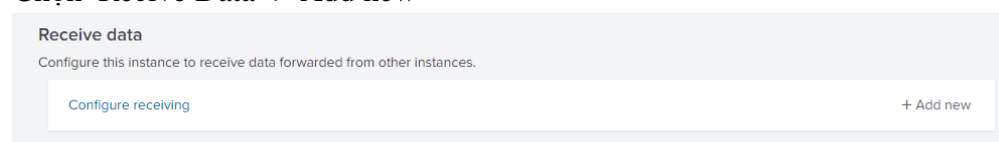
#### 1. Mở cổng kết nối nhận dữ liệu:

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



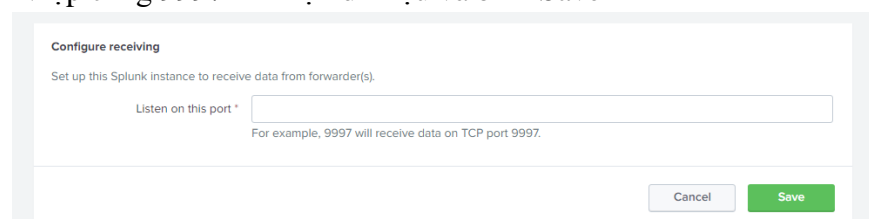
Hình III.1.1

- 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:

Listen on this port ▾	Status ▾	Actions
9997	Enabled   Disable	Delete

Hình III.1.4

## 2. Cấu hình nhận dữ liệu:

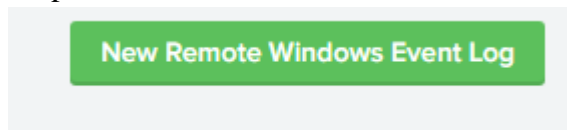
- Setting -> data input
- Bạn xuống mục Forwarded Input chọn Windows Event Logs

Forwarded inputs

Type	Inputs	Actions
<b>Windows Event Logs</b> Collect event logs from forwarders.	5	+ Add new
<b>Files &amp; Directories</b> Monitor files or directories on forwarders.	0	+ Add new
<b>Windows Performance Monitoring</b> Collect performance data from forwarders.	0	+ Add new
<b>TCP</b> Configure a forwarder to listen on a TCP port for incoming data.	0	+ Add new
<b>UDP</b> Configure a forwarder to listen on a UDP port for incoming data.	0	+ Add new
<b>Scripts</b> Collect data from scripts installed on forwarders.	0	+ Add new

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

Select Forwarders

Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.

To enable forwarding of data from deployment clients to this instance, set the output configurations on your forwarders. [Learn More](#)

Select Server Class

New

Existing

Available host(s)

add all >

WINDOWS Moodle-PC

Selected host(s)

< remove all

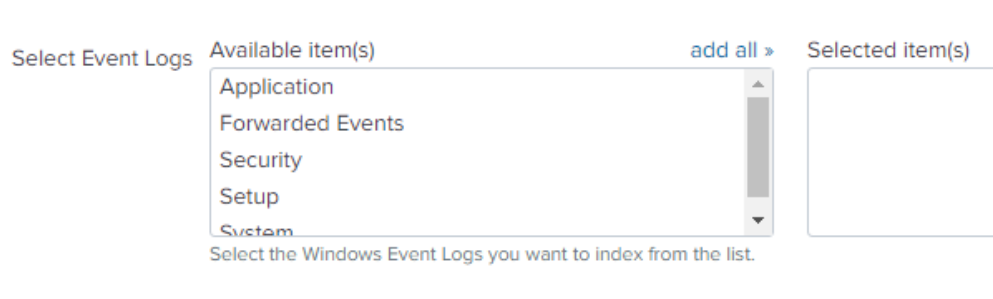
WINDOWS Moodle-PC

New Server Class Name

Hình III.2.3

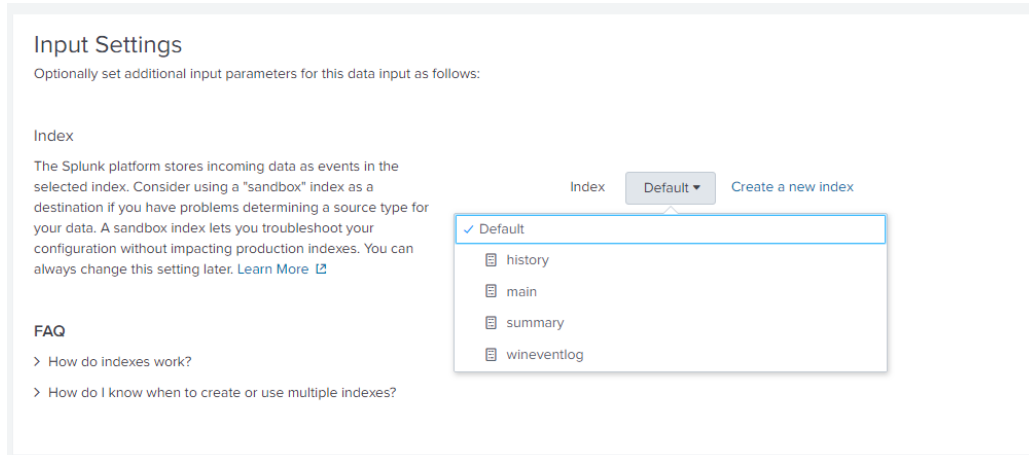
- Bạn chọn máy đó và đặt class name cho nó.

- Bạn lựa chọn loại log cần lấy (ở đây mình lấy tất cả)



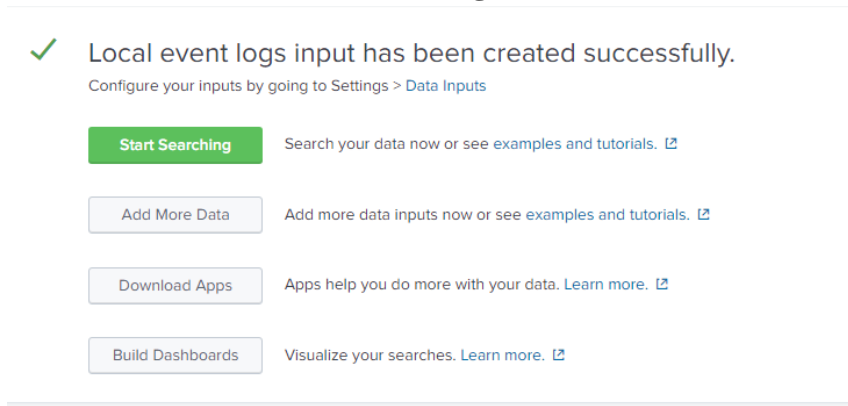
Hình III.2.4

- Trang tiếp Input setting mình chọn **wineventlog**



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:

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd c\
The system cannot find the path specified.

C:\Windows\system32>cd c:\

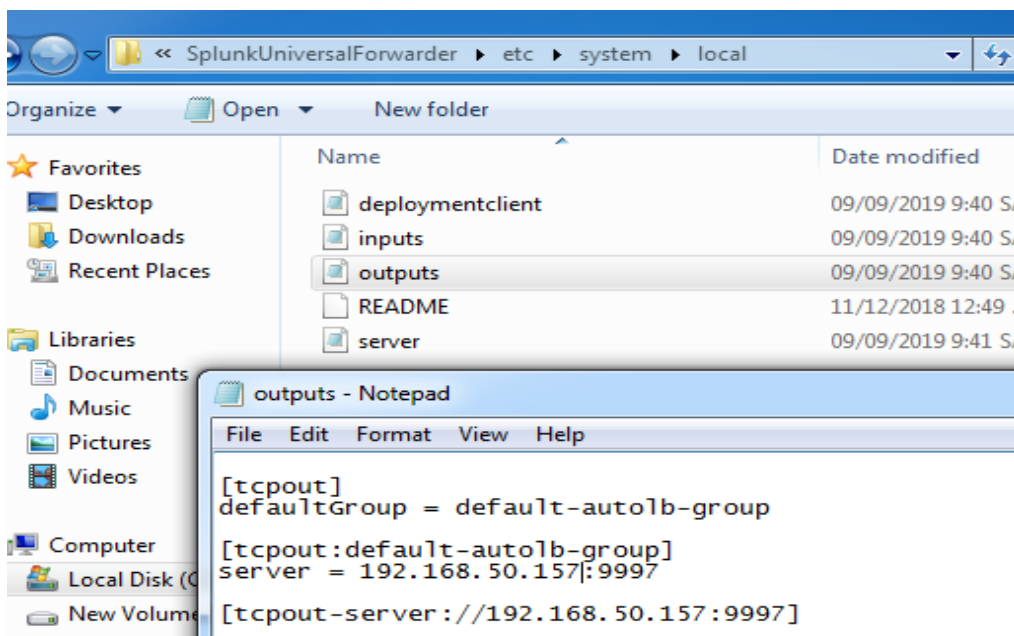
c:\>cd "Program Files"

c:\Program Files>cd SplunkUniversalForwarder

c:\Program Files\SplunkUniversalForwarder>cd bin

c:\Program Files\SplunkUniversalForwarder\bin>splunk list forward-server
Active forwards:
    192.168.50.157:9997
Configured but inactive forwards:
    None
```

Hình III.2.7

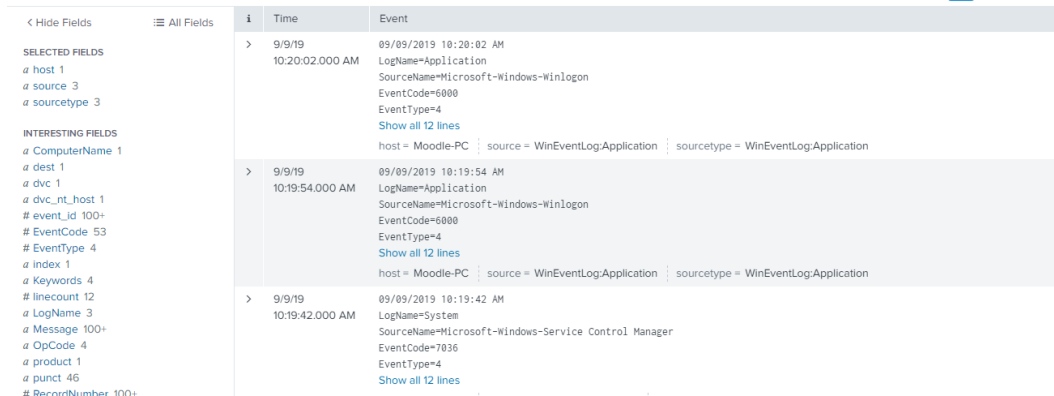


Hình III.2.8

- 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. Searching event trên Splunk sau Data mode

- Vào web browser truy cập [http://Splunk\\_server\\_ip:8000](http://Splunk_server_ip:8000)
- Kiểm tra xem log đã được đẩy lên splunk chưa.  
Search index = “winenventlog”

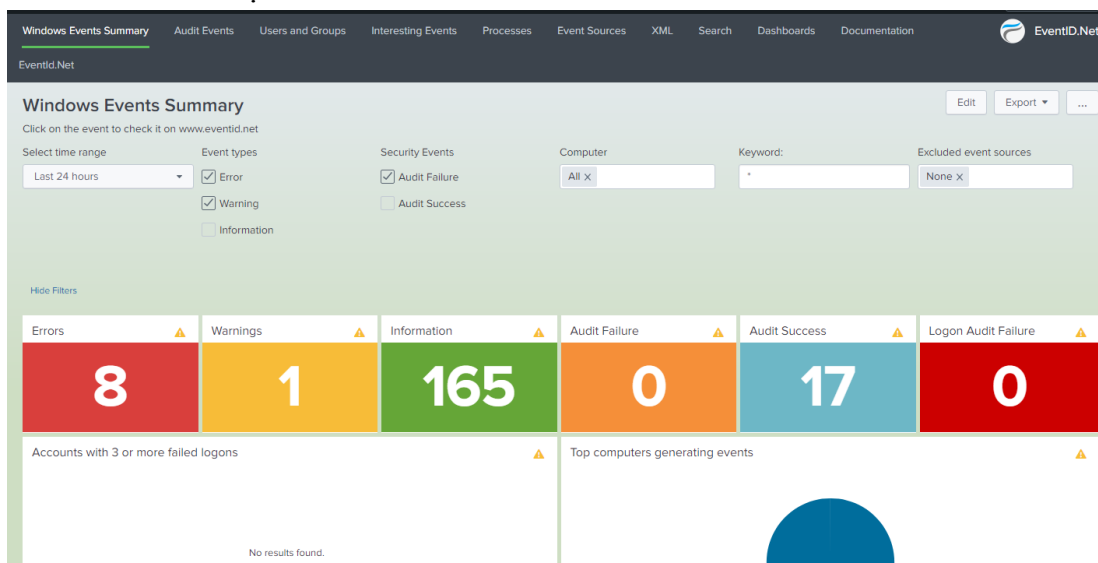


The screenshot shows the Splunk search interface. On the left, there are panels for 'SELECTED FIELDS' and 'INTERESTING FIELDS'. The main panel displays a list of search results with columns for Time and Event. The results show three log entries from 9/9/19, each with details like LogName, SourceName, EventCode, and EventType. The first two entries are from 'Moodle-PC' and the third is from 'System'.

Time	Event
9/9/19 10:20:02.000 AM	LogName=Application SourceName=Microsoft-Windows-winlogon EventCode=6000 EventType=4 host = Moodle-PC   source = WinEventLog:Application   sourcetype = WinEventLog:Application
9/9/19 10:19:54.000 AM	LogName=Application SourceName=Microsoft-Windows-winlogon EventCode=6000 EventType=4 host = Moodle-PC   source = WinEventLog:Application   sourcetype = WinEventLog:Application
9/9/19 10:19:42.000 AM	LogName=System SourceName=Microsoft-Windows-Service Control Manager EventCode=7036 EventType=4

Hình IV.1

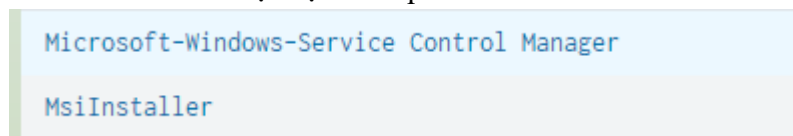
- Sau khi cấu hình và nhận event log thành công ta tiến hành phân tích sự kiện xảy ra trong hệ thống có thể sử dụng 2 app trên để thống kê báo cáo tình trạng của hệ thống mọi thời điểm một cách dễ nhất và nhanh gọn.
  - Lưu ý app: **windows infrastructure** chuyên dùng cho WindowServer, còn **windows-event-logs-analysis(EventID.Net)** 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 ra 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 thống
- **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 kiếm hiển thị sự kiện cách thủ công có chức năng giống app **search & reporting**
- **Doashboards:** Hiện thị danh sách các bảng điều khiển tự tạo sẵn ra khi cài app và thêm những cái của riêng bạn.

i	Title ^	Actions	Owner ⇅	App ⇅	Sharing ⇅
>	Audit Events	Edit ▾	nobody	eventid	App
>	Documentation	Edit ▾	nobody	eventid	App
>	Event Sources	Edit ▾	nobody	eventid	App
>	Interesting Events	Edit ▾	nobody	eventid	App
>	Processes	Edit ▾	nobody	eventid	App
>	Users and Groups	Edit ▾	nobody	eventid	App
>	Windows Events Summary	Edit ▾	nobody	eventid	App
>	XML	Edit ▾	nobody	eventid	App

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

```
> 9/11/19      09/11/2019 11:07:38 AM
11:07:38.000 AM LogName=System
                  SourceName=Microsoft-Windows-Service Control Manager
                  EventCode=7036
                  EventType=4
                  Type=Information
                  ComputerName=Moodle-PC
                  TaskCategory=The operation completed successfully.
                  OpCode=The operation completed successfully.
                  RecordNumber=2199
                  Keywords=Classic
                  Message=The Multimedia Class Scheduler service entered the running state.
                  Collapse
host = Moodle-PC | source = WinEventLog:System | sourcetype = WinEventLog:System
```

Hình V.1

```
> 9/11/19      09/11/2019 11:07:39 AM
11:07:39.000 AM LogName=System
                  SourceName=Microsoft-Windows-Application-Experience
                  EventCode=206
                  EventType=4
                  Type=Information
                  ComputerName=Moodle-PC
                  User=NOT_TRANSLATED
                  Sid=S-1-5-18
                  SidType=0
                  TaskCategory=The operation completed successfully.
                  OpCode=Info
                  RecordNumber=2200
                  Keywords=None
                  Message=The Program Compatibility Assistant service successfully performed phase two initialization.
                  Collapse
host = Moodle-PC | source = WinEventLog:System | sourcetype = WinEventLog:System
```

Hình V.2