**VIETNAM CYBERSPACE SECURITY TECHNOLOGY**

**JSC**

**🙜🙞🕮🙜🙞**



**BÁO CÁO**

**CÀI ĐẶT THU THẬP LOG**

**HỆ ĐIỀU HÀNH LINUX**

Người thực hiện: Mai Thành Thắng

Hà Nội, 9/2019

Mục Lục

[I. THÔNG TIN CHUNG 3](#_Toc19608445)

[1. Giới thiệu 3](#_Toc19608446)

[2. Source type và Data mode sử dụng 3](#_Toc19608447)

[3. Các bước thực hiện cấu hình, cài đặt 4](#_Toc19608448)

[II. CÀI ĐẶT SPLUNK VÀ ADD-ON,APP 5](#_Toc19608449)

[1. Hướng dẫn cài đặt splunk forwarder trên linux 5](#_Toc19608450)

[2. Hướng dẫn cài ADD-ON, APP: 5](#_Toc19608451)

[III. CẤU HÌNH NHẬN LOG TRÊN SPLUNK SERVER 6](#_Toc19608452)

[1. Mở cổng kết nối nhận dữ liệu: 6](#_Toc19608453)

[2. Cấu hình nhận dữ liệu: 7](#_Toc19608454)

[IV. SEACHING EVENT TRÊN SPLUNK SAU DATA MODE: 8](#_Toc19608455)

# THÔNG TIN CHUNG

## 1. Giới thiệu

* Mô tả việc thu thập log trên hệ điều hành Linux cài đặt trên VMware WorkStation 15 .
* Phiên bản win 7 Ultimate và Splunk 7.3+
* Loại log thu thập: syslog, CPU, DF, hardware, Interface, Iostat, lastlog, memory, netstat, open port, package,process, rlog,time, top, lsof, Users With Login Privs, who data

**Note:**

- DF: thông tin về ổ đĩa.

**-** Iostat: là một công cụ giám sát hệ thống máy tính được sử dụng để thu thập và hiển thị số liệu thống kê đầu vào và đầu ra của bộ lưu trữ hệ điều hành.

**-** lastlog: Nó định dạng và in nội dung của tệp nhật ký đăng nhập cuối cùng, / var / log / lastlog, bao gồm tên đăng nhập, cổng và ngày và thời gian đăng nhập cuối cùng.

**-** rlog: Hiển thị thông tin nhận dạng cho các tệp RCS, bao gồm thông báo nhật ký được liên kết với mỗi lần sửa đổi, số dòng được thêm hoặc xóa, ngày đăng ký cuối cùng, v.v.

- lsof: là một lệnh có trong nhiều hệ điều hành tựa Unix, có chức năng xuất ra danh sách tất cả các tập tin đamg được mở và những tiến trình đang mở chúng.

## 2. Source type và Data mode sử dụng

|  |  |  |
| --- | --- | --- |
| Sourcetype | Data model | **Ghi chú** |
| Syslog | web | Sử dụng Data model Web có sẵn trong app for unix |
| cpu |
| df |
| Hardware |
| Interfaces |
| iostat |
| Lastlog |
| lsof |
| vmstat |
| Netstat |
| openPorts |
| package |
| ps |
| rlog |
| Time |
| Top |
| usersWithLoginPrivs |
| who |

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

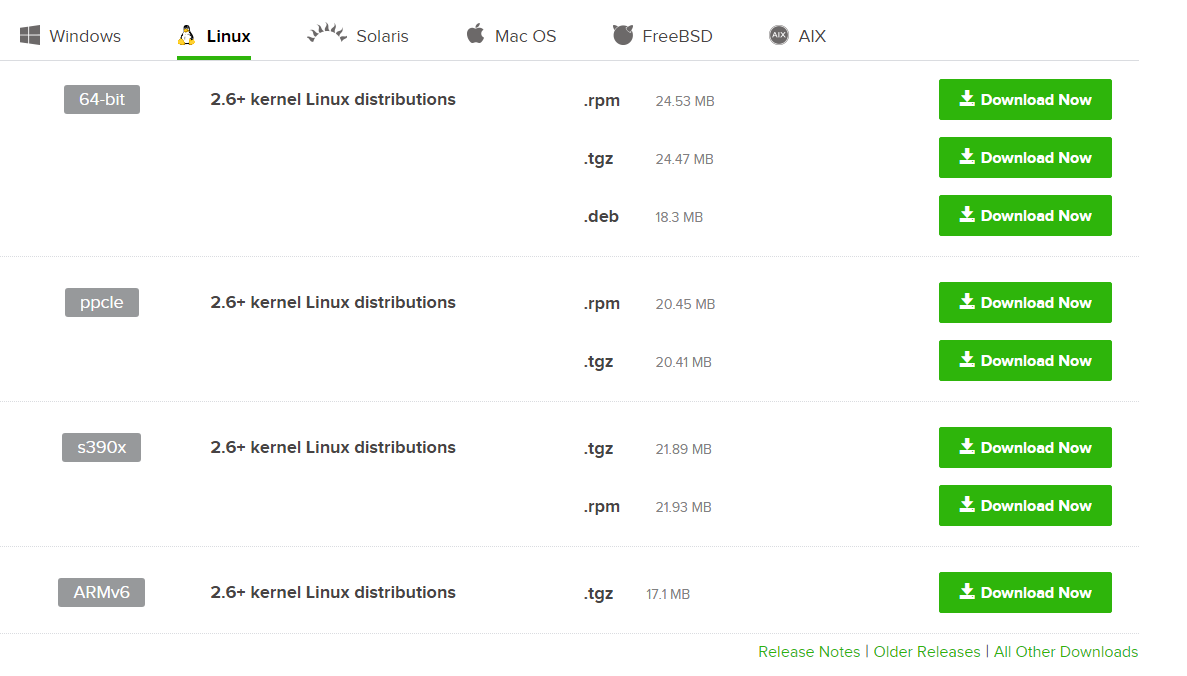
|  |  |  |
| --- | --- | --- |
| Bước thực hiện | Nội dung | Nơi cài đặt/cấu hình  (Agent, Server, SearchHead) |
| 1 | Cài đặt Splunk Server | Server |
| 2 | Cài đặt Linux server trên VM | Agent |
| 3 | Cài đặt Splunk forwarder | Agent |
| 4 | Cài đặt add-on và app Data Model | Server |
| 5 | Cài đặt 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 |

# CÀI ĐẶT SPLUNK VÀ ADD-ON,APP

* Các bước cài đặt splunk server đã trình bày trong [OnBoard – Vmware](https://github.com/Thang1102/OnBoard/blob/master/OnBroad-VMWorkStation.pdf)

## Hướng dẫn cài đặt splunk forwarder trên linux

- Lên trang chủ tải phầm mềm splunk forwarder về server linux cần lấy log(chọn đúng loại hệ điều hành bạn đang dùng trên linux):



- Tải về dùng lệnh wget ở đây mình dùng bản .tgz

- Lệnh cấu hình cài đặt:

$tar -xvzf splunkforwarder-7.3.0-657388c7a488-Linux-x86\_64.tgz -C /opt/

$cd /opt/splunkforwarder/bin

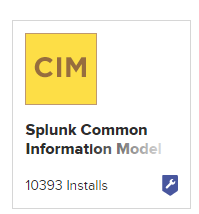
$ ./splunk start --accept-license

$ ./splunk enable boot-start

## 2. Hướng dẫn cài ADD-ON, APP:

* + Bước 1: vào url gõ: splunk base
  + Bước 2: Trên thanh tìm kiếm search “CIM”

Chọn phần mềm này:



* + Bước 3: tải về và tiến hành cài đặt giống như trình bày trong [OnBoard – Vmware](https://github.com/Thang1102/OnBoard/blob/master/OnBroad-VMWorkStation.pdf)

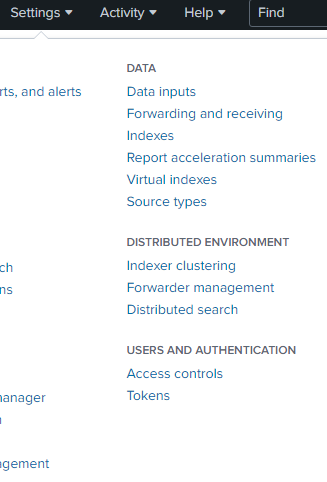
Kết quả:



# CẤU HÌNH NHẬN LOG TRÊN SPLUNK SERVER

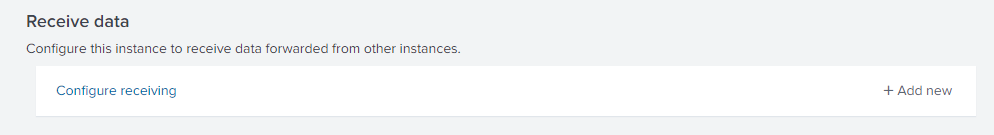
## **Mở cổng kết nối nhận dữ liệu**:

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



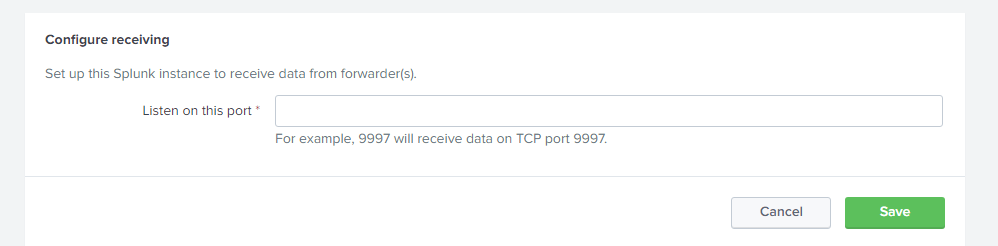
Hình III.1.1

* Chọn Recive Data -> Add new



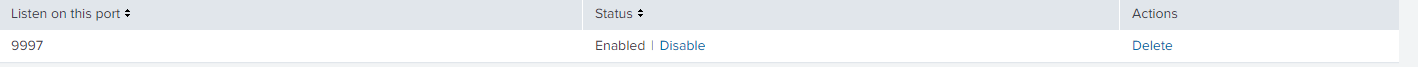
Hình III.1.2.

* Nhập cổng 9997 để nhận dữ liệu và bấm Save



Hình III.1.3

* Kết quả:



Hình III.1.4

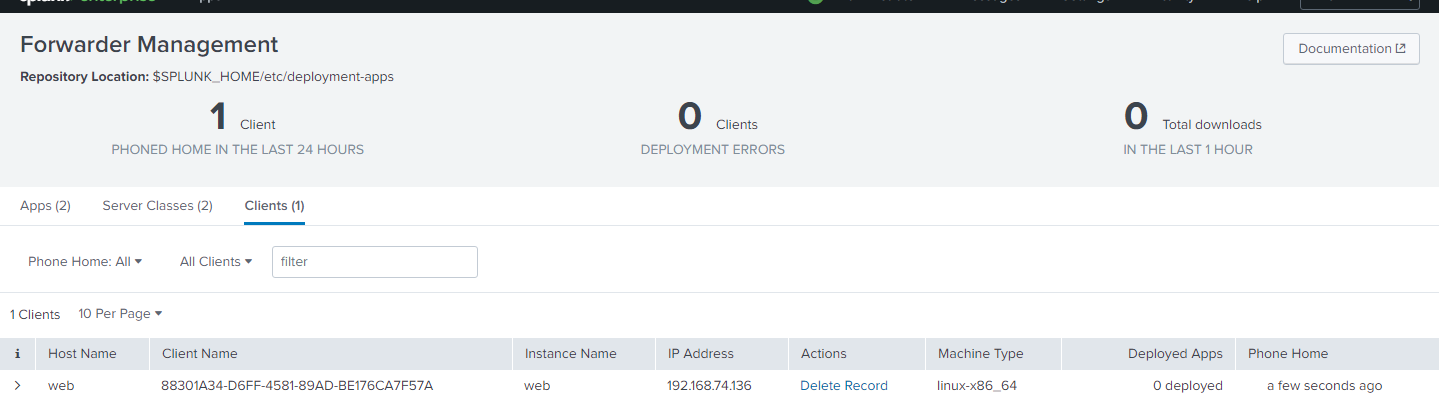
## Cấu hình nhận dữ liệu:

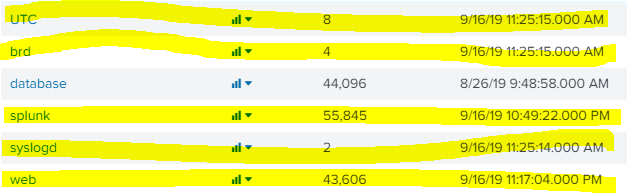
* Trên máy linux server ta sẽ cấu hình:

$ ./splunk add forward-server 192.168.74.131:9997

$ ./splunk set deploy-poll 192.168.74.131:8089

$ ./splunk add monitor /var/log/apache2/\*.log -index os

* Kết quả: 



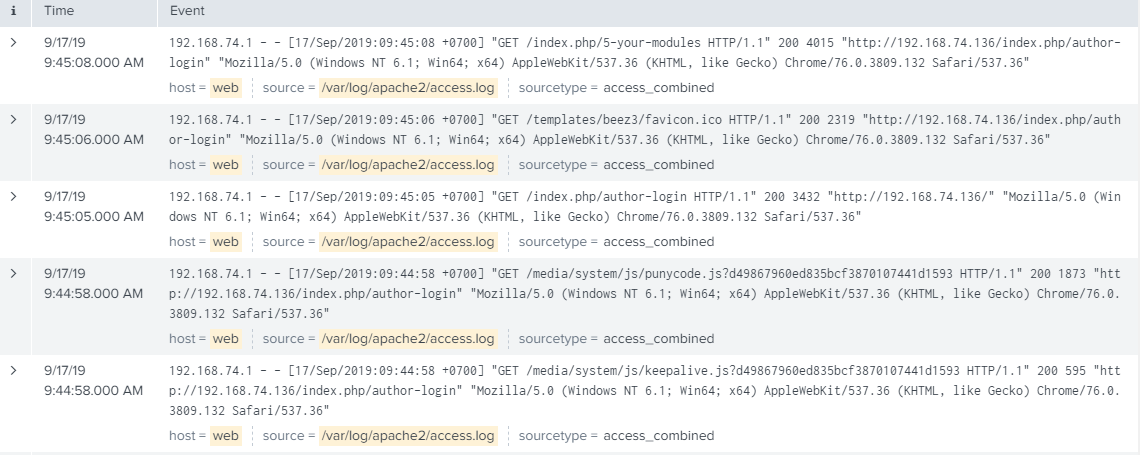
# SEACHING EVENT TRÊN SPLUNK SAU DATA MODE:

* Mô tả các trường được chỉnh sửa theo data model
* Searching theo data model
* Khi vào app search ta thực hiện search host = web ta có thể thấy một số thông tin



*Thông qua thông tin này ta có thể thấy sự kiện lấy từ file syslog. Sự kiện này là sự kiện quá trình máy linux được cấp ip.*

* Search index = os khi cài đặt ta có thể thấy sự kiện cập nhật về chỉ mục os.



*Sự kiện khi vào author-login hay là load lại trang web.*

# Một số vấn đề cần nhớ.

## Index cluster on splunk

* Index cluster là các nhóm gồm các indexer Splunk được cấu hình để lưu giữ nhiều bản sao dữ liệu. Điều này làm tăng dữ liệu tính sẵn sàng, độ trung thực của dữ liệu, dự phòng dữ liệu và hiệu suất tìm kiếm. Index clustersing là một tính năng phức tạp.

## Quyền hạn tối thiểu user để thực hiện cài đặt splunk forwarder

* Phải có quyền được đọc report và dashboard trên splunk
* Có quyền được xem, đọc sự kiện app được cài trong splunk forwarder

## Quản lý monitor từ forwarder lên splunk server

* Ngoài việc dùng lệnh CLI để add monitor ta có thể thêm cách thủ công: /opt/splunkforwarder/etc/apps/search/local
* Sau khi chỉnh sửa xong nhớ khởi động lại :

./splunk \_internal call /services/data/inputs/monitor/\_reload -auth