**VIETNAM CYBERSPACE SECURITY TECHNOLOGY**

**JSC**

**🙜🙞🕮🙜🙞**



**BÁO CÁO**

**CÀI ĐẶT SPLUNK THU THẬP LOG TỪ IIS**

NGƯỜI THỰC HIỆN : Lê Quốc Việt

**Hanoi, 2019**

MỤC LỤC

[DANH MỤC CÁC HÌNH VẼ 3](#_Toc16356331)

[1.1. Thông tin chung 4](#_Toc16356332)

[1.1.1. Giới thiệu 4](#_Toc16356333)

[1.1.1. Source type/Data model sử dụng 4](#_Toc16356334)

[1.1.2. Các bước thực hiện cài đặt, cấu hình 4](#_Toc16356335)

[1.2. Cài đặt và cấu hình Splunk Add-on 4](#_Toc16356336)

[1.2.1. Cài đặt Spunk Forwarder trên máy chủ IIS 4](#_Toc16356337)

[1.2.2. Cài đặt Splunk Add-on for IIS trên Splunk Indexer 6](#_Toc16356338)

[1.2.3. Cài đặt Splunk Add-on for IIS trên máy chủ IIS 7](#_Toc16356339)

[1.3. Cấu hình input dữ liệu từ IIS 8](#_Toc16356340)

[1.3.1. Cấu hình Splunk outputs 8](#_Toc16356341)

[1.3.2. Cấu hình enable log trên IIS 8](#_Toc16356342)

[1.3.3. Cấu hình inputs 10](#_Toc16356343)

[1.4. Searching dữ liệu indexed trên Splunk 10](#_Toc16356344)

[1.5. Chuẩn hóa dữ liệu theo data model 11](#_Toc16356345)

[1.5.1. Cài đặt CIM 11](#_Toc16356346)

[1.5.2. Cấu hình và chuẩn hóa data theo data model 11](#_Toc16356347)

[1.6. Searching dữ liệu sau data model 11](#_Toc16356348)

# DANH MỤC CÁC HÌNH VẼ

[Hình 1.5. Trang tải Splunk Forwarder 5](#_Toc16356206)

[Hình 1.6. Giao diện cài đặt UF 5](#_Toc16356207)

[Hình 1.1. Trang tải Splunk Add‑On for IIS 6](#_Toc16356208)

[Hình 1.2. Cài đặt Splunk Addon trên giao diện web 7](#_Toc16356209)

[Hình 1.1. Trang tải Splunk Add‑On for IIS 7](#_Toc16356210)

[Hình 1.7. Log IIS trên Splunk 11](#_Toc16356211)

## **Thông tin chung**

* + 1. **Giới thiệu**

Mô tả qua về việc việc thu thâp log IIS

* Phiên bản IIS được hỗ trợ
  + IIS 6, 7, 7.5, 8
* Các loại log sẽ cần lấy
  + Access log
  + Error log
    1. **Source type/Data model sử dụng**

|  |  |  |
| --- | --- | --- |
| Sourcetype | Data model | **Ghi chú** |
| ms:iis:default | Web | Sử dụng data model Web có sẵn trong CIM |
|  |  |  |

* + 1. **Các bước thực hiện cài đặt, cấu hình**

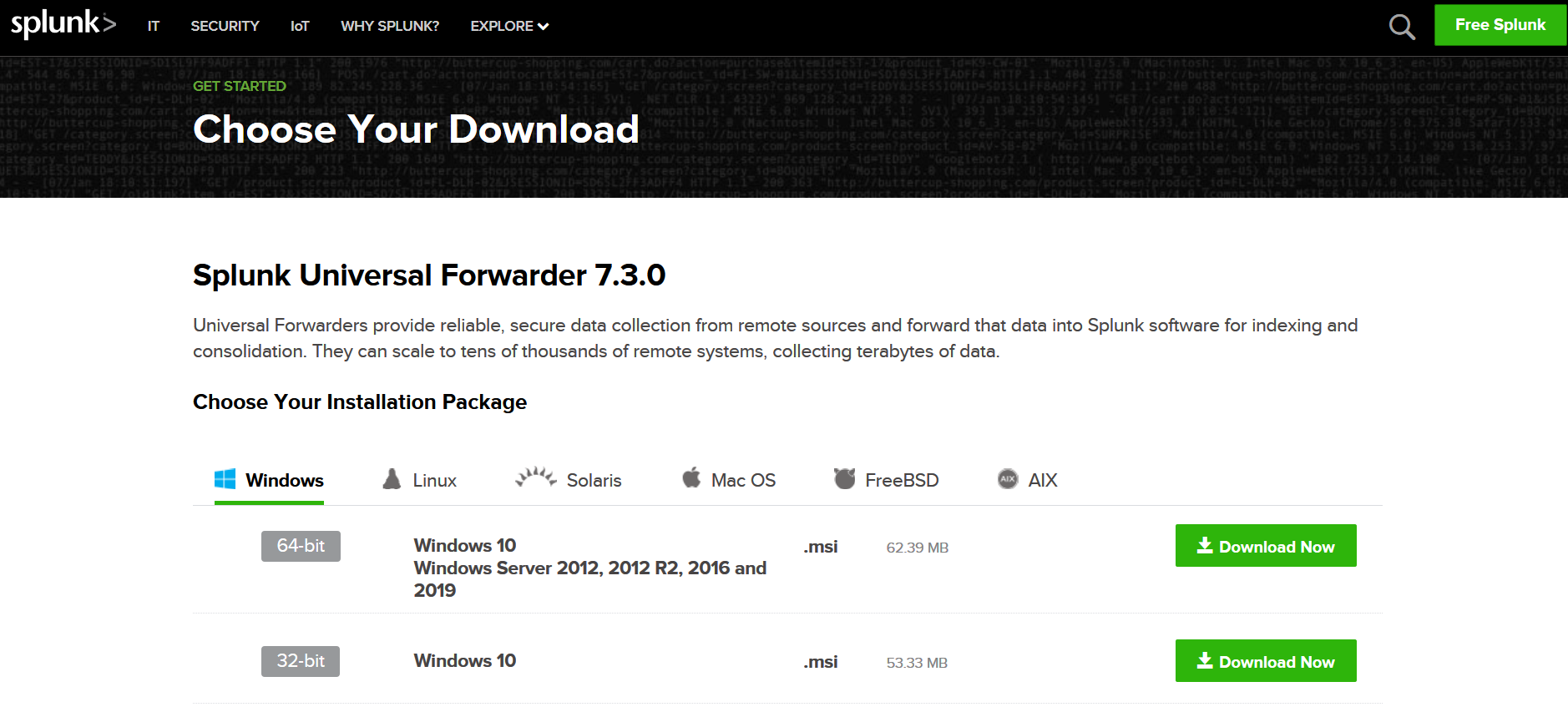
|  |  |  |
| --- | --- | --- |
| Bước thực hiện | Nội dung | Nơi cài đặt/cấu hình  (Agent, Indexer, SearchHead) |
| 1 | Cài đặt Splunk Add-on for IIS | Agent, Indexer |
| 2 | Cấu hình data input | Agent |
| 3 | Searching dữ liệu indexed trên Splunk | SearchHead |
| 4 | Chuẩn hóa dữ liệu theo data model | SearchHead |
| 5 | Searching dữ liệu sau data model | SearchHead |

## **Cài đặt và cấu hình Splunk** **Add-on**

* + 1. **Cài đặt Spunk Forwarder trên máy chủ IIS**

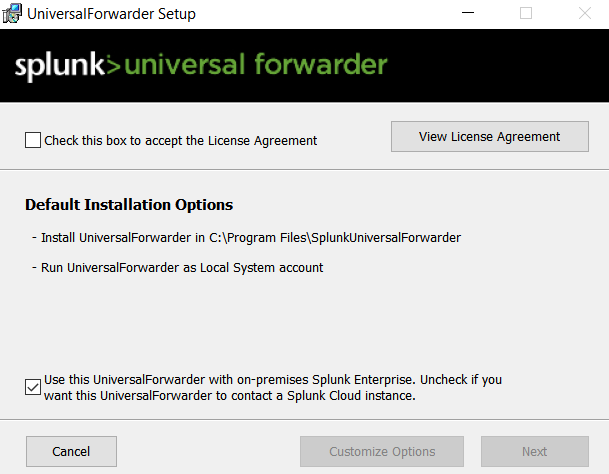
Để cài đặt Universal Forwarder, thực hiện các bước:

1. Kiểm tra máy tính cần cài đặt phù hợp với yêu cầu cấu hình của Splunk
2. [Download](http://www.splunk.com/download/universalforwarder) Tải **Splunk Forwarder** phù hợp với máy tính cài đặt.



**Hình 1.5. Trang tải Splunk Forwarder**

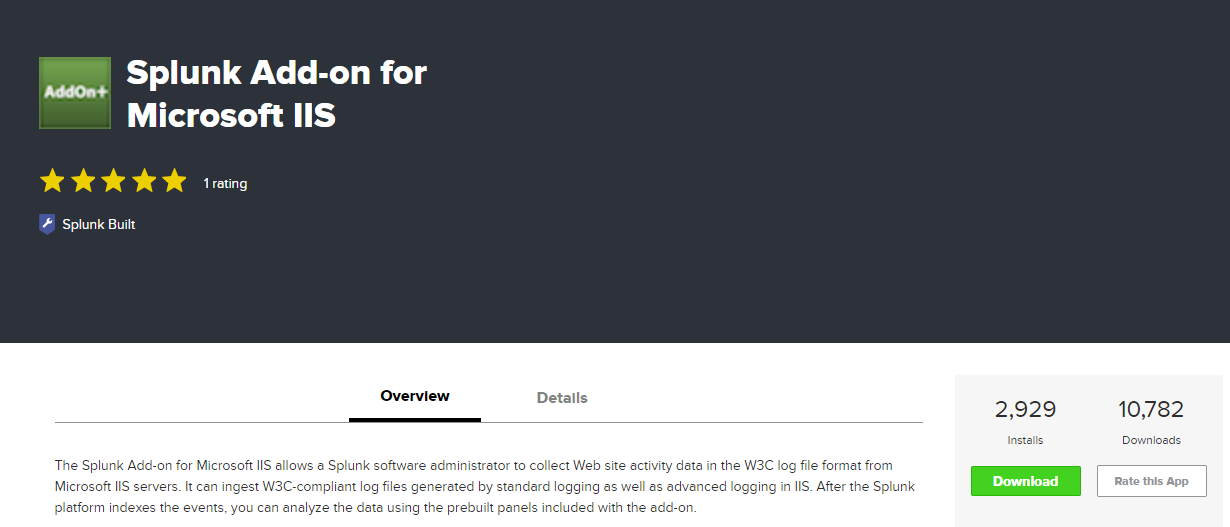
1. Tiến hành cài đặt:



**Hình 1.6. Giao diện cài đặt UF**

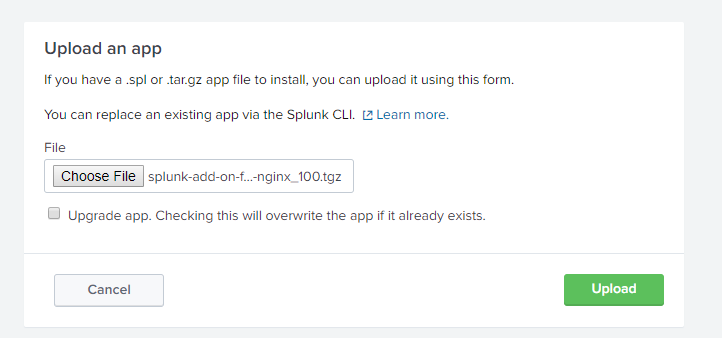
* + Chọn **Accept the license agreement**.
  + Chọn **Customize Options** để tùy chỉnh cấu hình cài đặt.
  + Chọn **Next** qua phần "Destination Folder".
  + Chọn **Next** qua phần "Certificate Information".
  + Ở phần "User selection”, chọn "Local System" và chọn **Next**
  + Ở phần "Enable Windows inputs", không tích vào ô nào và chọn **Next**.
  + Ở phần "Specify a Deployment Server" dialog, nhập địa chỉ IP của Deployment Server và cổng tương ứng (mặc định là 8089). Sau đó chọn **Next**.
  + Chọn **Next** qua phần "Receiving Indexer”.
  + Chọn **Install** để tiến hành cài đặt.

1. Sau khi cài đặt xong, có thể kiểm tra Splunk Forwarder đang chạy bằng cách:
   * Kiểm tra splunkforwarder trong Services control panel, hoặc
   * Sử dụng PowerShell window (vào thư mục %SPLUNK\_HOME%\bin và gõ.\splunk status).
     1. **Cài đặt Splunk Add-on for IIS trên Splunk Indexer**
2. Tải [Splunk Add-on for Microsoft IIS](https://splunkbase.splunk.com/app/3185/) từ splunkbase.



**Hình 1.1. Trang tải Splunk Add‑On for IIS**

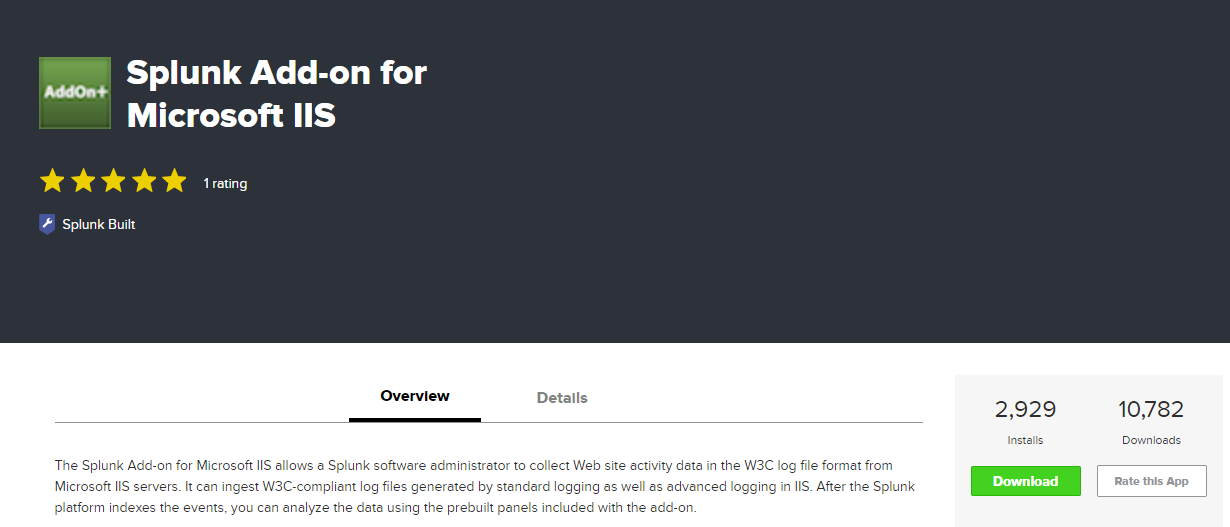
1. Mở giao diện Web của Splunk Enterprise trên trình duyệt và đăng nhập.
2. Đi đến phần quản lý app. **Apps > Manage Apps**
3. Chọn **Install app from file**và chọn addon đã tải xuống, có tên ***splunk-add-on-for-microsoft-iis\_101.tgz .***



**Hình 1.2. Cài đặt Splunk Addon trên giao diện web**

1. Click **Upload***.* Chờ đến khi cài xong và khởi động lại Splunk
   * 1. **Cài đặt Splunk Add-on for IIS trên máy chủ IIS**

* Tải [Splunk Add-on for Microsoft IIS](https://splunkbase.splunk.com/app/3185/) từ splunkbase.



**Hình 1.1. Trang tải Splunk Add‑On for IIS**

* Upload file ***splunk-add-on-for-microsoft-iis\_101.tgz*** lên máy chủ IIS tại thư mục **C:/setup**
* Cách 1: dùng lệnh cài đặt như sau:
  + Mở cửa sổ cmd bằng quyền Admin
  + Di chuyển đến thư mục C:/Program Files/Splunkforwarder/bin
  + Thực hiện lệnh cài đặt như sau:

***splunk install apps C:/setup/*** ***splunk-add-on-for-microsoft-iis\_101.tgz***

* Cách 2: giải nén file cài đặt và copy vào thư mục splunk
  + Giải nén file file ***splunk-add-on-for-microsoft-iis\_101.tgz***
  + Copy thư mục Splunk\_TA\_microsoft-iis vào thư mục cài đặt Splunk: **%SPLUNK\_HOME%\etc\apps\**
  + Khởi động lại Splunk
    - Truy cập cmd bằng quyền admin
    - Di chuyển đến thư mục C:/Program Files/Splunkforwarder/bin
    - Thực hiện lệnh: **splunk restart**

## **Cấu hình input dữ liệu từ IIS**

* + 1. **Cấu hình Splunk outputs**

1. Thêm Splunk forward-server và deploy-poll server

*./splunk set deploy-poll <host>:8089*

*./splunk add forward-server <host>:9997*

*./splunk restart*

1. Kiểm tra cấu hình

*./splunk show deploy-poll*

*Deployment Server URI is set to "<host>:8089".*

*./splunk list forward-server*

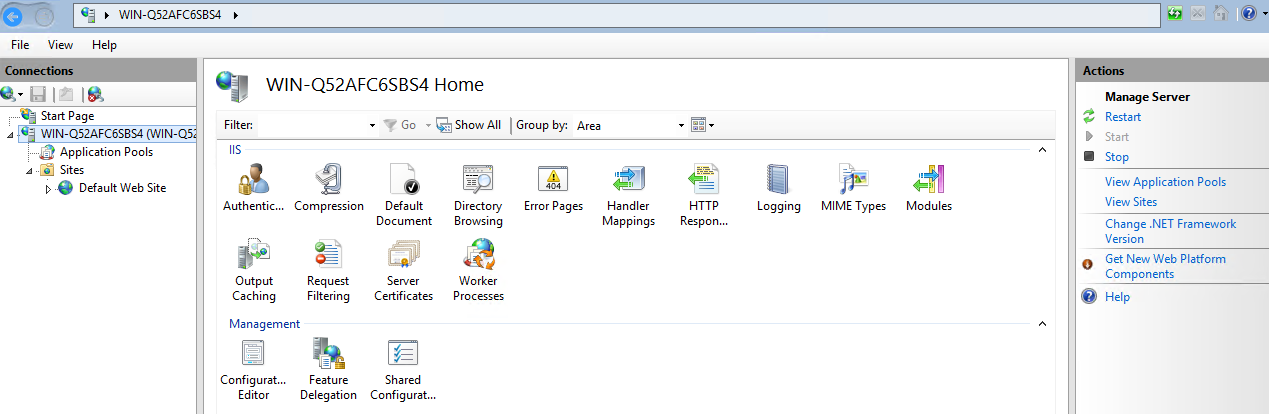
*Active forwards:*

*<host>:9997*

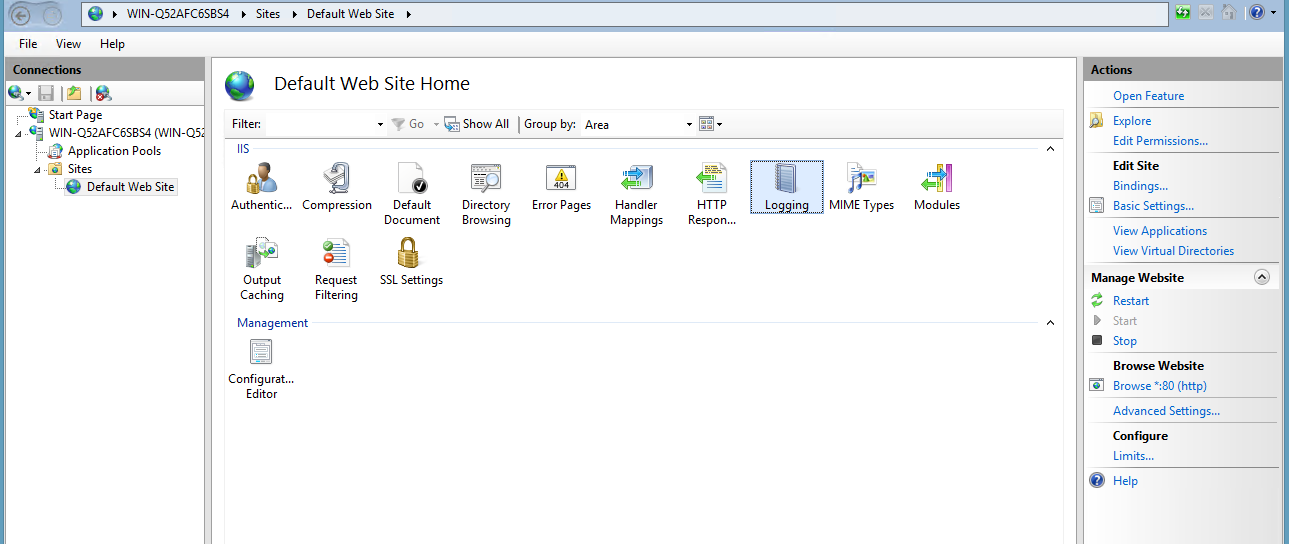
*Configured but inactive forwards:*

*None*

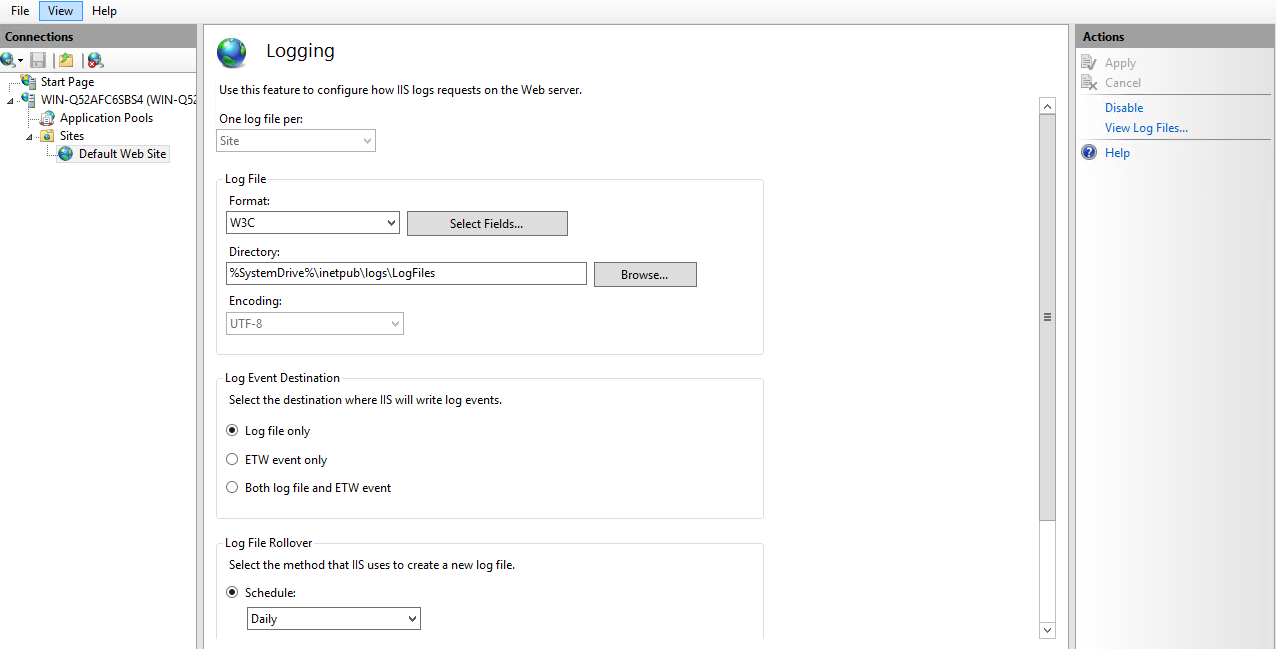
* + 1. **Cấu hình enable log trên IIS**
* Truy cập Internet Information Services (IIS) Manager trên windows Server
* Tại ServerName chọn website cần enable lấy log



* Chọn Logging



* Chọn Enable và format log IIS sử dụng



* + 1. **Cấu hình inputs**
* Cài đặt IIS log cho forwarder bằng cách sử file

*$SPLUNK\_HOME\etc\app\* *Splunk\_TA\_microsoft-iis\local\input.conf*

Ví dụ:

[monitor://C:\inetpub\logs\LogFiles\\*\\*.log]

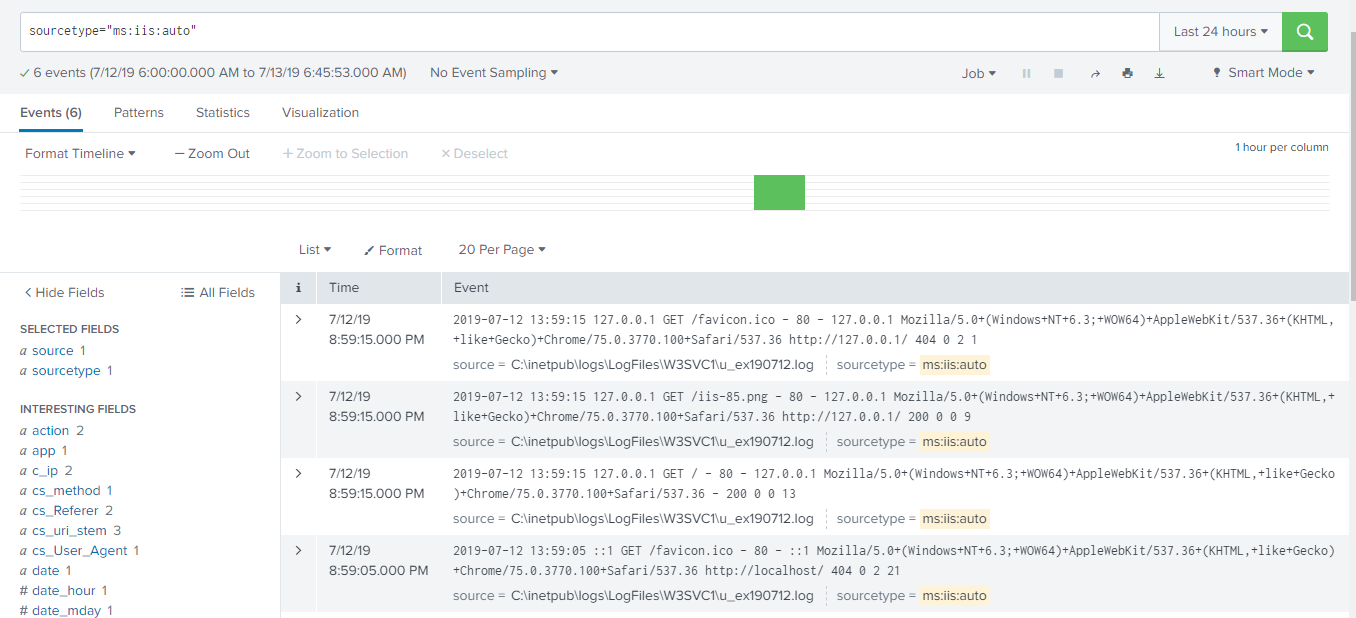
disabled = false

sourcetype = ms:iis:auto

* Khởi động lại Splunk Agent
  + Truy cập cmd bằng quyền admin
  + Di chuyển đến thư mục C:/Program Files/Splunkforwarder/bin
  + Thực hiện lệnh: **splunk restart**

## **Searching dữ liệu indexed trên Splunk**

1. Truy cập đến địa chỉ web thông qua trình duyệt http://<splunk\_ip>:8000.
2. Kiểm tra dữ liệu log đã được đẩy lên Splunk.

*sourcetype="ms:iis:auto"*

**Hình 1.7. Log IIS trên Splunk**

## **Chuẩn hóa dữ liệu theo data model**

* + 1. **Cài đặt CIM**
    2. **Cấu hình và chuẩn hóa data theo data model**

Mô tả các trường được chỉnh sửa theo data model

## **Searching dữ liệu sau data model**

Searching theo data model