Đồ Án Chuyên Đề Mạng Máy Tính

TRƯỜNG CAO ĐẲNG CÔNG NGHỆ THÔNG TIN
HỮU NGHỊ VIỆT – HÀN

KHOA CÔNG NGHỆ THÔNG TIN

ĐỒ ÁN CHUYÊN ĐỀ
NGÀNH: MẠNG MÁY TÍNH
Đề Tài:

TRIỂN KHAI PHÂN TÍCH FILE LOG
TRÊN WINDOWS SERVER 2012
GVHD: Th.S Lê Tự Thanh
SVTH: Trần Văn Lợi
Huỳnh Thanh Cường
Lớp:

CCMM07A

Khóa học: 2013 – 2016

Đà Nẵng, tháng 06 năm 2016

TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012

LỜI NÓI ĐẦU

Với tốc độ phát triển chóng mặt của ngành công nghệ thông tin với nhu cầu quá lớn từ nhiều người sử dụng, dẫn đến các hệ thống máy tính trở nên phức tạp, khó quản lý. Nhiều hệ thống không phải ở cùng một nơi, nằm phân tán. Các hệ điều hành, ứng dụng, dịch vụ được tạo ra bởi rất nhiều nguồn khác nhau. Lượng dữ liệu khổng lồ không ngừng gia tăng nhưng lại không tập trung. Vì vậy, chúng ta cần phải ghi lại hoạt động của hệ thống mà ở đây là Log. Thông thường, các bản ghi được lưu trữ phân tán trên các thiết bị khác nhau. Kiểm tra log theo phương pháp truyền thống là đăng nhập vào từng hệ thống để tìm kiểm tra, tìm kiếm lỗi gây mất thời gian, kém hiệu quả. Ngày nay, để giải quyết yêu cầu trên chúng em đã sử dụng bộ ELK để phân tích log theo thời gian thực giúp quản lý đăng nhập tập trung, thao tác đơn giản và tăng hiệu quả làm việc. Có thể đáp ứng một khối lượng lớn dữ liệu gây ra bởi một phân phối lưu trữ

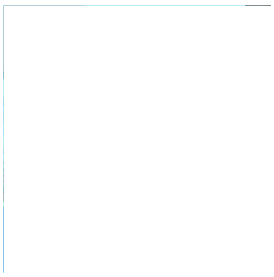
không phải chỉ có kích thước khổng lồ của dữ liệu để hoàn thành việc lập chỉ mục phân phối và thu hồi, mà còn cung cấp các phân tích tổng hợp số liệu; Logstash đối phó hiệu quả với nhiều nguồn dữ liệu khác nhau từ các thông tin đăng nhập, bảng điều khiển Kibana phân tích kết quả trực quan.

Cùng với đó, Windows Server 2012 đang ngày càng được sử dụng phổ biến rộng rãi. Và chúng ta rất dễ nhận thấy việc ghi lại mọi hoạt động của hệ thống mang lại nhiều lợi ích vô cùng cần thiết. Tuy nhiên, việc để phân tích được file log đối với nhiều người không phải là chuyện dễ dàng và không phải ai cũng làm được. Mà đặc biệt là đối với Windows Server 2012 hoặc đối với những người chưa thao tác nhiều với việc phân tích hoạt động của một hệ thống. Đây là lý do nhóm chúng em chọn "Triển Khai Phân Tích File Log Trên Windows Server 2012" làm đề tài Đồ án chuyên đề Mạng máy tính.

Nhóm chúng em xin được gửi lời cảm ơn chân thành đến thầy Ths.Lê Tự Thanh đã luôn đồng hành, định hướng, hỗ trợ nhiệt tình, với những ý kiến đóng góp quý báu của thầy đã giúp nhóm chúng em có thể hoàn thành đồ án chuyên đề này.

SVTH: Trần Văn Lợi_Huỳnh Thanh Cường

TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012



MỤC LỤC

SVTH: Trần Văn Lợi_Huỳnh Thanh Cường

2

TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012

DANH MỤC HÌNH ẢNH

SVTH: Trần Văn Lợi_Huỳnh Thanh Cường

3

TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012

CHƯƠNG 1 CƠ SỞ LÝ THUYẾT

1.1. Giới thiệu đề tài.

1.1.1 Bối cảnh thực hiện đề tài.

Hiện nay, với xu thế phát triển thế kỷ của lĩnh vực công nghệ thông tin, nó xâm nhập vào mọi lĩnh vực đời sống của con người song song với đó, chúng ta phải quản lý tốt các file trên hệ thống máy chủ web hoặc máy chủ proxy để phát hiện kịp thời, ngăn chặn nguy cơ tiềm ẩn từ các hoạt động web. Trước đó, nhóm chúng em đã triển khai phân tích file log Web Apache bằng bộ công cụ ELK. Tuy nhiên, mỗi hệ thống sẽ có nhiều loại log khác nhau đòi hỏi nhiều hướng phát triển phù hợp và có giá trị thực tế có thể ứng dụng vào thực tiễn. Chính vì thế, chúng em chọn “Triển khai phân tích file log trên Windows Server 2012” làm đề tài đồ án chuyên đề.

1.1.2 Mục đích thực hiện đề tài.

Triển khai phân tích, đánh giá được trạng thái hoạt động và quản lý tốt các filelog được tạo ra trên máy chủ có chứa tất cả thông tin hoạt động trên máy chủ đó.

1.2. Giới thiệu file log.

File log là một tập tin được tạo ra bởi một máy chủ web hoặc máy chủ proxy có chứa tất cả thông tin về các hoạt động trên máy chủ đó, như thông tin người truy cập, thời gian khách viếng thăm, địa chỉ IP, dữ liệu truy vấn. File log có rất nhiều tác dụng

Log bao gồm bản ghi hệ thống, các bản ghi ứng dụng, và bản ghi bảo mật. Hệ thống vận hành và bảo trì, và các nhà phát triển có thể đăng nhập cho phần cứng máy chủ và phần mềm thông tin, những lý do cho việc kiểm tra các lỗi cấu hình và các lỗi xảy ra. Phân tích các log thường có thể hiểu được tại máy chủ, hiệu suất, bảo mật để có biện pháp khắc phục kịp thời.

1.2.1 Log FTP

FTP (viết tắt của File Transfer Protocol dịch ra là “Giao thức truyền tập tin”) Thường được dùng để trao đổi tập tin qua mạng lưới truyền thông dùng giao thức TCP/IP (chẳng hạn như Internet – mạng diện rộng – mạng nội bộ). Hoạt động của FTP cần có hai máy tính, một máy chủ và một máy khách). Máy chủ FTP, dùng chạy phần mềm cung cấp dịch vụ FTP, gọi là trình chủ, lắng nghe yêu cầu về dịch vụ của các máy tính khác trên mạng lưới.

Log FTP như sau:

Hình 1.1 Nội dung file FTP

1.2.2 Log Firewall

Windows Firewall log là một tập tin văn bản thô có thể được xem thông qua bất kỳ trình soạn thảo. Notepad là trình soạn thảo văn bản mặc định cho các file log của Windows Firewall. Tùy thuộc vào kích thước giới hạn đặt ra cho các tập tin và thời gian các sự kiện xảy ra trên hệ thống.

Log Firewall có nội dung như sau:

Hình 1.2 Nội dung file log Firewall

1.3. Giới thiệu về bộ công cụ ELK (Elasticsearch + Logstash + Kibana).

1.3.1 Giới thiệu Elasticsearch.

Elasticsearch là một công cụ mã nguồn mở tìm kiếm toàn văn bản và phân tích khả năng mở rộng. Nó cho phép bạn lưu trữ, tìm kiếm và phân tích khối lượng lớn dữ liệu một cách nhanh chóng và gần thời gian thực.Nó thường được sử dụng như các công cụ / công nghệ cơ bản mà quyền hạn các ứng dụng có tính năng tìm kiếm phức tạp và yêu cầu.

Elasticsearch được xây dựng trên một công cụ tìm kiếm toàn văn bản dựa trên công cụ tìm kiếm của Apache Lucene, viết bằng Java.

Các tính năng chính:

- Phân tích thời gian
- Phân phối lưu trữ tập tin theo thời gian thực, và từng lĩnh vực được lập chỉ mục
- Tài liệu định hướng, tất cả các đối tượng là tất cả các tài liệu
- Tính sẵn sàng cao, dễ dàng mở rộng, hỗ trợ cluster (Cluster), phân mảnh và nhân rộng (Shards và bản sao).
- Giao diện thân thiện, hỗ trợ cho JSON

1.3.2 Giới thiệu Logstash.

Logstash là một công cụ mã nguồn mở cho việc thu thập, phân tích, và lưu trữ các bản ghi để sử dụng trong tương lai. Sử dụng ngôn ngữ Jruby.

Các tính năng chính:

- Hỗ trợ mở rộng đàn hồi.

Các thành phần chính:

- Shipper: gửi dữ liệu đăng nhập.
- Broker: thu thập dữ liệu, tích hợp mặc định Redis.
- Dữ liệu Indexer: viết.

Hình 1.3 Các thành phần cơ bản của Logstash

1.3.3 Giới thiệu Kibana.

Kibana là công cụ phân tích mã nguồn mở và trực quan được thiết kể để làm việc với Elasticsearch.

Kibana có giao diện web có thể được sử dụng để tìm kiếm, xem và tương tác với dữ liệu được lưu trữ tại các bản ghi mà Logstash đã lập chỉ mục. Cho phép bạn tạo và chia sẻ nhanh chóng các biểu đồ động hiển thị những thay đổi để Elasticsearch truy vấn trong thời gian thực.

Kibana dựa trên Apache giấy phép mã nguồn mở, sử dụng ngôn ngữ JavaScript.

Nó có thể được tìm thấy trong chỉ số Elasticsearch, dữ liệu tương tác và tạo ra một loạt các kích thước của bảng của FIG.

Có thể dễ dàng thực hiện phân tích dữ liệu tiên tiến và hiển thị dữ liệu của bạn trong một loạt các biểu đồ, bảng biểu và bản đồ.

Logstash-forwarder (tên gọi trước đây là Lumberjack) là một trong rất nhiều "shipper" dùng để đẩy log đến server log tập trung, có nhiều tính năng đặc biệt sau:

- Nhẹ và dễ sử dụng (viết bằng Go, không cần JVM)
- Sử dụng mật mã để truyền dữ liệu trên đường truyền.

Nguyên lý hoạt động cơ bản:

Hình 1.4 Kiến trúc ngăn sếp ELK

Quá trình thu thập log diễn ra như sau:

- Các Shipper(như logstash-forwarder,…) từ Client đẩy log đến Broker, sau khi xử lý xong Broker sẽ đưa log vào một hàng đợi trước khi nó được chuyển tiếp đến Logstash.
- Logstash xử lý các bản tin log vừa chuyển đến và lưu trữ nó dưới dạng JSON document vào trong ElasticSearch.
- ElasticSearch có nhiệm vụ chính là lưu trữ và tìm kiếm tất cả các dữ liệu.
- Sau đó bản tin Log được hiển thị trên Kibana Web Interface.

1.4 Yêu cầu hệ thống

Nền tảng thử nghiệm:

- Ubuntu Desktop 14.04
- Windows Server 2012
- RAM 4GB
- CPU 2

Phần mềm sử dụng:

- ElasticSearch
- LogStash

SVTH: Trần Văn Lợi_Huỳnh Thanh Cường

10

TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012

CHƯƠNG 2: TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012

2.1 Mô hình triển khai:

Hình 2.1 Mô hình triển khai.

2.2 Hướng dẫn cài đặt Windows Server 2012

Bước 1: Bật VMware Workstation => chọn Typical(Recommentded) => nhấn Next.

Hình 2.2 Cửa sổ làm việc của Vmware Workstation.

SVTH: Trần Văn Lợi_Huỳnh Thanh Cường

11

TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012

Bước 2: Chọn file .iso Windows Server 2012.

Hình 2.3 Chọn file .ISO

Bước 3: Tích vào Microsoft Windows. Ở phần Version chọn Windows Server 2012.

Hình 2.4 Chọn hệ điều hành và phiên bản.\

SVTH: Trần Văn Lợi_Huỳnh Thanh Cường

12

TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012

Bước 4: Đặt tên cho máy và chọn vị trí lưu cài đặt.

Hình 2.5 Đặt tên máy.

Bước 5: Chọn ngôn ngữ cài đặt, múi giờ, ngôn ngữ bàn phím.

Hình 2.6 Ngôn ngữ cài đặt, múi giờ, ngôn ngữ bàn phím.

SVTH: Trần Văn Lợi_Huỳnh Thanh Cường

13

TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012

Bước 6: Sau khi nhấp chuột vào Install Now (cài đặt) sẽ xuất hiện bảng yêu cầu nhập key cài đặt.

Hình 2.7 Nhập Key cài đặt.

Hình 2.8 Chọn phiên bản Windows server 2012.

SVTH: Trần Văn Lợi_Huỳnh Thanh Cường

14

TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012

Bước 8: Tích vào I accept the license items.

Hình 2.9 Giao diện license items.

Bước 9: Sau khi chọn Custom(cài đặt mới từ đầu) => Phân vùng ổ đĩa để cài đặt.

Hình 2.10 Giao diện phân vùng đĩa.

SVTH: Trần Văn Lợi_Huỳnh Thanh Cường

15

TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012

Bước 10: Quá trình cài đặt đang được tiến hành.

Hình 2.11 Đang bắt đầu quá trình cài đặt.

Giao diện màn hình Windows Server 2012 sau khi cài đặt xong.

Hình 2.12 Giao diện làm việc của Windows Server 2012.

SVTH: Trần Văn Lợi_Huỳnh Thanh Cường

16

TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012

2.3 Hướng dẫn cài đặt IIS trên Windows Server 2012
Bước 1: Tại Server Manager chọn Add roles and features
Bước 2: Click Next. Trong hộp Server Roles chọn Web Server (IIS) => Next =>
add features.

Hình 2.13 Cửa sổ Add roles and features Wizard.
Bước 3: Click next => chọn Roles Services

Hình 2.14 Giao diện Role services.

SVTH: Trần Văn Lợi_Huỳnh Thanh Cường

17

TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012

Bước 4: Nhấn Next rồi chọn Install để cài đặt.

Hình 2.15 Đang cài đặt Progress.

SVTH: Trần Văn Lợi_Huỳnh Thanh Cường

18

TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012

Sau khi quá trình cài đặt hoàn tất bạn chọn Close.
Để tạo ftp ta chọn vào tool => Internet information Services (IIS) Manager

Hình 2.17 Giao diện IIS Manager.

Sau đó right click vào Sites chọn Add FTP Sites
Đặt tên và lưu đường dẫn cho FTP sites

Hình 2.18 Đặt tên FTP site.

SVTH: Trần Văn Lợi_Huỳnh Thanh Cường

19

TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012

Vào FTP Authentication chọn Enabled ở trạng thái nhóm Anonymous Authentication

Hình 2.19 Giao diện làm việc FTP

2.4 Cách lấy file log trong Windows server 2012
2.4.1 Lấy Log FTP:

Hình 2.20 Vào phần IIS trên Windows Server 2012

SVTH: Trần Văn Lợi_Huỳnh Thanh Cường

20

TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012

Hình 2.21 Cấu hình thông tin để cho file log ftp.

Cài đặt client windown 7

Hình 2.22 Cài đặt windown 7 làm client cho hệ thống.

SVTH: Trần Văn Lợi_Huỳnh Thanh Cường

21

TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012

Hình 2.23 Quá trình đang cài đặt.
Sau khi quá trình cài đặt hoàn thành ta vào ftp với địa chỉ của máy windows server 2012.

Hình 2.24 Từ máy client ta truy cập vào ftp với địa chỉ ip của máy server.

22

TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012

Ta có thể cài đặt nhiều máy client để có thể phân tích được nhiều thông tin file log hơn
Tại máy server ta chọn vào view logs để xem nội dung của file log.

Hình 2.25 Nội dung file log ftp.

2.4.2 Lấy Log firewall
Để lấy file log firewall ta mở cửa sổ windows firewall with advanced security

Hình 2.26 Cửa sổ windows firewall.

SVTH: Trần Văn Lợi_Huỳnh Thanh Cường

23

TRIỂN KHAI PHÂN TÍCH FILE LOG TRÊN WINDOWS SERVER 2012

Sau đó kích chuột vào Action chọn properties

Hình 2.27 Vào Action chọn properties.
Ở mục Domain profile
Tại firewall state ta chọn On .
Tại logging ta kích vào Customize logging setting for the domain frofile để mở cửa sổ Customize logging setting for the domain frofile > chọn Yes ở mục Logdropped packets và chọn Yes ở mục Log successful connections. > chọn Ok.

Hình 2.28 Cửa sổ Domain profile.
SVTH: Trần Văn Lợi_Huỳnh Thanh Cường

24