



ĐẠI HỌC ĐÀ NẴNG
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG VIỆT - HÀN
Vietnam - Korea University of Information and Communication Technology

GIÁM SÁT MẠNG

Giảng viên: Lê Tự Thanh

Email : ltthanh@vku.udn.vn

Website : www.vku.udn.vn

<http://vku.udn.vn/>

4.1. Khái niệm Log file

Log file là file chứa danh sách các sự kiện đã được máy tính, thiết bị "ghi nhật ký". Log ghi lại liên tục các thông báo về hoạt động của cả hệ thống hoặc của các dịch vụ được triển khai trên hệ thống và file tương ứng. Log file thường là các file văn bản thông thường dưới dạng “clear text” tức là bạn có thể dễ dàng đọc được nó, vì thế có thể sử dụng các trình soạn thảo văn bản (vi, vim, nano...) hoặc các trình xem văn bản thông thường (word, notepad...) là có thể xem được file log.

Tác dụng của Log file

- ✓ Log file ghi lại liên tục các thông báo về hoạt động của cả hệ thống hoặc của các dịch vụ được triển khai trên hệ thống và file tương ứng.
- ✓ Phân tích nguyên nhân gốc rễ của một vấn đề.
- ✓ Giúp cho việc khắc phục sự cố nhanh hơn khi hệ thống gặp vấn đề.
- ✓ Giúp cho việc phát hiện, dự đoán một vấn đề có thể xảy ra đối với hệ thống.

CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

DrayTek **Vigor3900 Series**

System Maintenance >> Syslog / Mail Alert >> Syslog File

Auto Logout: 5Min

Quick Start Wizard
Online Status
WAN
LAN
Routing
NAT
Firewall
Objects Setting
User Management
Applications
VPN and Remote Access
Certificate Management
SSL Proxy
Bandwidth Management
USB Application
System Maintenance
TR-069
Administrator Password
Configuration Backup
Syslog / Mail Alert
Time and Date
Access Control
SNMP Setup
Reboot System
Firmware Upgrade
APP Signature Upgrade
APP Support List

Syslog File Syslog Access Setup Mail Alert

Refresh Download Log Clear Syslog Auto Refresh: 10 Seconds

Search

Log

1	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.21.18.254:57952 -> 13.89.178.26:443 (TCP)
2	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.21.17.250:49166 -> 74.125.200.138:443 (TCP)
3	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.21.17.250:49165 -> 142.250.4.139:443 (TCP)
4	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.22.18.250:57734 -> 172.217.194.102:443 (TCP)
5	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.21.18.250:38534 -> 54.88.105.17:443 (TCP)
6	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.21.19.250:45412 -> 52.77.180.34:443 (TCP)
7	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.22.12.240:57368 -> 20.190.144.165:443 (TCP)
8	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.21.19.250:63541 -> 143.92.85.2:443 (TCP)
9	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.22.18.250:57733 -> 142.251.12.155:443 (TCP)
10	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.21.19.250:49712 -> 104.208.16.90:443 (TCP)
11	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.21.17.250:62812 -> 142.250.4.139:443 (TCP)
12	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.22.12.240:57367 -> 52.98.33.130:443 (TCP)
13	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.22.12.240:57366 -> 20.44.229.112:443 (TCP)
14	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.22.12.240:57365 -> 52.98.71.50:443 (TCP)
15	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.22.12.240:57364 -> 20.197.75.125:443 (TCP)
16	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.22.12.240:57363 -> 117.18.232.173:443 (TCP)
17	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.21.19.250:63540 -> 103.115.78.89:443 (TCP)
18	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.21.19.250:51086 -> 103.115.76.67:443 (TCP)
19	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.21.19.250:65406 -> 142.251.12.132:443 (TCP)
20	<150>Dec 6 15:45:10 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.21.19.250:65405 -> 142.251.12.132:443 (TCP)
21	<150>Dec 6 15:45:09 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.21.18.250:54720 -> 151.139.128.10:443 (TCP)
22	<150>Dec 6 15:45:09 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.22.18.250:57732 -> 125.253.113.30:443 (TCP)
23	<150>Dec 6 15:45:09 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.21.19.40:50261 -> 51.79.234.101:443 (TCP)
24	<150>Dec 6 15:45:09 Vigor: Local User: (MAC=00:11:88:b8:65:22) 10.21.19.40:50260 -> 103.231.98.193:443 (TCP)

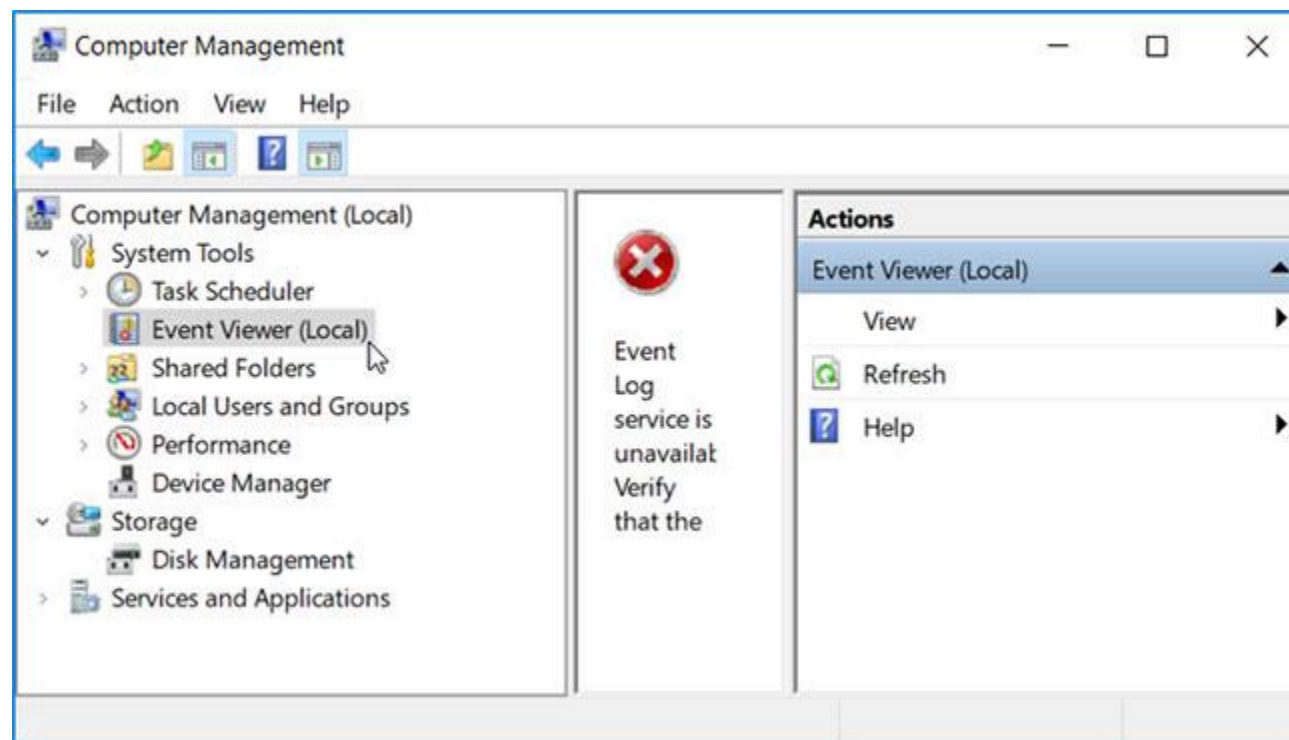
4.2. Phân loại log file

- Log file của các thiết bị firewall, router, ...
- Log file của hệ điều hành Linux, Windows, ...
- Log file của ứng dụng Web, Mail, Database, ...
- Log file của các phần mềm truyền thông, ...

CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

4.3. Các kỹ thuật phân tích log file

4.3.1. Phân tích Windows log file



Các kiểu Event

- ✓ Hệ điều hành Windows phân loại các sự kiện thành 5 loại:
Information event: Mô tả sự thành công của một công việc, chẳng hạn như cài đặt xong một ứng dụng.
- ✓ Warning event: Thông báo cho quản trị viên một vấn đề tiềm ẩn, chẳng hạn không gian đĩa thấp.
- ✓ Error message: Mô tả một vấn đề quan trọng mà có thể dẫn đến tính năng nào đó bị vô hiệu hóa.
- ✓ Success audit event: Mô tả một hoạt động thành công, chẳng hạn như một người dùng cuối đăng nhập thành công vào hệ thống.

CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

Các kiểu Event

- ✓ Failure audit event: Mô tả một hoạt động không thành công, chẳng hạn như một người dùng cuối nhận được thông báo khi nhập mật khẩu không chính xác.

Cấu trúc Event log

Mỗi sự kiện trong một bản ghi chứa các thông tin sau:

- ✓ Date: Ngày mà sự kiện xảy ra.
- ✓ Time: Thời gian diễn ra sự kiện.
- ✓ User: Tên người sử dụng của người dùng đã đăng nhập vào khi sự kiện xảy ra.
- ✓ Computer: Tên của máy tính.
- ✓ Event ID: Số định danh tương ứng với sự kiện.
- ✓ Source: Chương trình hoặc một ứng dụng thực hiện sự kiện..
- ✓ Type: Kiểu của sự kiện (information event, warning event, error message, security success audit event hoặc failure audit event).

4.3.2. Phân tích Linux log file

Trong hệ quản trị Linux thì kho lưu trữ Log được tập trung tại các file log trong thư mục **/var/log/**, nó chứa hầu hết các file log như access log, error log, app log, service log, system log.

4.3.2. Phân tích Linux log file

- Audit.log: Chứa thông tin xác thực trên hệ thống trong máy chủ được ghi lại. Khi các bạn tìm kiếm vấn đề liên quan đến cơ chế ủy quyền của người dùng
- Boot.log: chính là nơi lưu trữ tất cả thông tin liên quan đến khởi động và mọi thông báo được ghi lại trong quá trình khởi động bao gồm tập lệnh khởi tạo hệ thống,...
- Kern.log: Thông qua file log này giúp cho chúng ta có thể khắc phục các lỗi và cảnh báo liên quan đến kernel. Kernel log có thể hữu ích trong việc khắc phục sự cố kernel và có ích trong việc gỡ lỗi các vấn đề phần cứng.

CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

4.3.2. Phân tích Linux log file

- Yum.log: Thông qua file log này giúp cho chúng ta có thể theo dõi việc cài đặt các thành phần hệ thống và gói phần mềm. Kiểm tra các thông tin được ghi lại ở đây để xem một gói đã được cài đặt chính xác hay chưa. Từ đây giúp cho chúng ta có thể khắc phục sự cố liên quan đến cài đặt phần mềm.
- Mail.log: File log lưu trữ các thông tin từ máy chủ mail đang chạy trên hệ thống bao gồm các thông tin về dịch vụ email.
- Ngoài ra còn có nhiều file log khác như: user.log, dpkg.log,...

4.3.2. Phân tích Linux log file

Ví dụ: Log đăng nhập thành công

```
[root@vqmanh ~]# last -f /var/log/wtmp
hoặc utmpdump /var/log/wtmp
root      pts/3      66.0.0.254      Tue Sep 17 08:24    still logged in
vqmanh    pts/1      66.0.0.254      Tue Sep 17 08:19    still logged in
root      pts/2      66.0.0.254      Tue Sep 17 08:13    still logged in
vqmanh    pts/1      66.0.0.254      Tue Sep 17 08:04 - 08:18  (00:14)
```

4.3.2. Phân tích Linux log file

Apache error log:

```
[Fri Dec 16 01:46:23 2005] [error] [client 1.2.3.4] Directory index forbidden by rule: /home/test/  
[Fri Dec 16 01:54:34 2005] [error] [client 1.2.3.4] Directory index forbidden by rule: /apache/web-data/test2  
[Fri Dec 16 02:25:55 2005] [error] [client 1.2.3.4] Client sent malformed Host header  
[Mon Dec 19 23:02:01 2005] [error] [client 1.2.3.4] user test: authentication failure for "/~dcid/test1": Password Mismatch
```

Apache error log (startup) 3 examples:

```
** Normal (v2.x)  
[Sat Aug 12 04:05:51 2006] [notice] Apache/1.3.11 (Unix) mod_perl/1.21 configured -- resuming normal operations  
[Thu Jun 22 14:20:55 2006] [notice] Digest: generating secret for digest authentication ...  
[Thu Jun 22 14:20:55 2006] [notice] Digest: done  
[Thu Jun 22 14:20:55 2006] [notice] Apache/2.0.46 (Red Hat) DAV/2 configured -- resuming normal operations  
  
** Restart by HUP signal (optional suEXEC)  
[Sat Aug 12 04:05:49 2006] [notice] SIGHUP received. Attempting to restart  
[Sat Aug 12 04:05:51 2006] [notice] suEXEC mechanism enabled (wrapper: /usr/local/apache/sbin/suexec)  
  
** after 'unclean' shutdown (left over PID file)  
[Sat Jun 24 09:06:22 2006] [warn] pid file /opt/CA/BrightStorARCserve/httpd/logs/httpd.pid overwritten -- Unclean shutdown of previous Apache run?  
[Sat Jun 24 09:06:23 2006] [notice] Apache/2.0.46 (Red Hat) DAV/2 configured -- resuming normal operations  
[Sat Jun 24 09:06:22 2006] [notice] Digest: generating secret for digest authentication ...  
[Sat Jun 24 09:06:22 2006] [notice] Digest: done
```

4.3.3. Phân tích Web log file

IIS là viết tắt của từ Internet Information Services (các dịch vụ cung cấp thông tin Internet), IIS được đính kèm với các phiên bản của Windows. IIS là các dịch vụ dành cho máy chủ chạy trên nền Hệ điều hành Windows nhằm cung cấp và phân tán các thông tin lên mạng, nó bao gồm nhiều dịch vụ khác nhau như Web Server, FTP Server, ... Nó có thể được sử dụng để xuất bản nội dung của các trang Web lên Internet/Intranet bằng việc sử dụng “Phương thức chuyển giao siêu văn bản” – Hypertext Transport Protocol (HTTP).



CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

Kích hoạt IIS Logging

Bạn phải kích hoạt việc ghi log cho mỗi Website, FTP và máy chủ SMTP riêng để thu thập và chuyển đổi dữ liệu sử dụng. Hãy chắc chắn rằng bạn đã chọn Enable Logging trên trang Windows Internet Information Services.

CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

Định dạng IIS Log File

Field Name	Description/Values
Date	The date that the action occurred.
Time	The time that the action occurred.
c-ip (client IP address)	The IP address of the client that accessed the server.
cs-username (user name)	The name of the authenticated user who accessed the server. This does not include anonymous users, which are represented by a hyphen (-).
s-sitename (service name)	The Internet service and instance number that was accessed by the client.
s-computername (server name)	The name of the server on which the log entry was generated.
s-ip (server IP address)	The IP address of the server on which the log entry was generated.
s-port (server port)	The port number the client was connected to.
cs-method (method)	The action the client was trying to perform (for example, a GET method).

CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

cs-uri-stem (URI stem)	The resource accessed (for example, Default.htm).
cs-uri-query (URI query)	The query, if any, the client was trying to perform.
sc-status (protocol status)	The status of the action, in HTTP or FTP terms.
sc-win32-status (protocol status)	The status of the action, in terms used by Windows.
sc-bytes (bytes sent)	The number of bytes sent by the server.
cs-bytes (bytes received)	The number of bytes received by the server.
time-taken	The length of time the action took.
cs-version (protocol version)	The protocol (HTTP, FTP) version used by the client. For HTTP, this will be either HTTP 1.0 or HTTP 1.1.
cs-host (host)	Displays the content of the host header.
cs(User-Agent) (user agent)	The browser used on the client.
cs(Cookie) (cookie)	The content of the cookie sent or received, if

CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

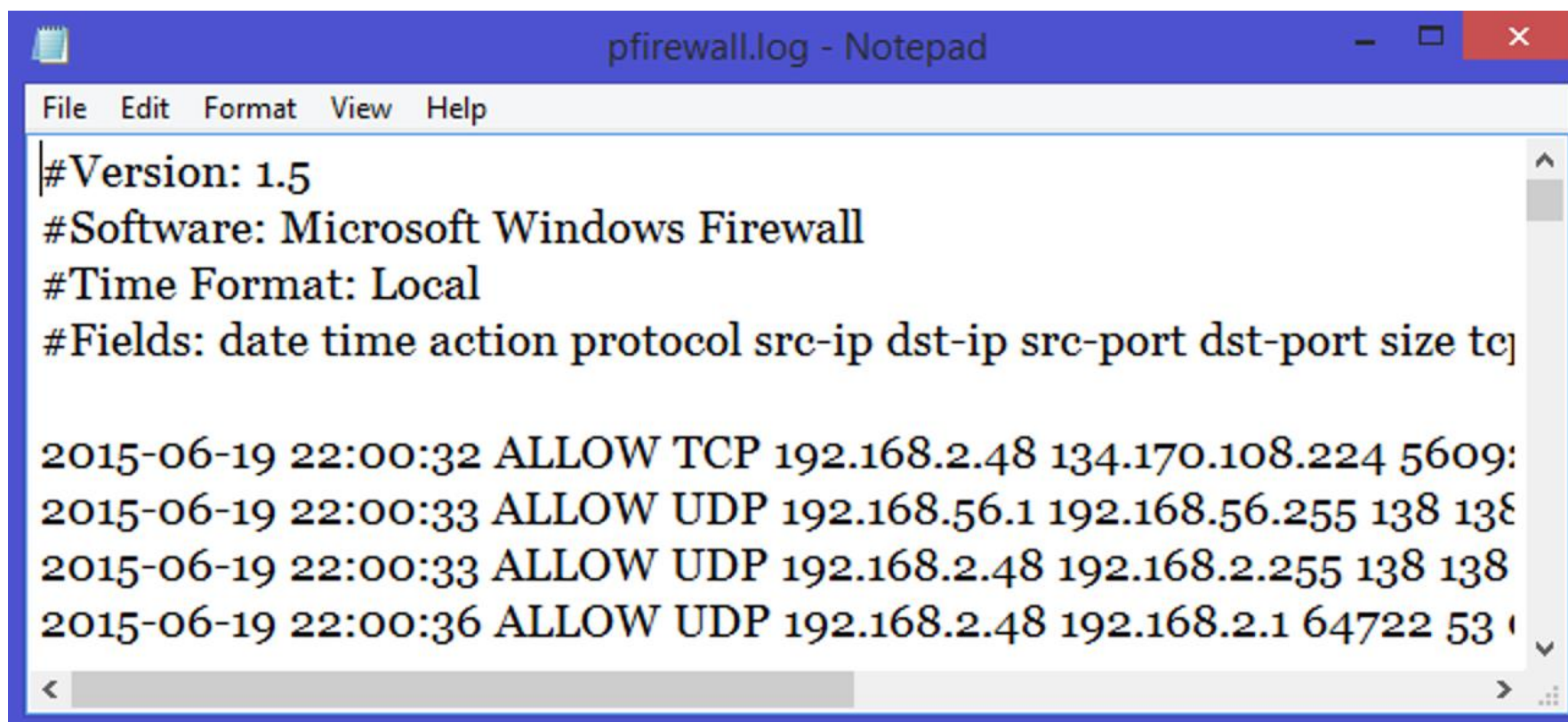
Field Name	Description/Values
	any.
cs(Referrer)	The previous site visited by the user. This site provided a link to the current site.

4.3.4. Phân tích Windows Firewall log file

Việc ghi log chỉ sẵn sàng đối với các thiết bị đã bật Windows Firewall. Tuy nhiên không phải toàn bộ các kết nối đều được ghi log lại, mà chỉ những kết nối được cấu hình bảo vệ bởi Windows Firewall. Tất cả các lưu lượng đi ra gửi đến đích thành công đều không ghi log lại. Ngoài ra, lưu lượng gửi đi mà không bị chặn cũng không được ghi log. Kích thước mặc định của file log trong Windows Firewall là 4.096 kilobyte (KB); kích thước tối đa là 32,767 KB. Khi file log đạt đến kích thước giới hạn mà bạn thiết lập, các file log sẽ được đổi tên và một file log mới được tạo ra.

CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

Ví dụ: Windows firewall log file



```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size total-bytes

2015-06-19 22:00:32 ALLOW TCP 192.168.2.48 134.170.108.224 5609:80
2015-06-19 22:00:33 ALLOW UDP 192.168.56.1 192.168.56.255 138 138
2015-06-19 22:00:33 ALLOW UDP 192.168.2.48 192.168.2.255 138 138
2015-06-19 22:00:36 ALLOW UDP 192.168.2.48 192.168.2.1 64722 53
```

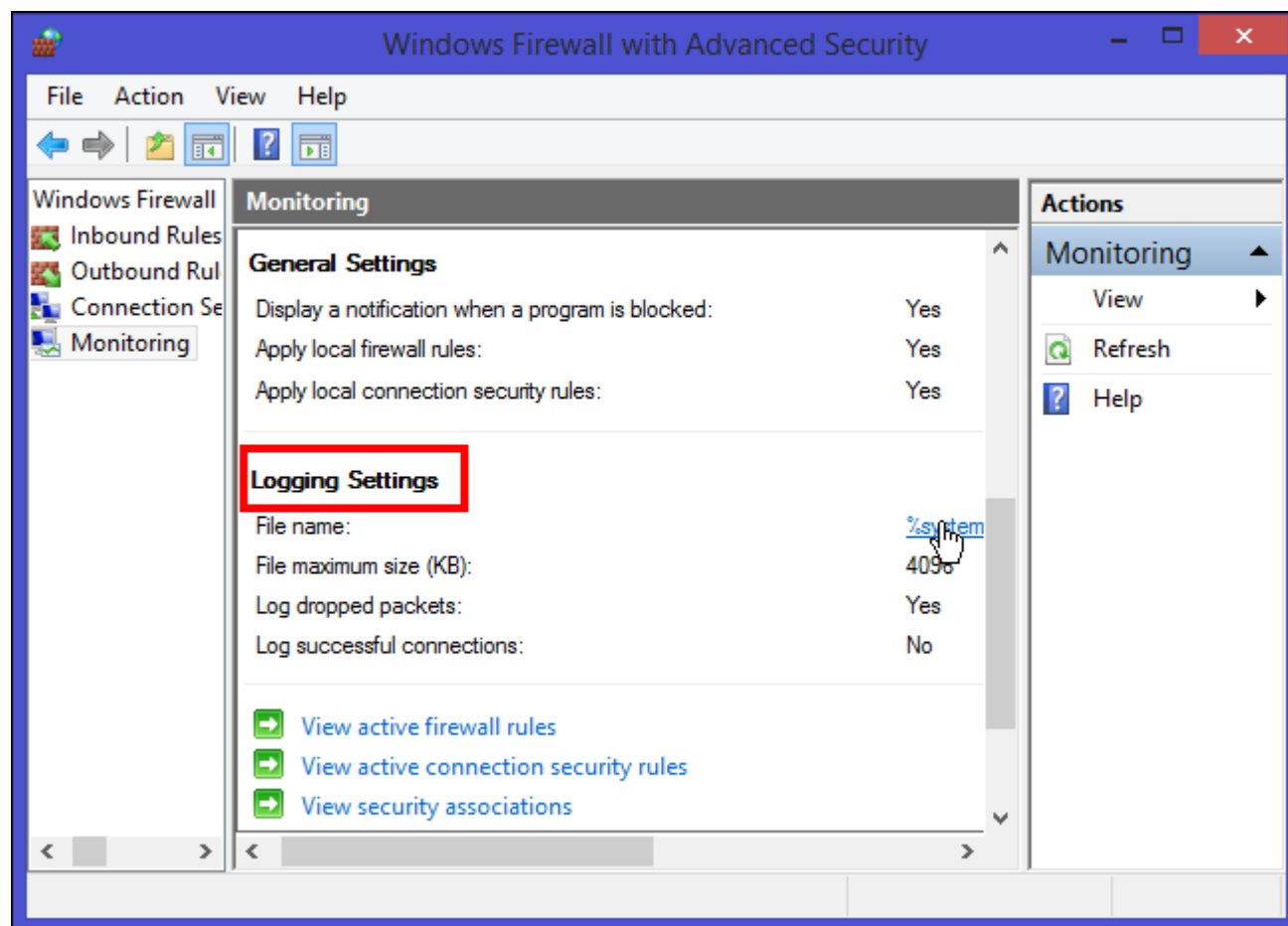
CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

Ví dụ: Windows firewall log file



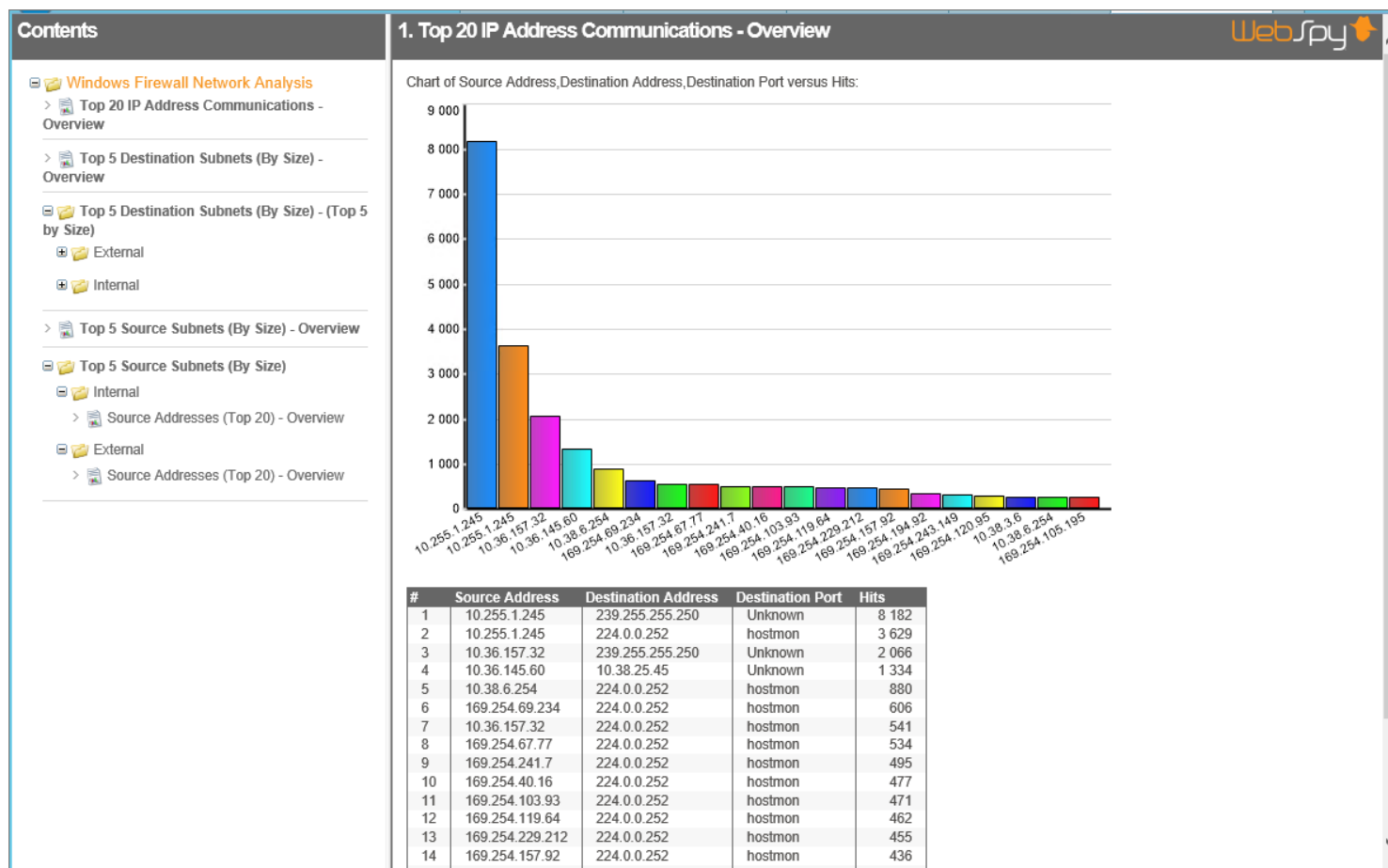
CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

Ví dụ: Windows firewall log file



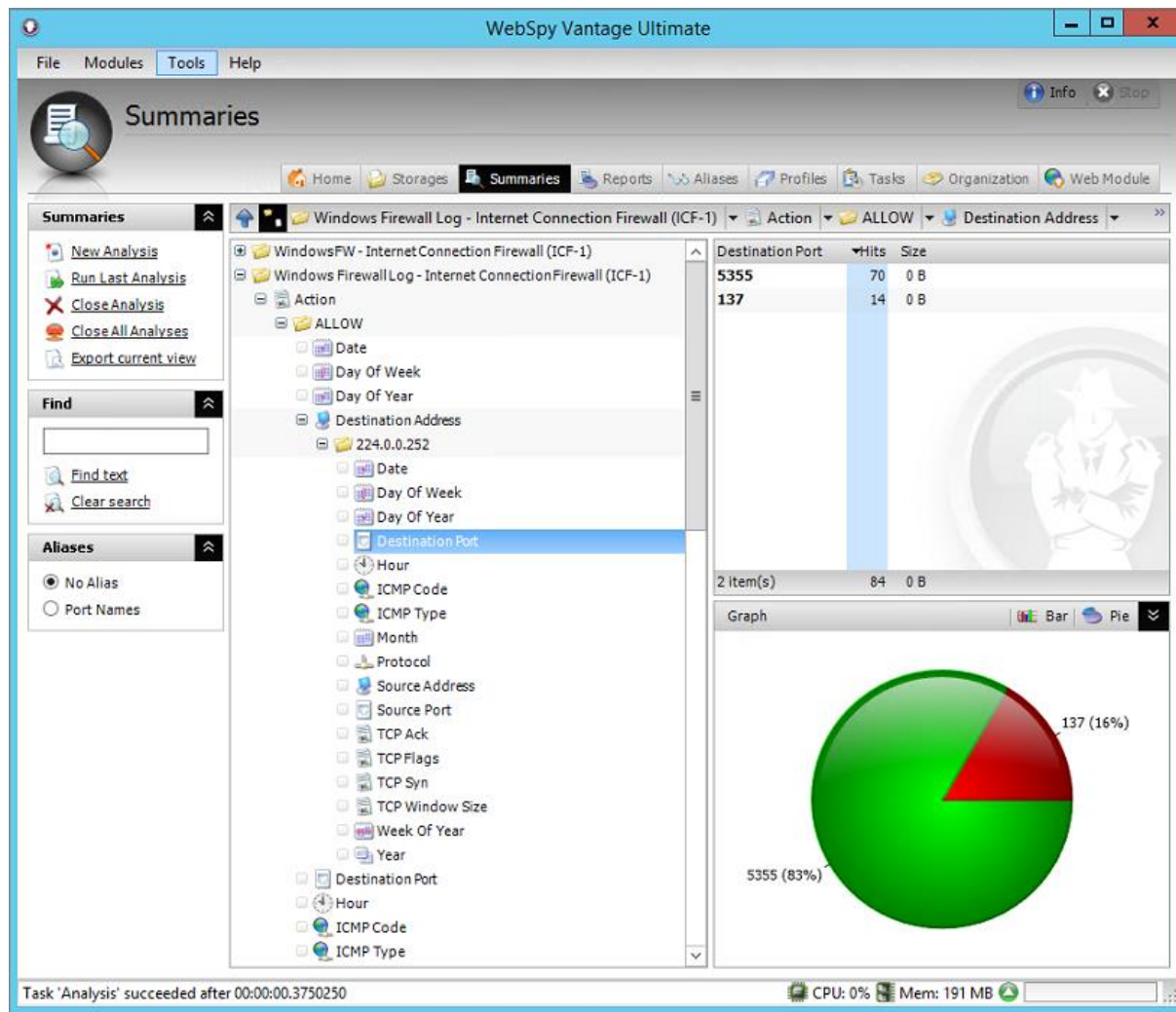
CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

Ví dụ: Windows firewall log file



CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

*Ví dụ: Windows
firewall log file*



CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

Ví dụ: Firewall log file Sophos

Firewall

Name	Description	Log file	Service
BWM	Bandwidth management service (QoS)	bwm.log	bwm
Firewall rule logging.	Firewall rule logging service	firewall_rule.log	
Firewall	Virtual host service	vhost.log	
FWlog	Firewall logging service	fwlog.log	fwlog
NAT	NAT rule log files	nat_rule.log	
NAT	NAT rule log files	pimd.log	pimd
Pktcap	Packet capture service (GUI DG option)	pktpd.log	pktpd

CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

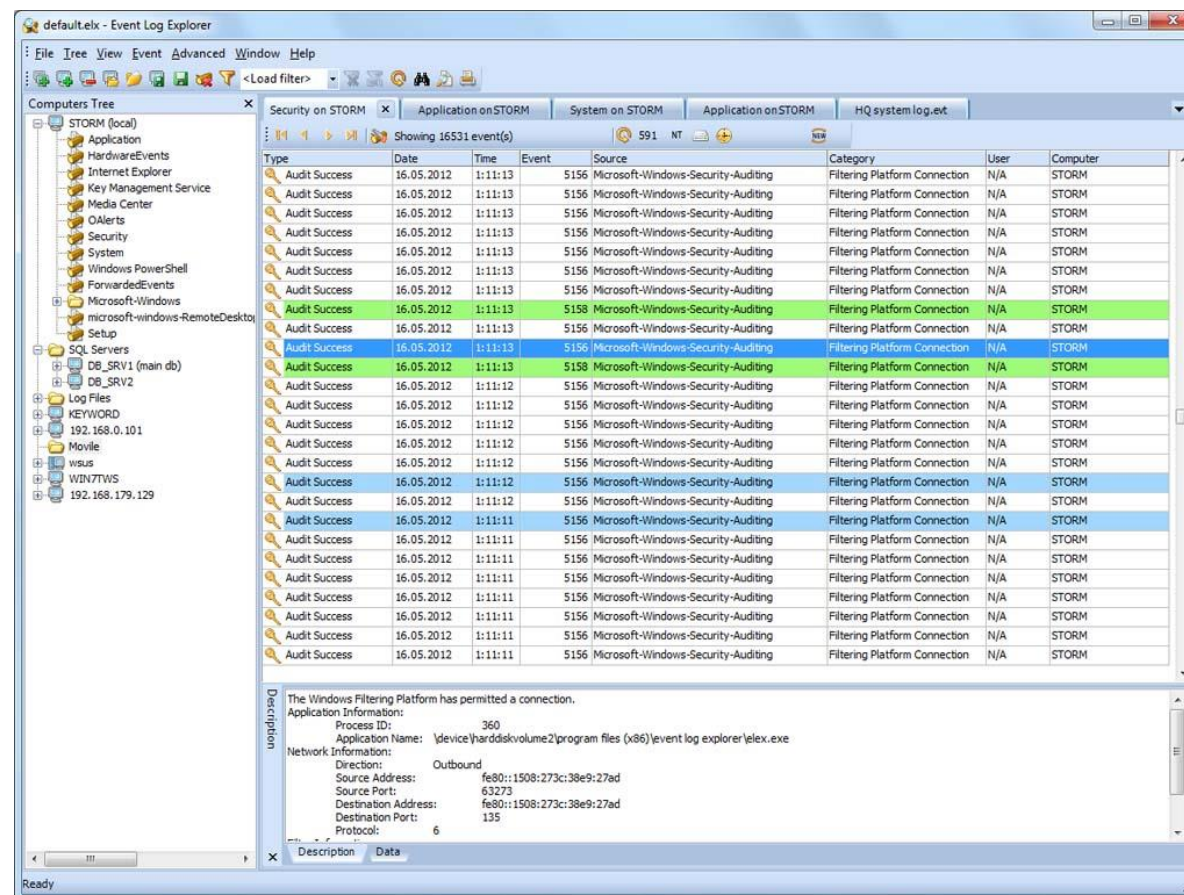
```

pfirewall - Notepad
File Edit Format View Help
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path

2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63064 135 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.14 63065 49156 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63066 65386 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63067 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.14 62292 389 0 - - - - - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63068 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63069 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.13 62293 389 0 - - - - - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63070 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63071 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63072 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63073 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63074 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63075 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63076 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 55053 53 0 - - - - - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 50845 53 0 - - - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP fe80::29ea:1a3c:24d6:fb49 ff02::1:3 57333 5355 0 - - - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP 10.40.4.252 224.0.0.252 59629 5355 0 - - - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 58846 5355 0 - - - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP 10.40.4.182 224.0.0.252 58846 5355 0 - - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 137 137 0 - - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 63504 5355 0 - - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 63504 5355 0 - - - - - - - SEND

```

Event Log Explorer



4.3.5. Một số công cụ phân tích log file

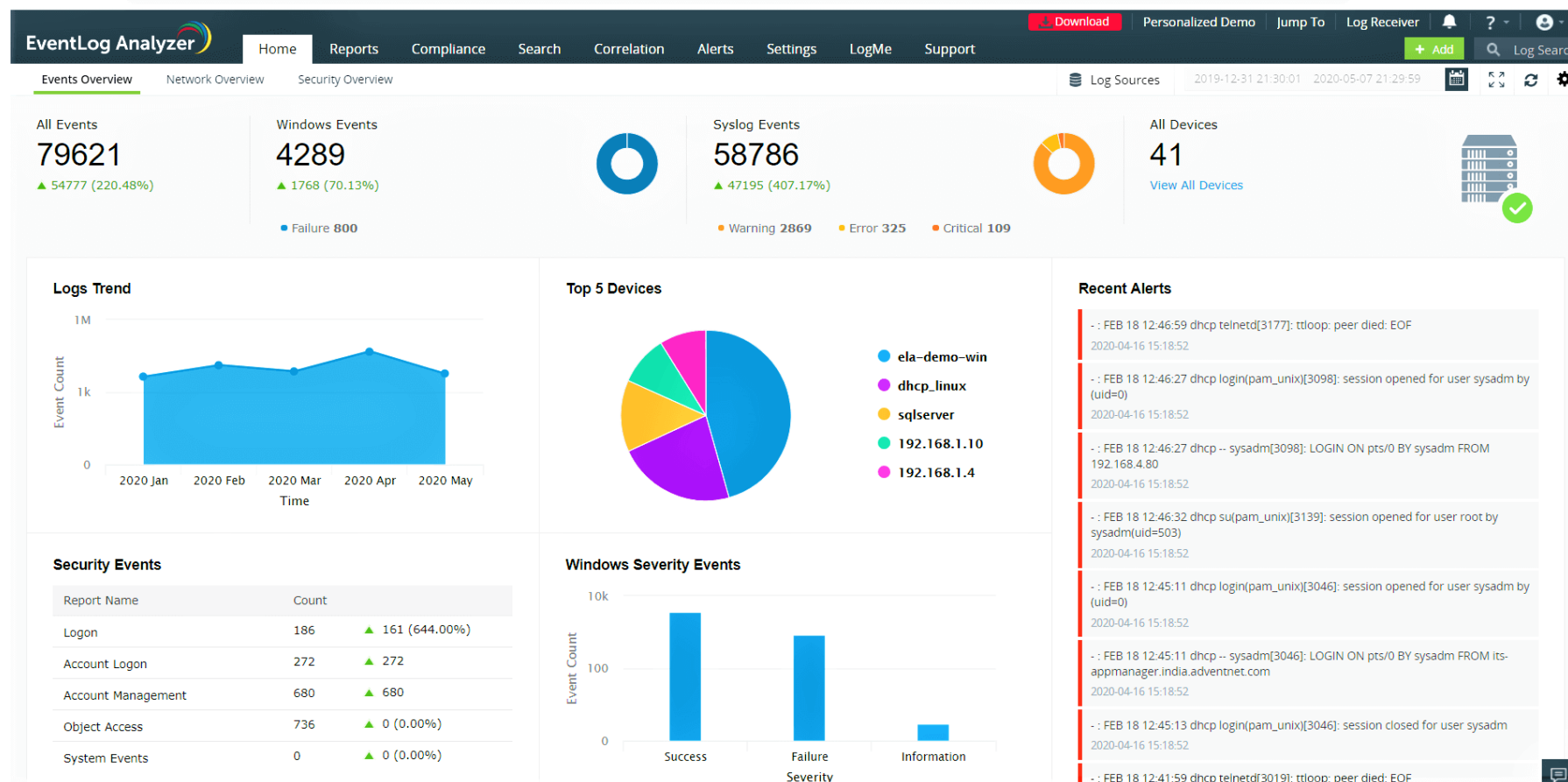
Event Log Explorer

Công cụ miễn phí, Event Log Explorer, có thể thay thế cho Windows Event Viewer. Event Log Explorer hiển thị số lượng thông tin như Event Viewer, nhưng ngoài ra nó còn cho phép tra cứu nhanh các Event ID trên Internet. Chỉ cần kích phải vào một sự kiện, bạn sẽ có thể tra cứu Event ID trong cơ sở dữ liệu EventID.Net hoặc trong Microsoft KnowledgeBase



CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

ManageEngine EventLog Analyzer





CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

ManageEngine EventLog Analyzer

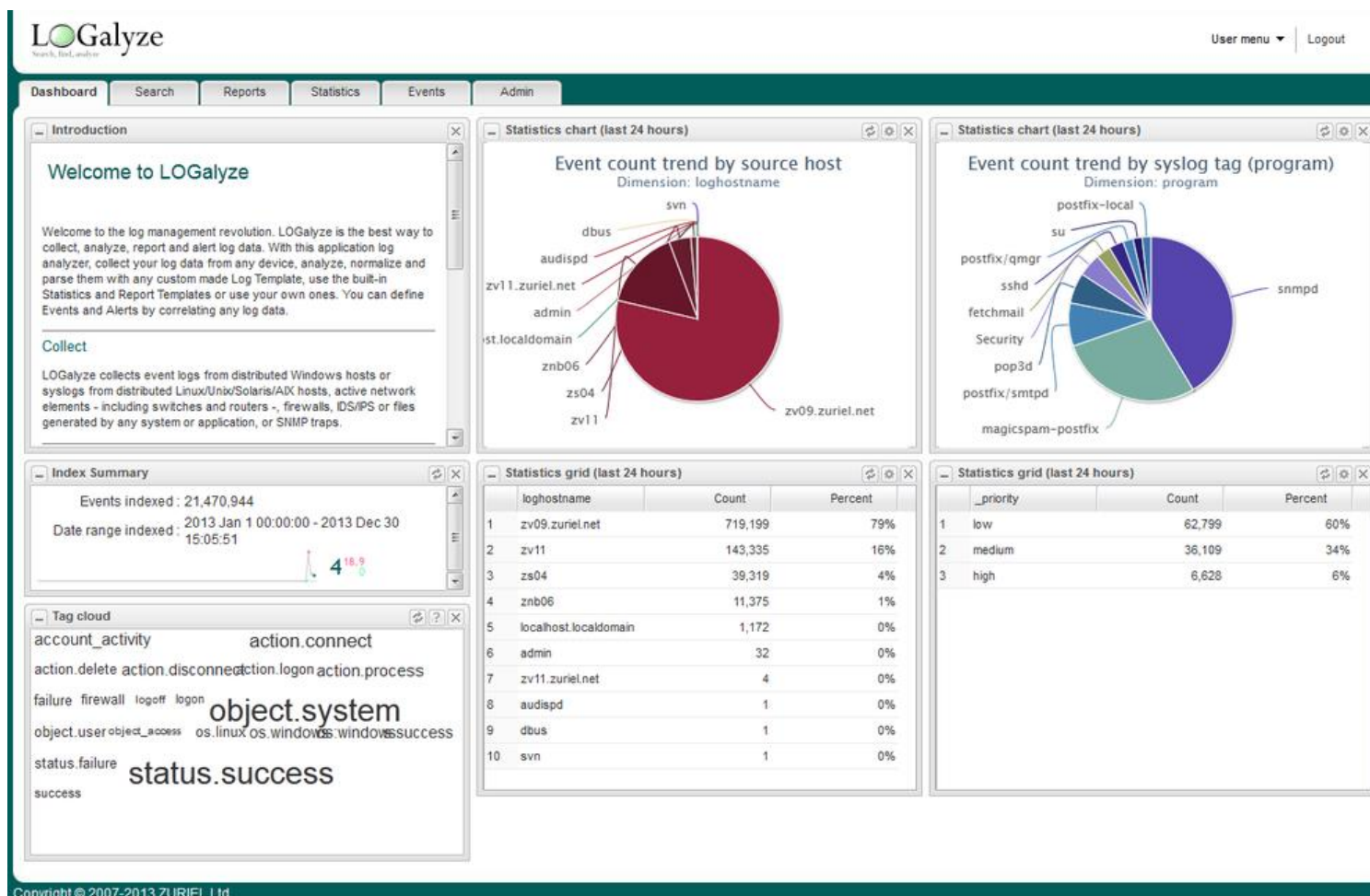
ManageEngine EventLog Analyzer thu thập dữ liệu từ các nguồn khác nhau và lưu chúng trong một kho lưu trữ tập trung. Dữ liệu lưu trữ này được đóng dấu thời gian và hash để đảm bảo rằng các bản ghi không bị giả mạo.

EventLog Analyzer có ba phiên bản: Free, Premium và Distributed. Phiên bản Free (miễn phí) hỗ trợ tối đa 5 nguồn log, phiên bản Premium (cao cấp) hỗ trợ 10 đến 100 nguồn log và bản Distributed hỗ trợ số lượng nguồn log không giới hạn



LOGalyze

CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE





CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

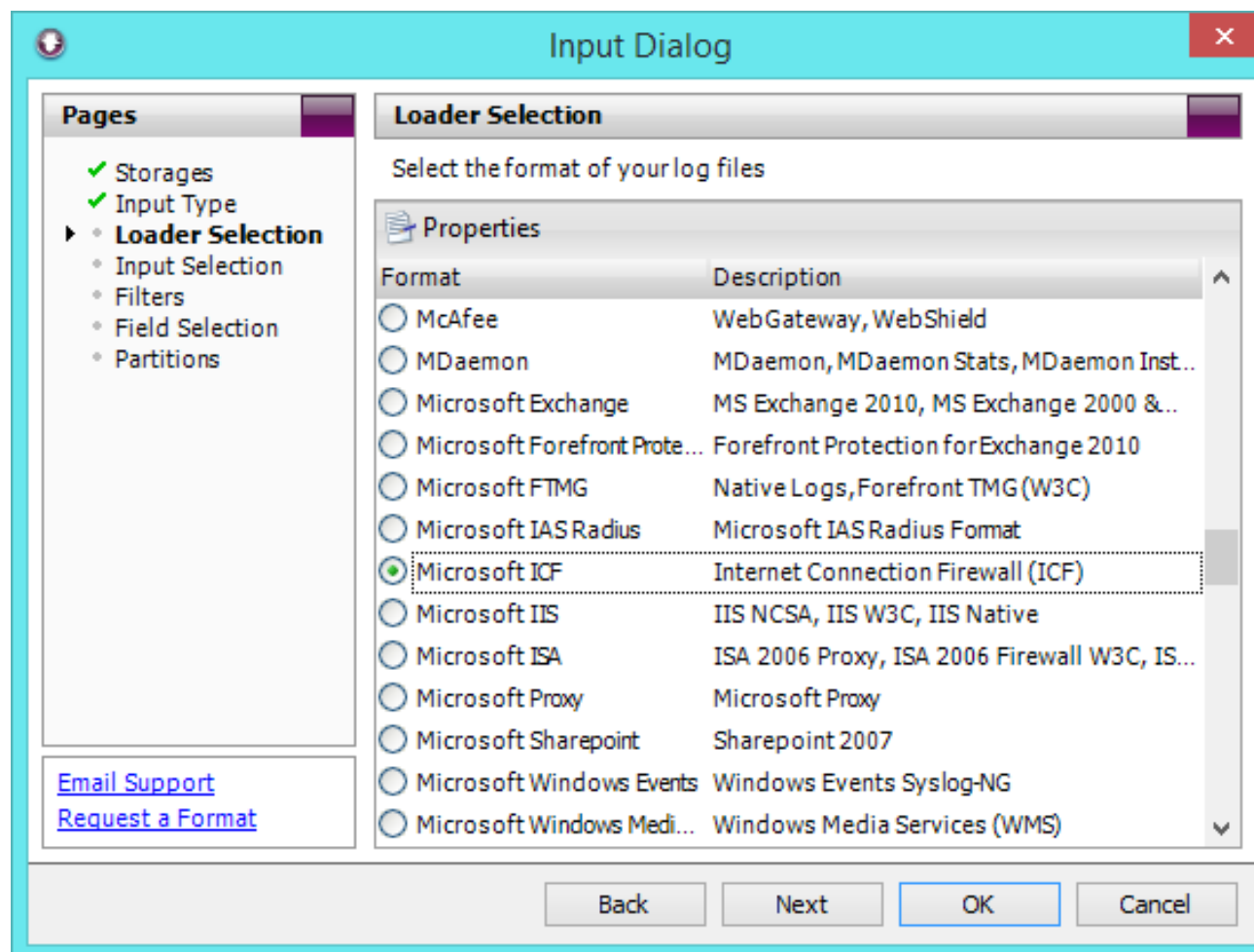
LOGalyze

LOGalyze là một phần mềm phân tích log mã nguồn mở, hỗ trợ cho UNIX, Linux, Windows và các hệ điều hành khác. Phần mềm này thu thập dữ liệu, phân tích để xác định nguồn, mức độ nghiêm trọng, loại dữ liệu và lưu trữ chúng trong kho lưu trữ. Nó phân tích dữ liệu và cung cấp các cảnh báo và đưa ra các báo cáo về việc tuân thủ nguyên tắc.

CHƯƠNG 4. PHÂN TÍCH CÁC LOG FILE

WebSpy Vantage

Phần mềm cho phép phân tích log file mạnh mẽ và có thể được sử dụng cho nhiều mục đích hơn là chỉ báo cáo việc sử dụng web trên Internet.





CÁC KHÁI NIỆM CƠ BẢN VỀ QUẢN TRỊ MẠNG

Q & A