WEBSERVER LOGS

Trình bày: Nguyễn Xuân Việt – FPT CIO

NỘI DUNG CHÍNH

01 Kiến trúc WebServer

02 Phân loại, định dạng Log Webserver

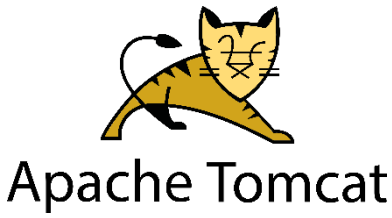
03 Các công cụ, các tool điều tra Webserver

04 Các ví dụ về log Webserver

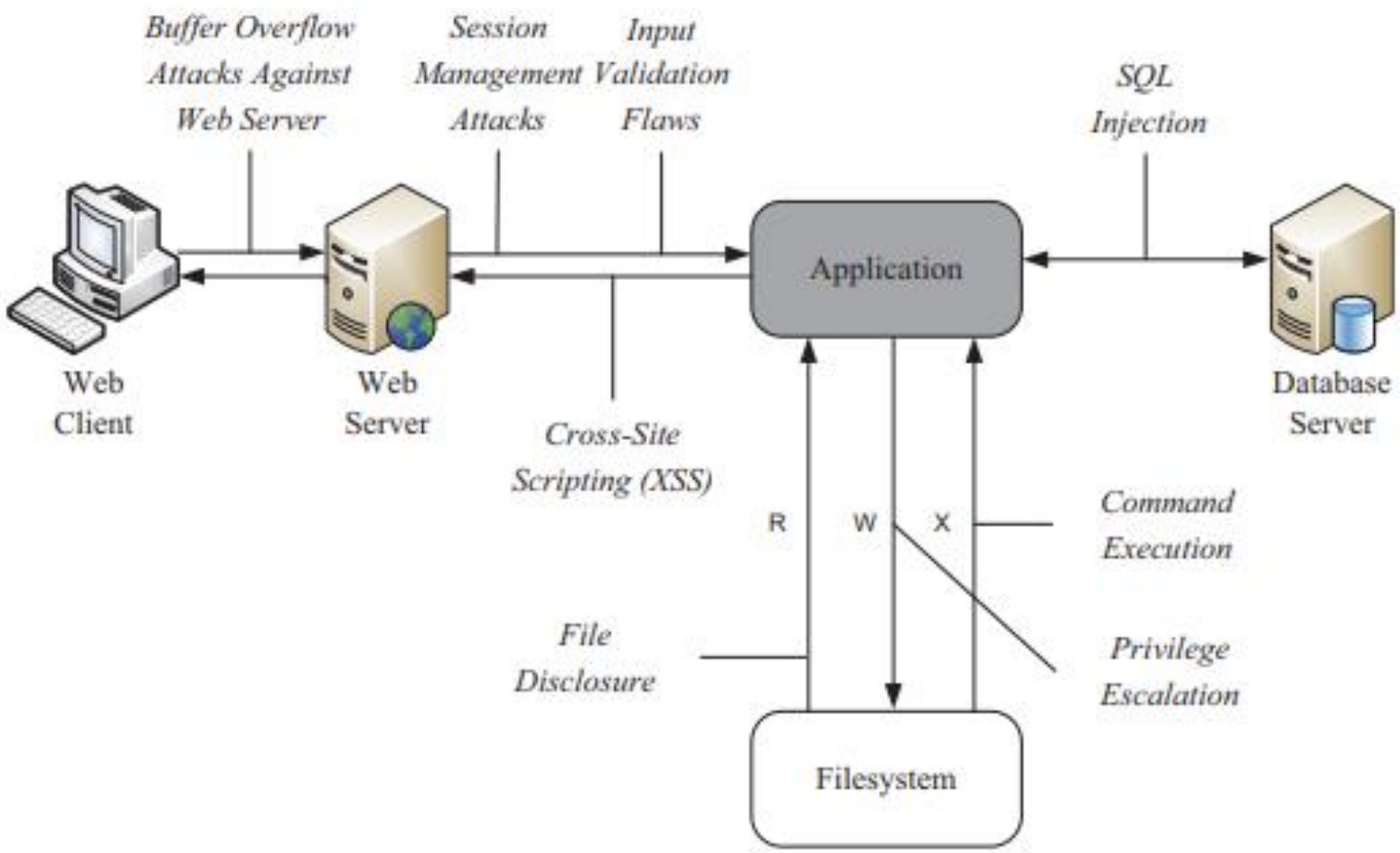
CÁC WEBSEVER PHỔ BIẾN

Các Webserver phổ biến như:

- IIS
- Apache
- Apache Tomcat
- Nginx



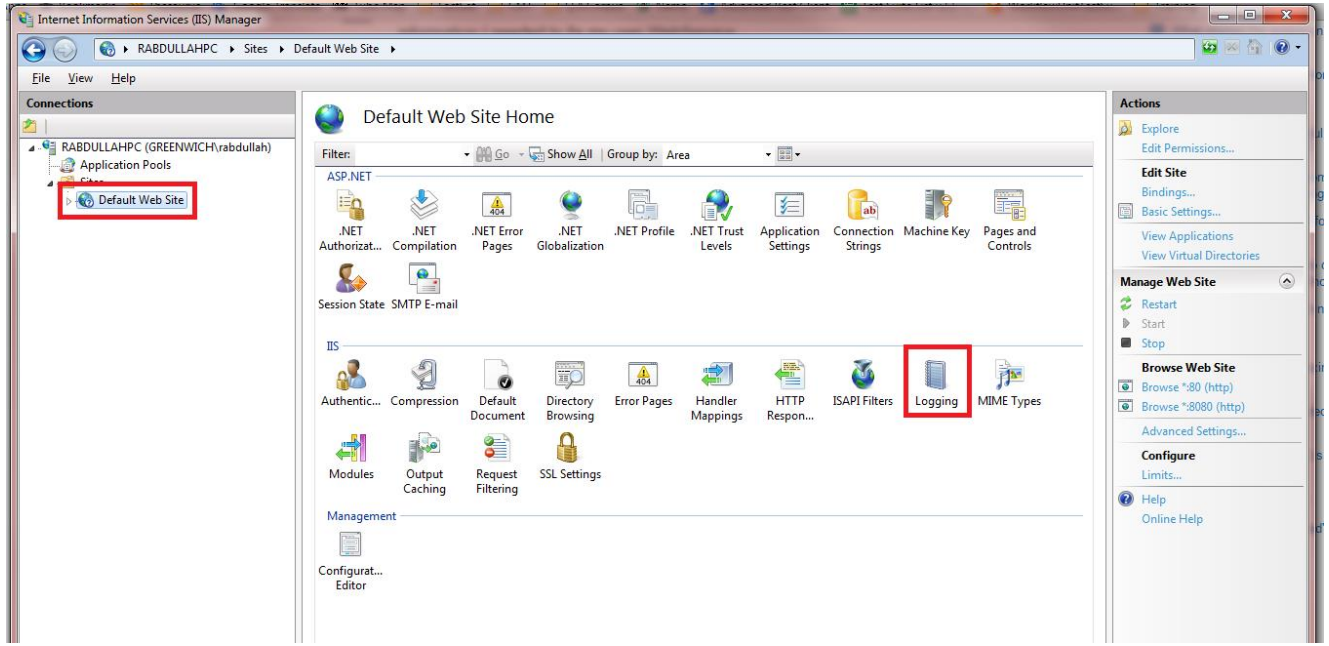
KIẾN TRÚC WEBSEVER



PHÂN LOẠI LOG WEBSERVER

Đường dẫn lưu trữ log được quy định ở các file cấu hình

- **Ở IIS:** Vào Site → Chọn Logging → Open (File log thường được cấu hình sang Disk khác Disk C)
- **Ở Nginx, Apache**: Truy cập vào file conf thường nằm trong thư mục ***/etc/nginx/conf.d*** và ***/etc/httpd/conf.d*** để kiểm tra nơi lưu trữ log (File log thường được lưu trữ tại đường dẫn ***/var/log/nginx*** hoặc /***var/log/httpd***)



PHÂN LOẠI LOG WEBSERVER

Log webserver thông thường phân thành 2 loại log chính:

1. **Access log**: Ghi nhận các thông tin truy cập đến Webserver và phản hồi từ Webserver đối với các truy cập đó
2. **Error log:** Ghi nhận các thông tin lỗi liên quan đến cấu hình, hoạt động không đúng từ bản thân Webserver

ĐỊNH DẠNG LOG WEBSERVER

Access log

- log_format main '$remote_addr - $remote_user [$time_local] "$request" ' '$status $body_bytes_sent "$http_referer" ' '"$http_user_agent" "$http_x_forwarded_for"';
- Main: tên gọi của log format, có thể tạo nhiều định dạng log khác nhau và gán với tên log format để đưa vào file cấu hình
- $remote_addr: địa chỉ IP gửi request
- $remote_user: tài khoản truy cập nếu có xác thực người dùng
- $time_local: Thời gian gửi request đến
- $request: Info của request bao gồm các thông tin như Method (GET, POST, PUT…), URI truy cập, HTTP version,…
- $status: trạng thái của response
- $body_bytes_sent: kích thước body mà server response
- $http_user_agent: thông tin trình duyệt, hệ điều hành mà người dùng truy cập
- $http_x_forwarded_for: Xác định người dùng truy cập qua proxy

Error log

- Error_log log_file log_level
- Các mức log_level bao gồm: emerg, alert, crit, error, warn, notice, info, debug

CÔNG CỤ KIỂM TRA LOG WEBSERVER

Một số công cụ kiểm tra Log Webserver:

- Đối với **IIS**: Sử dụng Notepad, noted++, wordpad….
- Đối với **Nginx, Apache, Apache Tomcat** sử dụng:
  - ✓ *Vi or vim*
  - ✓ *Tail*
  - ✓ *Cat*
  - ✓ *Nano*

CÁC TOOL ĐIỀU TRA WEBSERVER

	Tools	Descriptions										
		Standards Compliance	Performs Correlation	Correlation Data Source	Admissibility†	Multiple Platform	Useability	Reporting	Scalability	Real-Time	Compression	Generation of Alerts
Application Specific	Psacct	N	N	Y	-	Y [i]	CL	-	Y	Y	N	Y [b]
	Acctsum	N	N	N	-	Y [i]	CL	Y [H]	Y	N [c]	N [t]	N
	Analog	N	N	N	-	Y [ii]	CL	Y [H,e]	Y	N [c]	N	N
	Anteater	N	N	N	-	Y [iii]	CL	Y [H,e]	N	N	N	N
	Awstats	N	N	N	-	Y [iv]	B	Y [S,P,H]	N	Y [f]	N	N
	Breadboard Bi Web Analytics	N	N	N [v,h]	-	Y [iv]	B	Y [P,H,X,R]	Y	Y	N	N
	Calamaris	N	N	Y	-	Y [i]	CL	Y [H]	Y	N [c]	N	N
	Chklogs	N	N [a]	N	-	Y [i]	CL	N	N	N [c]	Y [rt]	N
	CORE Wisdom	N	N [j]	N	-	N [v]	EUI	Y [g]	Y	Y	N	N
	Eventlog Analyzer	Y	Y [SF]	N	-	Y [iv]	B	Y [H,P,C]	Y	Y	N	N
	Ftpweblog & Wwwstat	N	N	N	-	Y [i]	CL	Y [H]	Y	N [c]	N	N
	Funnel Web® Analyzer	Y	N	N	-	Y [ii]	CL	Y [P,H,E,R,W]	Y [$]	Y [$]	N	N
	HTTP-Analyze	N	Y [SF]	N	-	Y [iii]	CL	Y [H]	N	N [c]	Y [rt]	N

Continued . . .

CÁC TOOL ĐIỀU TRA WEBSERVER

	Tools	Descriptions										
		Standards Compliance	Performs Correlation	Correlation Data Source	Admissibility†	Multiple Platform	Useability	Reporting	Scalability	Real-Time	Compression	Generation of Alerts
Application Specific	logjam	Y	N	Y	-	N [v]	B	Y [H]	N	N	N	N
	Logparser	Y	N [a]	N	-	N [v]	N[EXT]	Y [*]	Y	N	N	N
	Lire	Y	N	N	-	Y [1]	CL	Y[H,X]	Y	N	N	Y
	Logrep	Y	N	N	-	Y [ii]	CL	Y [H]	Y	Y	N [xs]	N
	Logstalgia	N	N	N	-	Y [ii]	EUI[g]	N	Y	Y [c]	N	N
	Logsurfer	N	Y	Y	-	Y [i]	CL	Y	Y	Y	N	Y
	Swatch	N	Y	Y	-	Y [i]	CL	N	Y	Y	N	Y
	Tenshii	N	N [a]	Y	-	Y [i]	CL	Y [C]	Y	Y	N	Y
	Mywebalizer	N	N	Y	-	Y [ii]	CL	Y [H]	Y	N	Y	N
	Open Web Analytics	N	N	N	-	Y [ii]	B	Y [H]	Y	Y	N	N
	Pyflag	Y	N [a]	Y	-	Y [ii]	B	Y [H]	Y	N	N	N
	Sawmill	Y	N [a]	Y	-	Y [ii]	B	Y [H]	Y	Y	Y [xs]	N
	Squidj	N	N	Y	-	Y [i]	CL	Y [S]	Y	N [c]	N	Y
	Scansquidlog	N	N	Y	-	Y [i]	CL	Y [S]	Y	N [c]	N	N
	Visitors	N	N	Y	-	Y [ii]	CL	Y [H]	Y	N	N	N
	Weblogmon	N	N	Y	-	Y [iii]	CL	N [F]	Y	Y	N [xs]	Y

Continued . . .

CÁC TOOL ĐIỀU TRA WEBSERVER

	Tools	Descriptions										
		Standards Compliance	Performs Correlation	Correlation Data Source	Admissibility†	Multiple Platform	Useability	Reporting	Scalability	Real-Time	Compression	Generation of Alerts
Development Tools	ApacheDB	Y	N [a]	N	-	Y [ii]	D	D	Y	D	N	D
	Mod_log_SQL	Y	N	Y	-	Y [ii]	D	D	Y	D	N	D
	Cascade Software	Y	N [a]	N	-	Y [ii]	D	Q	Y	Y	N	Y
	Crystal Reports	Y	N [a]	N	-	N [v]	EUI	Q	Y	Y	D	D
	JasperReports	N	N [a]	N	-	Y [iii]	EUI	Q	Y	Y	D	D
	SEC	N	Y [a]	N	-	Y [iii]	CL	D	Y	N [c]	N	D
IDS and HIMS	ArcSight Logger and ESM	Y	Y [a]	Y	-	N [A]	B	Y [r,g]	Y	Y	Y	Y
	Guard26	N	N	Y	-	Y [i]	CL	N	N	Y	N	Y [b]
	Osiris	Y	N [j]	Y	-	Y [ii]	CL/B	N	Y	Y	N	Y [b]
	Samhain	Y	N [j]	Y	-	N [vii]	CL	N	Y	Y	N	Y [b]
	OSSEC	N	N [a,j]	Y	-	Y [ii]	CL	N	Y	Y	N [xs]	Y [b]
	Snort	N	N	Y	-	Y [ii]	CL	Y [uf]	Y	Y	N	Y
	Splunk	N	N [a,j]	Y	-	Y [ii]	CL/B	Y	Y	Y	D	Y

VÍ DỤ VỀ WEBSEVER LOG

Kiểm tra log access Nginx: Log Access Nginx thường được cấu hình tại đường dẫn **/var/log/nginx/access.log**

- *Các thông tin có thể xem gồm: IP nào truy cập? Thời gian truy cập? Method truy cập? Truy cập vào URI nào? Truy cập bằng trình duyệt nào? Mã server trả về là thành công hay không?...*

```
[root@                ]# cat itop.access.log-20201118
10.4.32.254 - - [17/Nov/2020:11:26:11 +0700] "GET / HTTP/1.1" 403 2020 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36" "itop.ho.fpt.
vn" sn="itop.ho.fpt.vn" rt=0.004 ua="10.1.11.51:80" us="403" ut="0.004" ul="4897" "-"
10.4.32.254 - - [17/Nov/2020:11:26:11 +0700] "GET /noindex/css/bootstrap.min.css HTTP/1.1" 200 4771 "http://itop.ho.fpt.vn/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0) AppleWebKit/537.36 (KHTML, like Gecko)
 Chrome/86.0.4240.193 Safari/537.36" "itop.ho.fpt.vn" sn="itop.ho.fpt.vn" rt=0.004 ua="10.1.11.51:80" us="200" ut="0.004" ul="19341" "-"
10.4.32.254 - - [17/Nov/2020:11:26:12 +0700] "GET /noindex/css/fonts/Bold/OpenSans-Bold.woff HTTP/1.1" 404 211 "http://itop.ho.fpt.vn/noindex/css/open-sans.css" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0) Ap
pleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36" "itop.ho.fpt.vn" sn="itop.ho.fpt.vn" rt=0.003 ua="10.1.11.51:80" us="404" ut="0.003" ul="239" "-"
10.4.32.254 - - [17/Nov/2020:11:26:12 +0700] "GET /noindex/css/fonts/Light/OpenSans-Light.woff HTTP/1.1" 404 212 "http://itop.ho.fpt.vn/noindex/css/open-sans.css" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36" "itop.ho.fpt.vn" sn="itop.ho.fpt.vn" rt=0.003 ua="10.1.11.51:80" us="404" ut="0.003" ul="241" "-"
10.4.32.254 - - [17/Nov/2020:11:26:12 +0700] "GET /noindex/css/fonts/Bold/OpenSans-Bold.ttf HTTP/1.1" 404 210 "http://itop.ho.fpt.vn/noindex/css/open-sans.css" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0) App
leWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36" "itop.ho.fpt.vn" sn="itop.ho.fpt.vn" rt=0.003 ua="10.1.11.51:80" us="404" ut="0.003" ul="238" "-"
10.4.32.254 - - [17/Nov/2020:11:26:12 +0700] "GET /noindex/css/fonts/Light/OpenSans-Light.ttf HTTP/1.1" 404 211 "http://itop.ho.fpt.vn/noindex/css/open-sans.css" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0) A
ppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36" "itop.ho.fpt.vn" sn="itop.ho.fpt.vn" rt=0.003 ua="10.1.11.51:80" us="404" ut="0.003" ul="240" "-"
10.4.32.254 - - [17/Nov/2020:11:26:13 +0700] "GET /favicon.ico HTTP/1.1" 404 194 "http://itop.ho.fpt.vn/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.1
93 Safari/537.36" "itop.ho.fpt.vn" sn="itop.ho.fpt.vn" rt=0.003 ua="10.1.11.51:80" us="404" ut="0.001" ul="209" "-"
10.4.32.254 - - [17/Nov/2020:11:26:19 +0700] "GET /itop HTTP/1.1" 301 235 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36" "itop.ho.f
pt.vn" sn="itop.ho.fpt.vn" rt=0.004 ua="10.1.11.51:80" us="301" ut="0.002" ul="235" "-"
10.4.32.254 - - [17/Nov/2020:11:26:19 +0700] "GET /itop/ HTTP/1.1" 302 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36" "itop.ho.fp
t.vn" sn="itop.ho.fpt.vn" rt=0.005 ua="10.1.11.51:80" us="302" ut="0.004" ul="0" "-"
10.4.32.254 - - [17/Nov/2020:11:26:19 +0700] "GET /itop/pages/UI.php HTTP/1.1" 200 1824 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.
36" "itop.ho.fpt.vn" sn="itop.ho.fpt.vn" rt=0.317 ua="10.1.11.51:80" us="200" ut="0.317" ul="5758" "-"
```

VÍ DỤ VỀ WEBSEVER LOG

Kiểm tra log Error Nginx: Log Error Nginx thường được cấu hình tại đường dẫn **/var/log/nginx/error.log**

- *Ta có thể biết đường thông tin lỗi từ thời gian nào? IP nào truy cập bị lỗi? Method truy cập? Lý do lỗi.*
- *Ví dụ bên dưới là từ IP 10.4.32.202 truy cập đến upstream 10.1.11.51 port 80 tại thời điểm 11:16:37 ngày 11/12/2020 bị lỗi. Lí do không có kết nối tới host.*
- *Với các thông tin trên ta sẽ kiểm tra kết nối về mặt network, kiểm tra cấu hình upstream*

```
[root@                    # cat itop.error.log-20201113
2020/11/12 11:16:37 [error] 22618#22618: *25548639 connect() failed (113: No route to host) while connecting to upstream, client: 10.4.32.202, server: itop.ho.fpt.vn, request: "GET / HTTP/1.1", upstream: "http://10.1.11.51:80/", host: "itop.ho.fpt.vn"
```

Thank You !