عنوان: **آشنایی با ساختار IIS قسمت دوازدهم**
نویسنده: علی یگانه مقدم
تاریخ: ۱۳۹۳/۱۱/۲۰ ۱۲:۰
آدرس: www.dotnettips.info
گروه‌ها: ASP.Net, IIS, log, Logfile, LogParser

پیکربندی قسمت لاگ‌ها، میتواند برای یک سرور و یا وب سایت خاص از طریق فایل کانفیگ یا از طریق خود IIS انجام گیرد. برای اینکه به بیشتر این قابلیت‌ها در IIS دسترسی داشت، باید یکی از نسخه‌های ویندوز سرور 2012 و ویندوز 8 را نصب کرده باشید.
لاگ‌ها به ثبت خطاها و درخواست‌های HTTP می‌پردازند و با تحلیل آن‌ها میتوان عملیات بهینه سازی را بر روی سرو اجرا کرد.
تمامی ثبت لاگ‌ها توسط Http.sys انجام می‌گیرد.

نحوه‌ی ذخیره سازی لاگها

در این بخش نحوه‌ی ذخیره سازی و فرمت ذخیره‌ی لاگ‌ها را در دو سطح سایت و سرور به طور جداگانه بررسی می‌کنیم. در IIS ماژول Logging را باز کنید و در لیست One log file per می‌توانید مشخص کنید که لاگ‌ها در چه سطحی اجرا شوند. اگر گزینه‌ی server باشد، تمامی خطاها و درخواست‌های رسیده به سرور در یک فایل لاگ ثبت می‌شوند. ولی اگر سطح سایت باشد، برای هر سایت بر روی IIS لاگ‌ها، جداگانه بررسی می‌شوند. به طور پیش فرض سطح سایت انتخاب شده است.

سطح سایت

موقعی‌که در لیست، سایت را انتخاب کنید، در لیست format می‌توانید تعیین کنید که لاگ‌ها به چه صورتی باید ذخیره شوند.
مواردی که در این حالت لیست می‌شوند گزینه‌های W3C,IIS,NCSA,Custom می‌باشند که در زیر یکایک آن‌ها را بررسی می‌کنیم:

فرمت IIS: این فرمت توسط مایکروسافت ارائه شده و در این حالت لاگ‌های همه‌ی وب سایت‌ها ذخیره می‌شوند. به این فرمت Fixed ASCII Based Text نیز می‌گویند؛ چرا که اجازه‌ی خصوصی سازی ندارد و نمی‌توانید بگویید چه فیلدهایی در لاگ قرار داشته باشند. لاگ فایل‌های این فرمت با ، (کاما) از هم جدا می‌شوند و مقدار زمانی که برای هر فیلد ثبت می‌شود، به صورت محلی local Time می‌باشد.
فیلدهایی که در لاگ این نوع فرمت خواهند آمد، به شرح زیر است:

Client IP address

User name

Date

Time

Service and instance

Server name

Server IP address

Time taken

Client bytes sent

Server bytes sent

Service status code (A value of 200 indicates that the request was fulfilled successfully)

.Windows status code (A value of 0 indicates that the request was fulfilled successfully)

Request type

Target of operation

Parameters (the parameters that are passed to a script)

احتمال این وجود دارد که بعضی از فیلدها در بعضی رکوردها، شامل اطلاعاتی نباشند که به جای مقدار آن علامت - ثبت می‌گردد و برای کاراکترهایی که قابل نمایش نیستند یا کاراکتر نمایشی ندارند، از علامت + استفاده می‌شود. دلیل اینکار هم این است که ممکن است یک کاربر مهاجم، به ارسال اطلاعات کلیدهای کنترلی چون Carriage return اختصارا CR یا Line Feed به اختصار LF کند، که باعث شکسته شدن خط لاگ فایل می‌شود و در نتیجه از استاندارد خارج خواهد شد و هنگام خواندن آن هم با خطا روبرو می‌شویم؛ در نتیجه با جایگزینی چنین کاراکترهایی با + از این اتفاق جلوگیری می‌شود.
شکل زیر نمونه ای از یک خط لاگ در این فرمت است:

```
192.168.114.201, -, 03/20/01, 7:55:20, W3SVC2, SERVER, 172.21.13.45, 4502, 163, 3223, 200, 0, GET, /DeptLogo.gif, -,
```

نام فیلد	نوع حالت مقداردهی	توضیح اتفاقات افتاده
Client IP address	192.168.114.201	آی پی کلاینت
User name	-	کاربر ناشناس است
Date	03/20/01	تاریخ فعالیت
Time	7:55:20	ساعت فعالیت
	Service and instance	W3SVC2
لاگی که مربوط به سایت خاصی می‌شود به صورت #W3SVC نمایش داده می‌شود که علامت # شماره سایت می‌باشد که در اینجا این لاگ مربوط به سایت شماره 2 است	**Server name**	SERVER
نام سرور	**Server IP**	172.21.13.45
آی پی سرور	**Time taken**	4502
چقدر انجام عملیات این درخواست به طول انجامیده است که بر حسب میلی ثانیه است.	**Client bytes sent**	163
تعداد بایت هایی که از طرف کلاینت به سرور ارسال شده است	**Server bytes sent**	3223
تعداد بایت هایی که از طرف سرور به سمت کلاینت ارسال شده است	**Service status code**	200
درخواست کاملا موفقیت آمیز بوده است	**Windows status code**	0
درخواست کاملا موفقیت آمیز بوده است	**Request type**	GET
نوع درخواست کاربر	**Target of operation**	/DeptLogo.gif
کاربر قصد دانلود یک فایل تصویری GIF	**Parameters**	-

نام فیلد	نوع حالت مقداردهی	توضیح اتفاقات افتاده
داشته است که نامش Deptlogo است		

فرمت NCSA: این فرمت توسط مرکز علمی کاربردهای ابرمحاسباتی National Center for Supercomputing Applications ایجاد شده و دقیقا مانند قبلی نمیتوان در آن نوع فیلدها را مشخص کرد و برای جدا سازی، از فاصله space استفاده می‌کند و ثبت مقدار زمان در آن هم به صورت محلی و هم UTC می‌باشد.
این فیلدها در لاگ آن نمایش داده می‌شوند:

Remote host address

Remote log name (This value is always a hyphen)

User name

Date, time, and Greenwich mean time (GMT) offset

Request and protocol version

Service status code (A value of 200 indicates that the request was fulfilled successfully)

Bytes sen

نمونه ای از یک لاگ ثبت شده:

```
172.21.13.45 - Microsoft\JohnDoe [08/Apr/2001:17:39:04 -0800] "GET /scripts/iisadmin/ism.dll?http/serv
HTTP/1.0" 200 3401
```

نام فیلد	مقدار ثبت شده	توضیح اتفاق افتاده
Remote host address	172.21.13.45	آی پی کلاینت
Remote log name	-	نامی وجود ندارد
User name	Microsoft\JohnDoe	نام کاربری
Date, time, and GMT offset	[08/Apr/2001:17:39:04 -0800]	تاریخ و ساعت فعالیت به صورت محلی که 8 ساعت از مبدا گرینویچ بیشتر است
Request and protocol version	GET /scripts/iisadmin/ism.dll?http/serv HTTP/1.0	کاربر با متد GET و Http نسخه‌ی یک، درخواست فایل ism.dll را کرده است.
Service status code	200	عملیات کاملا موفقیت آمیز بود.
Bytes sent	3401	تعداد بایت‌های ارسال شده به سمت کاربر

امنیت در برابر کاربران مهاجم مانند همان فرمت قبلی صورت گرفته است.

فرمت W3C : توسط W3C توسط کنسرسیوم جهانی وب ارائه شده است و یک فرمت ASCII text-based customizable است. به این معنی که میتوان فیلدهایی که در گزارش نهایی می‌آید را خودتان مشخص کنید، که برای اینکار در کنار لیست، دکمه‌ی Select

وجود دارد که میتوانید هر کدام از فیلدهایی را که خواستید، انتخاب کنید تا به ترتیب در خط لاگ ظاهر شوند. تاریخ ثبت به صورت UTC است.

نام فیلد	توضیح	به طور پیش فرض انتخاب شده است
Date	تاریخ رخ دادن فعالیت	بله
Time	ساعت زخ دادن فعالیت بر اساس UTC	بله
Client IP Addres s	آی پی کلاینت	بله
User Name	نام کاربری که هویت آن تایید شده و در صورتی که هویت تایید شده نباشد و کاربر ناشناس باشد، جای آن - قرار می‌گیرد	بله
Service Name and Instance Number	نام و شماره سایتی که درخواست در آن صورت گرفته است	خیر
Server Name	نام سروری که لاگ روی آن ثبت می‌شود	خیر
Server IP Address	آی پی سرور که لاگ روی آن ثبت می‌شود	بله
Server Port	شمره پورتی که سرویس مورد نظر روی آن پورت اعمال می‌شود.	بله
Method	متد درخواست مثل GET	بله
URI Stem	هدف درخواست یا Target مثل index.htm	بله
URI Query	کوئری ارسال شده برای صفحات داینامیک	بله
HTTP Status	کد وضیعینی HTTP status	بله
Win32 Status	کد وضعیتی ویندوز	خیر
Bytes Sent	تعداد بایت‌های ارسال شده به سمت کلاینت	خیر
Bytes Received	تعداد بایت‌های دریافت شده از سمت کلاینت	خیر
Time Taken	زمان به طول انجامیدن درخواست بر حسب میلی ثانیه	خیر
Protocol Version	درخواست با چه نسخه‌ای از پروتکل http یا ftp ارسال شده است	خیر
Host	اگر در هدر درخواست ارسالی این گزینه بوده باشد، نوشته خواهد شد.	خیر
User Agent	اطلاعات را از هدر درخواست می‌گیرد.	بله
Cookie	اگر کوکی رد و بدل شده باشد، محتویات کوکی ارسالی یا دریافت شده	خیر
Referrer	کاربر از چه سایتی به سمت سایت ما آمده است.	خیر
Protocol Substatus		بله

نام فیلد	توضیح	به طور پیش فرض انتخاب شده است
	در صورت رخ دادن خطا در IIS ، کد خطا بازگردانده میشود. در IIS به منظور امنیت بیشتر و کاهش حملات، محتوای خطاهای رخ داده در IIS به صورت متنی نمایش داده نمی‌شوند و شامل کد خطایی به اسم Substatus Code هستند تا مدیران شبکه با ردیابی لاگ‌ها پی به دلیل خطا و درخواست‌های ناموفق ببرند. برای مثال Error 404.2 به این معنی است که فایل درخواستی به دلیل قوانین محدود کنده، قفل شده و قابل ارائه نیست. ولی هکر تنها با خطای 404 یعنی وجود نداشتن فایل روبرو می‌شود. در حالت substatus code، کد شماره 2 را هم خواهید داشت که در لاگ ثبت می‌شود. هر شخصی که در سرور توانایی دسترسی به لاگ‌ها را داشته باشد، می‌تواند کد دوم خطا را نیز مشاهده کند. برای مثال مدیر سرور متوجه میشود که یکی از فایل‌های مورد نظر به کاربران، خطای 404 نمایش میدهد و با بررسی لاگ‌ها متوجه می‌شود که کد خطا 404.9 هست. از آنجا که ما همه‌ی کدها را حفظ نیستیم به این صفحه رجوع می‌کنیم و متوجه میشویم تعداد کاربرانی که برای این فایل، اتصال connection ایجاد کرده‌اند بیش از مقدار مجاز است و مدیر میتواند این وضع را کنترل کند. برای مثال تعداد اتصالات مجاز را نامحدود unlimited تعیین کند.	

حروف - و + برای موارد بالا هم صدق می‌کند. در ضمن گزینه‌های زیر در حالتی که درخواست از پروتکل FTP باشد مقداری نخواهند گرفت:

uri-query

host

(User-Agent)

Cookie

Referrer

substatus

گزینه Custom : موقعی که شما این گزینه را انتخاب کنید ماژول logging غیرفعال خواهد شد. زیرا این امکان در IIS قابل پیکربندی نیست و نوشتن ماژول آن بر عهده شما خواهد بود؛ با استفاده از اینترفیس های ILogPluginEx ، ILogPlugin و ILogUIPlugin آن را پیاده سازی کنید.

ذخیره اطلاعات به انکدینگ UTF-8 و موضوع امنیت

در صورتی که شما از سایتی با زبانی غیر از انگلیسی و لاتین و فراتر از ANSI استفاده می‌کنید، این گزینه حتما باید انتخاب شده باشد تا درخواست را بهتر لاگ کند. حتی برای وب سایت‌های انگلیسی زبان هم انتخاب این گزینه بسیار خوب است؛ چرا که اگر به سمت سرور کاراکترهای خاصی در URL ارسال شوند، نمی‌تواند با کدپیج موجود آن‌ها را درست تبدیل کند.

ادامه‌ی تنظیمات

موارد بعدی که در تنظیمات لاگ‌ها کاملا مشخص و واضح است، عملیات زمان بندی است که برای ساخت یک فایل لاگ جدید به کار می‌رود؛ برای مثال هر ساعت یک لاگ فایل جدید بسازد و فعالیت‌های موجود در هر ساعت در یک لاگ ذخیره می‌شوند.

گزینه‌ی بعدی حداکثر حجم هر فایل لاگ است که به صورت بایت مشخص می‌شود. اگر مقداری که تعیین میکنید کمتر از 1048576 بایت باشد، خودش به طور پیش فرض همان 1048576 بایت را در نظر خواهد گرفت.

گزینه بعدی do not create a new logfile بدین معناست که همه‌ی لاگ‌ها در یک فایل ذخیره می‌شوند و فایل جدیدی برای لاگ‌ها ایجاد نمی‌شود.

گزینه آخری به اسم use local time for filenaming and rollover است که اگر انتخاب شود، نامگذاری هر فایل لاگ بر اساس زمان محلی ساخت فایل لاگ خواهد بود. در صورتیکه انتخاب نشود، نامگذاری با زمان UTC درج خواهد شد.

سطح سرور

لاگ‌ها فقط در سمت سرور انجام می‌گیرد و لاگ هر سایت در یک فایل لاگ ثبت می‌شود. اگر بخواهید لاگ‌ها را در سطح سرور انجام دهید، گزینه‌ی binary هم اضافه خواهد شد.

Binary: در این گزینه دیگر از قالب بندی یا فرمت بندی لاگ‌ها خبری نیست و لاگ هر وب سایت به صورت اختصاصی صورت نمی‌گیرد. عملیات ذخیره سازی و ثبت هر لاگ می‌تواند از منابع یک سرور از قبیل حافظه و CPU و ... استفاده کند و اگر تعداد این وب سایت‌ها بالا باشد، باقی روش‌ها باعث فشار به سرور می‌شوند. برای همین ایجاد یک فایل خام از لاگ‌ها در این مواقع می‌تواند راهگشا باشد. برای همه یک فایل لاگ ایجاد شده و بدون قالب بندی ذخیره می‌کند. پسوند این نوع لاگ‌ها ibl است که مخفف Internet Binary Log می‌باشد. دلیل این تغییر پسوند این است که اطمینان کسب شود کاربر، با برنامه‌های متنی چون notepad یا امثال آن که به Text Utilities معروفند فایل را باز نمی‌کند. برای خواندن این فایل‌های میتوان از برنامه‌ی Log parser استفاده کرد. پروتکل‌های FTP,NNTP و SMTP در این حالت لاگشان ثبت نمی‌شود.