COMPUTERWORLD

Microsoft Log Parser, Windows logfil analyse

Microsoft's logfiler er ikke lette at bruge. med Microsoft Log Parser, har du alle muligheder. Log parser er et gratis og meget kraftfuldt værktøj til gennemsyn af alle mulige windows logfiler

Skrevet den **08. Feb 2009** af **bufferzone** I kategorien **Styresystemer / Generelt** | ⭐⭐⭐☆☆

Gennemsyn af logfiler fra Windows baserede programmer, herunder de forskellige Windows elementer (f.eks. IIS, Exchange og MSSql) selv, har altid været bøvlet og svært at få noget brugbart ud af det. Det har Microsoft, ganske ubemærket, faktisk gjort noget ved. Programmet Microsoft Log Parser kan downloades fra MS hjemmeside, og dette værktøj giver fantastisk kontrol med forskellige logfiler og mulighed for at få mange brugbare svar, hvis man ved hvordan programmet skal bruges.

Microsoft Log Parser er et kommandolinie værktøj der er bygget oven på en SQL motor og derfor baserer sig på helt almindelige SQL Queries.

Grundlæggende forespørgsler

Lad os starte med at kikke på en rimelig simpel forespørgsel.

```
C:\>LogParser -i:EVT -o:NAT "SELECT TimeGenerated, SourceName FROM System"
```

Log Parser arbejder, ud over SQL statements, med input- og output format (se sidst i artiklen), til at styre henholdsvis hvorfra data skal hentes og hvordan resultatet skal præsenteres.
I ovenstående kommando ser vi følgende:

-i:EVT der fortæller at input data skal hentes (enumereres) fra Windows Event Log, "FROM System" fortæller at det er system loggen vi kikker på.

-o:NAT der fortæller at output formatet via tabulatorer som et letlæseligt skema

SELECT der fortæller hvad vi ønsker at hente fra event loggen. I dette tilfælde er det TimeGenerated og SourceName vi ønsker at se.

Hvis du vil se hvilke tabel felter du kan hente ud af event loggen, så brug nedenstående kommando

```
C:\>LogParser -h -i:EVT
```

Der lister alle mulighederne

FROM Der fortæller hvilken af de tre logge (system, application eller security) vi ønsker at kikke i.

Resultatet fra vores Log Parser forespørgsel ser således ud:

<pre
TimeGenerated SourceName
------------------- ----------------------

2005-07-18 22:45:03 EventLog
2005-07-18 22:45:03 EventLog
2005-07-18 22:45:26 Service Control Manager
2005-07-18 22:45:26 Service Control Manager
2005-07-18 22:45:26 Service Control Manager
2005-07-18 22:45:26 Service Control Manager
2005-07-18 22:45:26 Service Control Manager
2005-07-18 22:45:26 Service Control Manager
2005-07-18 22:45:26 Service Control Manager
2005-07-18 22:45:26 Service Control Manager

Press a key...
[/pre]

Du kan faktisk hente data fra andre computere på nettet ved at anvende UNC notation, herunder er et eksempel du kan prøve:

```
C:\>LogParser -i:EVT -o:NAT "SELECT TimeGenerated, SourceName FROM
\\MYCOMPUTER1\System, \\MYCOMPUTER2\Security"
```

Du kan også søge efter specifikke informationer, f.eks. vil nedenstående kommando give alle records der er genereret af Service Control Manager

```
C:\>LogParser -i:EVT -o:NAT "SELECT TimeGenerated, SourceName FROM
System WHERE SourceName ='Service Control Manager'"
(husk de små ')
```

Langt de fleste input- og output formater accepterer forskellige parametre der styre eller rettere fin tuner deres opførsel. Ovenfor ses et output på 10 linier, hvorefter du promptes for at trykke på en tast for at fortsætte. Denne standard opførsel kan ændres med rtp parametren.

```
C:\>LogParser -i:EVT -o:NAT -rtp:5 "SELECT TimeGenerated, SourceName FROM
System"
```

Der kun vil outputte 5 linier før du promptes for et taste tryk. Hvis du indsætter -rtp:-1 vil du ikke blive promptet overhoved og hele indholdet vil blive udskrevet uden mulighed for at gøre noget.

Vi kan også skrive outputtet til en fil, f.eks. sådan

```
C:\>LogParser -i:EVT -o:NAT "SELECT TimeGenerated, SourceName
INTO log.txt"
```

Der skriver resultatet til filen log.txt.

Du kan også bruge de logiske operatorer And eller/og OR. Her henter vi data generet af Service Control

Manager og hvor event ID er 7024 (en service termineret med en fejl)

```
C:\>logparser.exe file: "SELECT TimeGenerated, SourceName FROM
System WHERE SourceName ='Service Control Manager' AND
EventID = 7024"
```

Vi kan også hente burger oplysninger fra en server. Herunder henter vi logon oplysninger og vi henter det fulde kontonavn og ikke bare konto identifikation.

```
C:\>logparser.exe file: "SELECT TimeGenerated, SID FROM Security WHERE EventID =
528" -resolveSIDs:ON
```

EventID = 528 er logon og resolveSIDs:ON fortæller EVT input formatet at vi ønsker det fulde kontonavn

Hente ting fra en IIS Log

Lad os starte med at se hvilke tabelfelter vi kan hente ud af IIS log.

```
C:\>logparser.exe file: -h -i:IISW3C
```

Vi kunne derefter beslutte at hente felterne date, time , og cs -uri - stem. Kommandoen ville se sådan ud:

```
C:\>LogParser -i:IISW3C -o:NAT "SELECT date, time, cs-uri-stem
FROM <1>"
```

Vi bruger her FROM til at specificere hvilken log fil vi ønsker at kikke i. Vi kan bruge stien til den logfil vi ønsker eller ID nummeret for det virtuelle site vi ønsker. Her har jeg brugt ID 1 der er ID nummeret på Default web site.

Hvis du har flere web sites på din server, kan du hente fra alle logs ved at specificere flere ID'ere adskilt af komme således:

```
C:\>logparser.exe file: -i:IISW3C -o:NAT "SELECT date, time,
cs-uri-stem FROM <1>, <2>, <3>"
```

Her henter vi oplysninger der viser hvilke sider der tager mere end 30 sekunder at udføre

```
C:\>logparser.exe file: "SELECT TO_TIMESTAMP(date, time) AS Timestamp, cs-uri-
stem FROM W3SVC2\ex0402*.log WHERE time-taken
>= 30000" -i:IISW3C
```

Ovenstående er et eksempel på endnu et eksempel på den styrke log parser har via SQL motoren. Log Parser SQL indeholder mere end 80 forskellige funktioner, der bl.a. laver streng manipulation , aritmetikfunktioner, system informationsfunktioner og meget mere.
Her bruger vi TO_TIMESTAMP funktionen til at anvende date og time som argumenter.

Input formater:

ADS: Active Directory Services henter fra AD.
BIN: Henter binær data fra IIS 6.0 og senere logfiler.
COM: Indpakker custom input format plug-ins, hvilket gør det muligt at bruge den slags plug-ins.
CSV: Henter data fra komma separerede text filer.
ETW: Henter data fra Enterprise Tracing for Windows trace log files og live tracing sessions.
EVT: Henter data fra Windows Event Log
FS: Returnere egenskaber fra filer og mapper
HTTPERR: Henter data fra HTTP Error log files der genereres af Http.sys Windows HTTP driver.
IIS: Henter data fra IIS log filer
IISODBC: Henter data fra den database hvortil IIS logger Web requests når IIS er konfigureret til at bruge ODBC Log Format.
IISW3C: Henter data fra W3C Extended Log File Format.
NCSA: Henter data fra NCSA Common, Combined, and Extended Log Fil format.
NETMON: Henter data fra NetMon capture filer (.cap files).
REG: Henter egenskaber fra registreringsdatabasen I form af registry keys og værdier.
TEXTLINE: Henter data fra generiske text filer I form af hele linier.
TEXTWORD: Henter data fra generiske text filer I form af hele ord.
TSV: Henter data fra tabulator- og mellemrums separerede filer.
URLSCAN: Henter data fra logfiler fra IIS URLScan filter.
W3C: Henter data fra ikke IIS W3C Extended Log File Format, f.eks. Exchange Tracking log filer, Personal Firewall log filer, og Windows Media Server log filer.
XML: Henter element- og attribute- data fra XML dokumenter

Output formater:

CHART: laver GIF eller JPG diagrammer som output
CSV: Laver komma separerede tekst filer der kan efterbehandles af f.eks. excel.
DATAGRID: Viser data i et separat vindue så data kan klippes og sættes ind via Clip Board.
DATAGRID: Laver output som IIS logfil
NAT: Laver output i et læseligt, tabuleret format
SQL: uploader output til tabeller i ODBC- compliant database format.
SYSLOG: Muliggør at outputted leveres til en syslog server
TPL: Laver output formateret efter en bruger defineret skabelon
TSV: Laver et tabulator separet output

Som du sikkert kan gennemskue af ovenstående artikel er der uendeligt mange muligheder for at parse stort set nøjagtig de informationer du måtte ønske og præsentere disse på den måde du ønsker, selv grafisk præsentation med GIF eller JPG diagrammer er muligt. Artiklen skulle gerne kunne starte dig og ved at følge eksemplerne vil det være muligt for dig at bygge videre med -h for hjælp og de to sidste lister med input og output formater.

Log parser er et stort område og der kan godt være at jeg beslutter at skrive endnu en artikel. Alle kommentarer, tilføjelser, bemærkninger er meget velkomne. Du kan også stille spørgsmål, både her på eksperten og via kim@bufferzone.dk, jeg beder om at I ikke stiller spørgsmål i artiklens kommentarer da

jeg her ikke kan svare

Kommentar af kepsus d. 22. Aug 2005 | 1

Kommentar af lenk d. 05. Aug 2005 | 2

En meget nyttig artikel om et meget nyttigt værktøj. Alle der har servere kørende bør læse og prøve selv

Kommentar af john_stigers (nedlagt brugerprofil) d. 03. Feb 2006 | 3

Ok artikel som dog burde have været gratis.

Kommentar af barbarbo d. 02. Aug 2005 | 4

Rigtig god artikel der giver mulighed for at nå ret langt med windows logfiler. De eksempelvise kommandoer kombineret med hjæle kommandoen og listen over mulighdere er en stor hjælp