Using the Logparser Utility to Analyze Exchange/IIS Logs

Written by Marc Grote - mailto:grotem@it-training-grote.de

Abstract

In this article I will show you how to use the Microsoft Logparser Utility to analyze Microsoft Exchange Server/IIS log files.

Let's begin

Logparser is a Tool developed by Microsoft which you can use to analyze different Log files and File formats. It is not primary designed for Exchange Server but can be used to analyze the different Exchange and IIS log files.

Logparser is a command line tool but a rudimentarily GUI is available as an Addon which I will show you later.

Other possibilities of Logparser are the possibility to analyze Windows Event Logs, to aggregate Data and to display Logparser data in HTML forms and other formats.

Logparser Historie

Logparser 1.0 (2000) was the first version from Microsoft used internally to analyze IIS log files.
Logparser 2.0 was the first public available version from Microsoft.
Logparser 2.1 is part of the IIS 6 Resource Kit.
The next version was Logparser 2.2 from January 2005.
The actual version of Logparser is 2.2.10 from April 2005.

Logparser Architecture

As you can see in the following picture, Logparser can analyze Log files from many different Log file formats like Textfiles, EventLogs and Registry. Microsoft Logparser uses a SQL like Engine to make Data queries, to aggregate data and to format data for displaying.

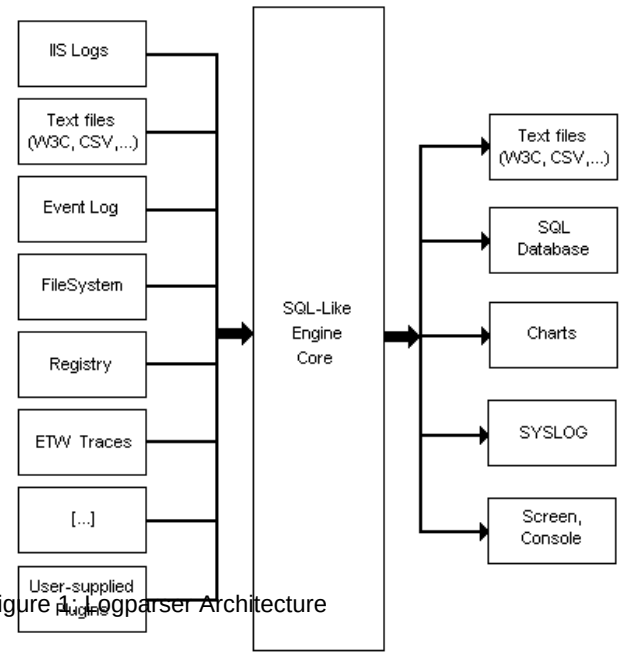

Figure 1: Logparser Architecture

Logparser Download

You can Download the newest version from Microsoft Logparser at the following website:
http://www.microsoft.com/downloads/details.aspx?FamilyID=890cd06b-abf8-4c25-91b2-f8d975cf8c07&displaylang=en

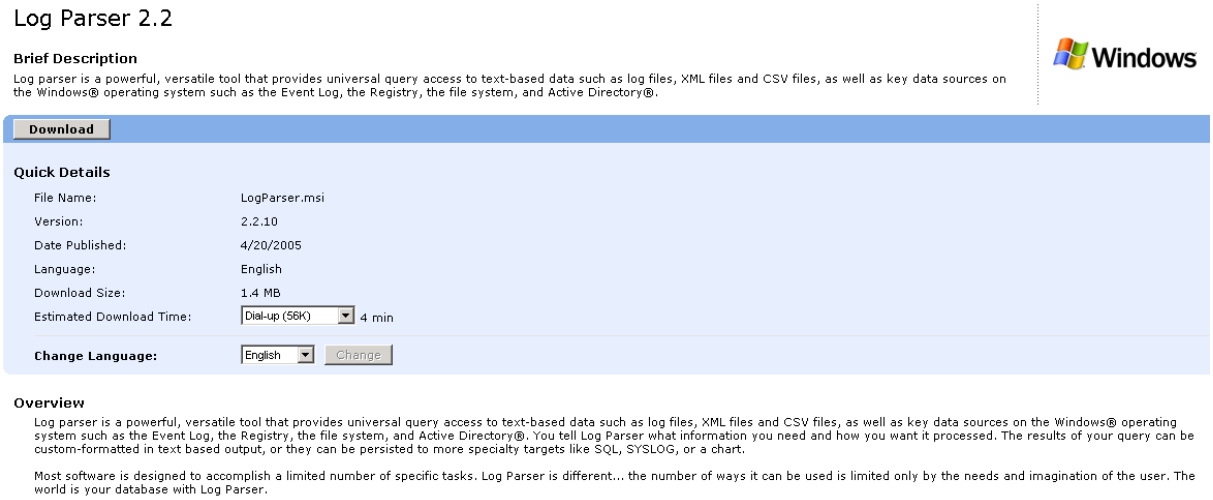

Figure 2: Downloading Logparser

Installation

After downloading Logparser, simply double click the installation file and follow the installation instructions. When you install the package select “Documentation” and “Samples” to get a quick start guide how to use Logparser and some samples to understand the Logparser syntax which is for person like me with minimal knowledge in programming and scripting not so easy to understand.

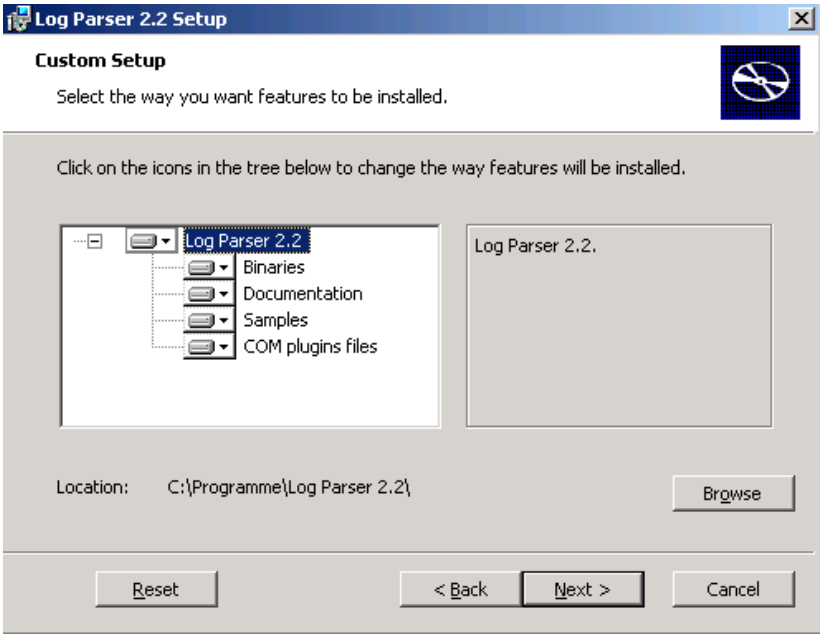

Figure 3: Logparser components

Logparser installs itself in a folder in Program Files without modifying the system's PATH environment variable, so you have to manually edit the System's PATH variable or copy Logparser.exe to the \Windows\system32 path.

Do you want to have more Information about Logparser?

The website http://www.logparser.com is the official unofficial website for Logparser resources. You will find some more helpful information about Logparser at http://www.securityfocus.com/infocus/1712.

GUI for Logparser

On the unofficial Logparser Website you will find a small Utility which gives Logparser an rudimentary GUI. The GUI has only a few menu items. The function to save a query for later execution or edit is nice.

You can download the Logparser GUI from the following website http://www.logparser.com/simpleLPview00.zip.

No installation is required. Simply open the Window and enter your query.

The command ...

*SELECT * FROM System*

Will show you all system event log entries on the local machine.

You can export the query results to a CSV file.

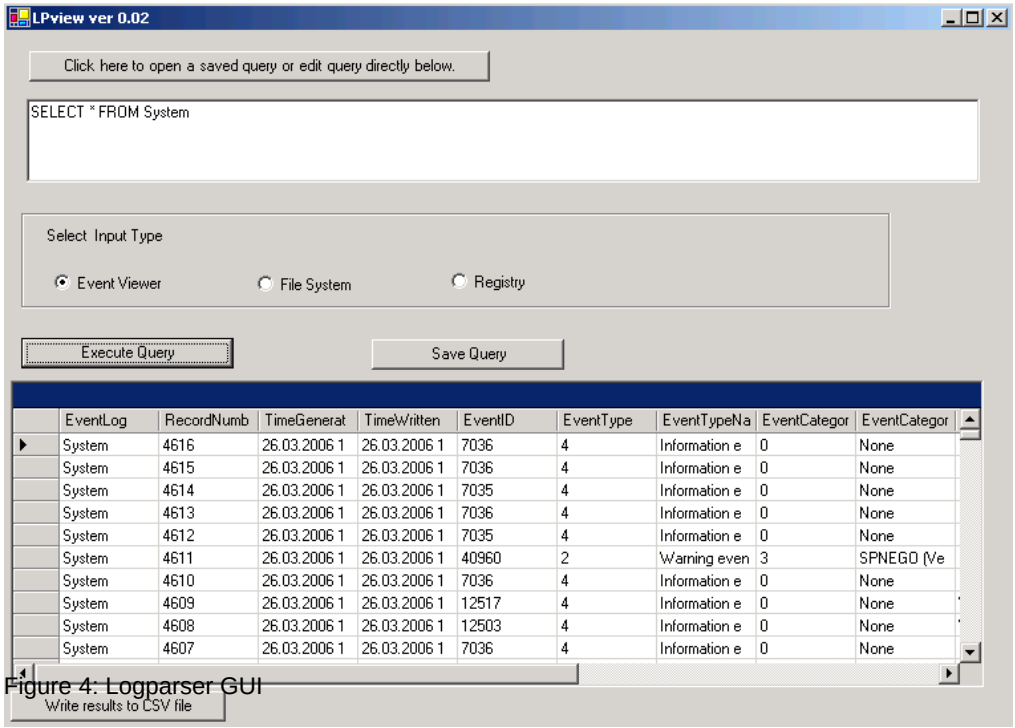

Figure 4: Logparser GUI

The command ....

SELECT Path, Size FROM C:\temp*.* ORDER BY SIZE

Lists all files and subdirectories from c:\temp, ordered by file size, beginning with the smallest file size.

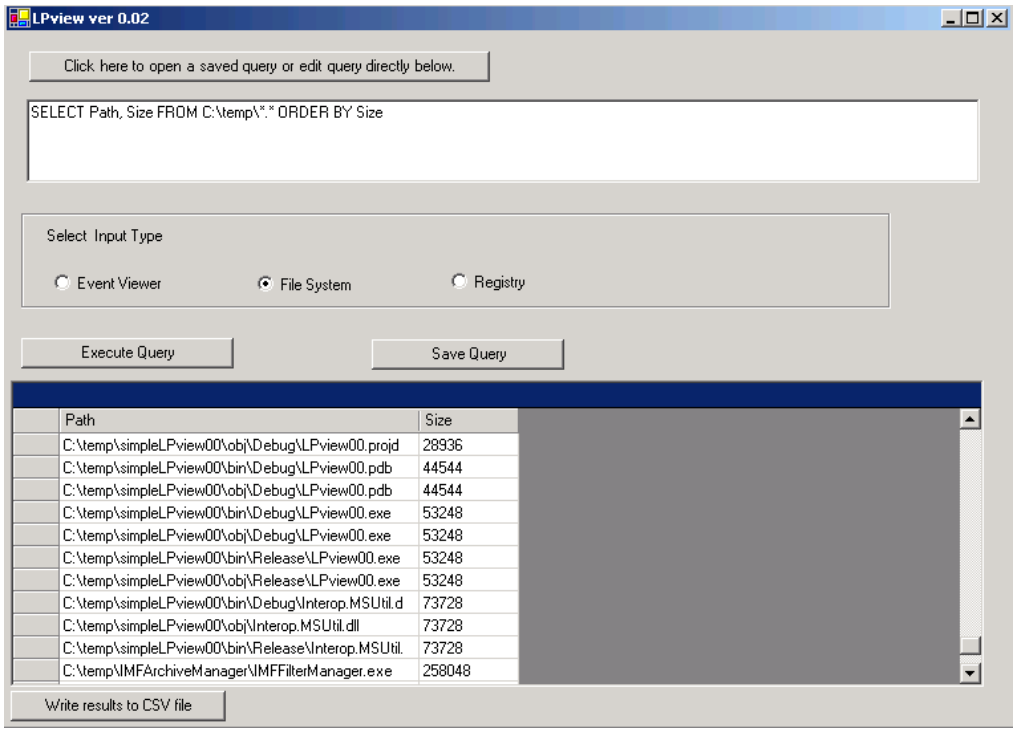

Figure 5: Logparser GUI – command to order files by size

IIS Services and Log file Formats

The following table shows the supported log file formats for Exchange services like Web, SMTP and NNTP.

Table 2.1 IIS Services and Logging Formats

Type of Service	IIS	NCSA	ODBC	W3C Extended	Centralized Binary
FTP	Yes	No	Yes	Yes	No
Web	Yes	Yes	Yes	Yes	Yes
SMTP	Yes	Yes	Yes	Yes	No
NNTP	Yes	Yes	Yes	Yes	No

Figure 6: Supported Log file formats

IIS W3C Protocol fields

If you want to analyze the W3C log files for OWA usage, you must know which Properties you can specify in the Logparser tool. You will find the same table for SMTP Log Fields in the Online help from Microsoft Exchange 2003.

Table 2.2 W3C Extended Log Fields

Property	Field	Description
Client IP Address	c-ip	Client IP address that accessed the IIS server
User Name	cs-username	User name that accessed the IIS server
Service Name	s-sitename	Site name serving the request, for example, W3Svc1
Server Name	s-computername	IIS server name
Server IP Address	s-ip	IIS server IP address serving the request
Server Port	s-port	IIS server port number serving the request
Method	cs-method	Client action request, for example, GET, POST
URI Stem	cs-uri-stem	Request content name, for example, html, asp page
URI Query	cs-uri-query	Query action along with client request
Protocol Status	sc-status	Status code of the request
Protocol Substatus	sc-substatus	Substatus code of the request
Win32 Status	sc-win32-status	Status code in Windows terms
Bytes Sent	sc-bytes	Number of bytes sent by server
Bytes Received	cs-bytes	Number of bytes received by server
Time Taken	time-taken	Amount of time to process the request
Protocol Version	cs-version	Client protocol version, for example, HTTP, FTP
Host	cs-host	Client computer name
User Agent	cs(User-Agent)	Application used by client, for example, browser
Cookie	cs(Cookie)	Content of cookies send or received
Referer	cs(Referer)	Previous URL that directed client to current site

Figure 7: W3C extended Log Fields

Input Formats

The input formats provided by Log Parser 2.2 include:

- Input formats that parse log files generated by IIS and return the entries in the logs
- Input formats that parse generic text log files formatted according to the CSV, TSV, NCSA, W3C, and XML standards and return the fields contained in the logs
- An input format that returns events from the Windows Event Log
- Input formats that return information on Active Directory objects, on files and directories, and on registry keys
- An input format that parses NetMon capture files and returns information on TCP/IP packets and connections

Output Formats

Output formats perform the opposite function of the input formats: they consume records and do something useful with the fields contained in the records. The output formats provided with Log Parser 2.2 can:

- Save records to text files formatted according to the CSV, TSV, W3C, and XML standards
- Save records to text files formatted according to generic user-specified templates
- Display records to the console or to a GUI window
- Upload records to a table in a SQL database
- Format records according to the Syslog standard, and dispatch records to a Syslog server, to a text file, or to a user
- Create Excel-style charts that present the record's numeric data in a graphical format

Logparser Basics

If you use Logparser the first time you should open Logparser with the /? Command to display a list of available commands. As you can see, Logparser is capable of many Input formats.

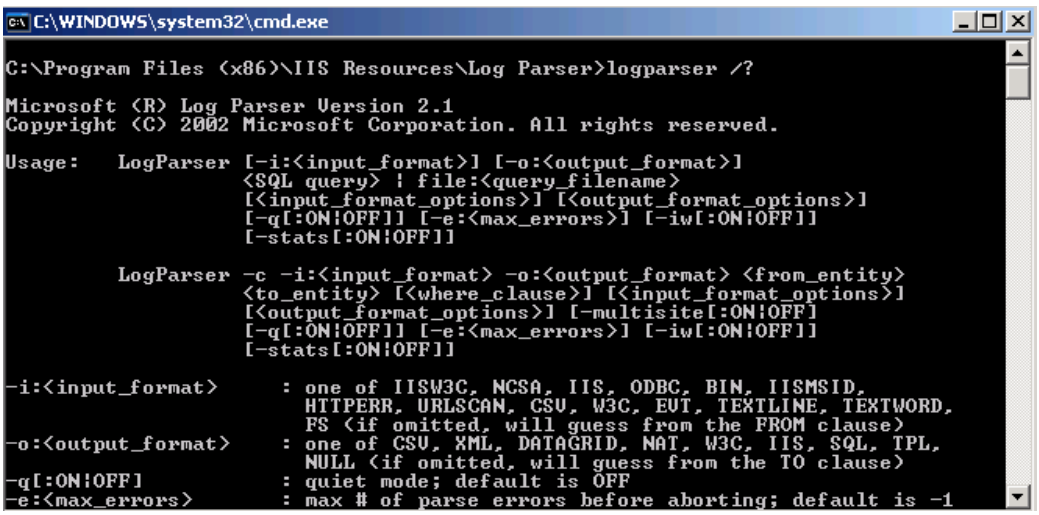

Figure 8: Logparser help

A simple query

The following Picture shows Logparser in Action to query a logfile in W3C format to find how often the IP address 84.233.178.2 is in the logfile. Logparser queries the Exchange Logfile named EX060326.LOG.

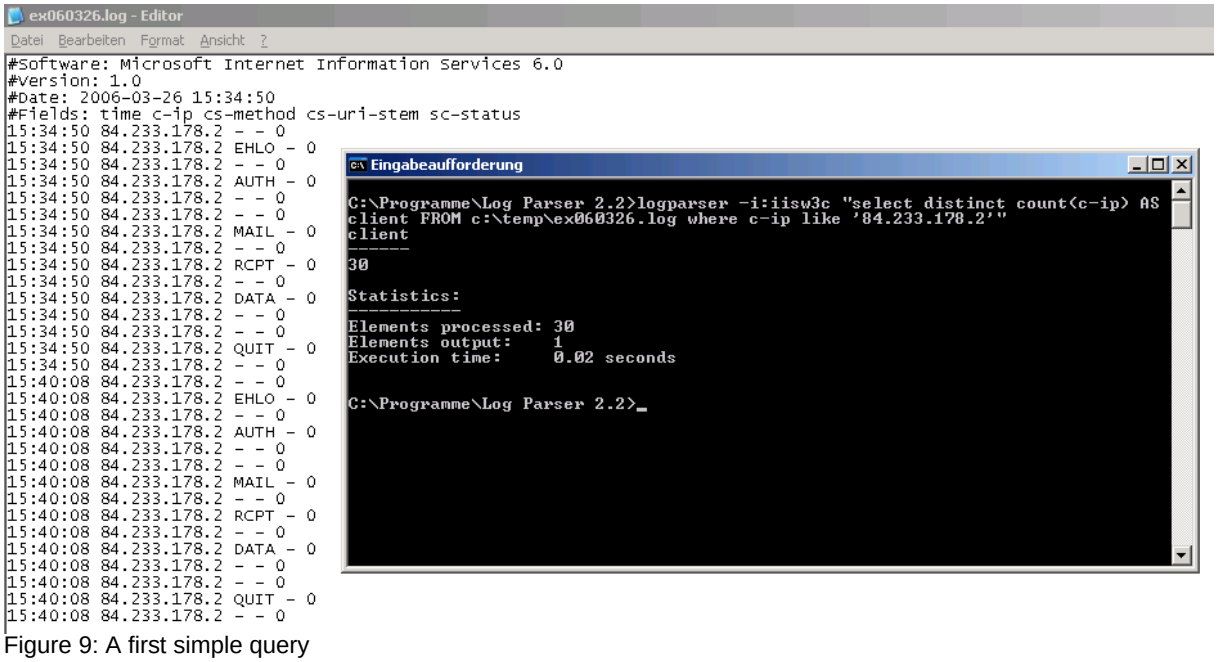

Figure 9: A first simple query

Output

With the help of the “NAT” option Logparser will display the results in the CLI (Command Line Interface) a little bit clearer. You can also use Logparser to display Logparser results as HTML reports. To use Logparser with HTML output you must use Templates. Templates will give Logparser the option to display query results in HTML format.

The following example shows a graphical HTML Report with a template.

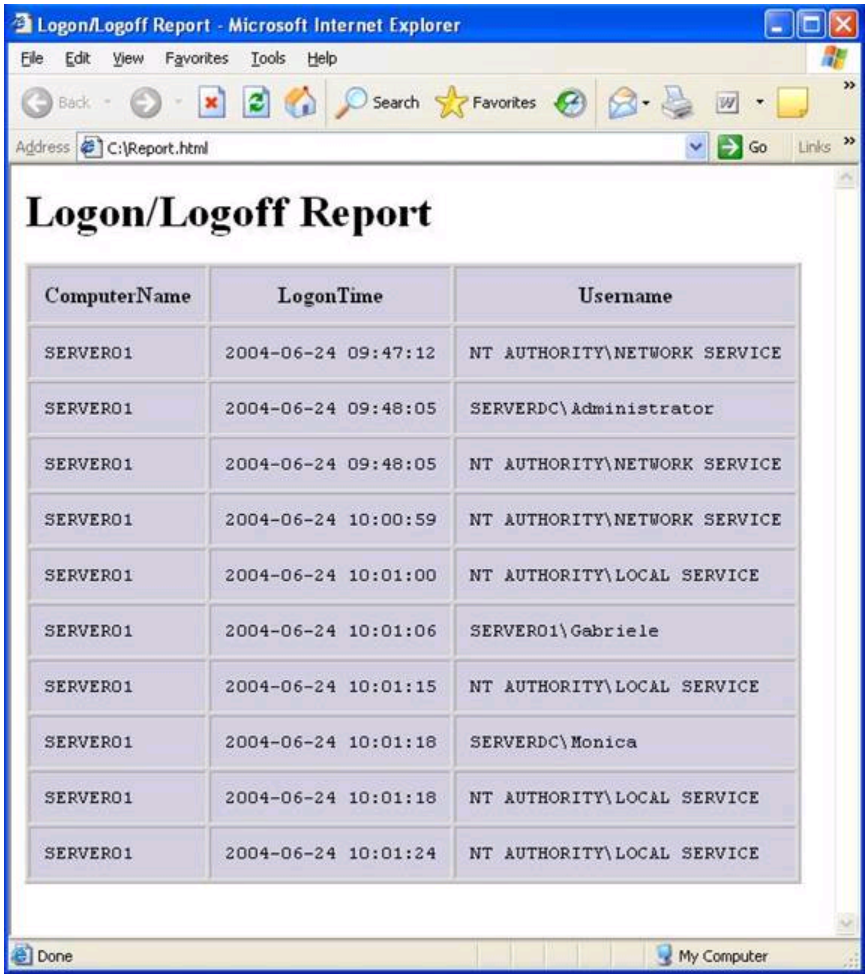

Figure 10: Logparser HTML Output

Logparser and Remote Systems

You can use Logparser to define queries from remote systems. You can extend Logparser queries for remote systems. The only thing you have to do is to extend the normal Logparser query with the remote Server in UNC convention.

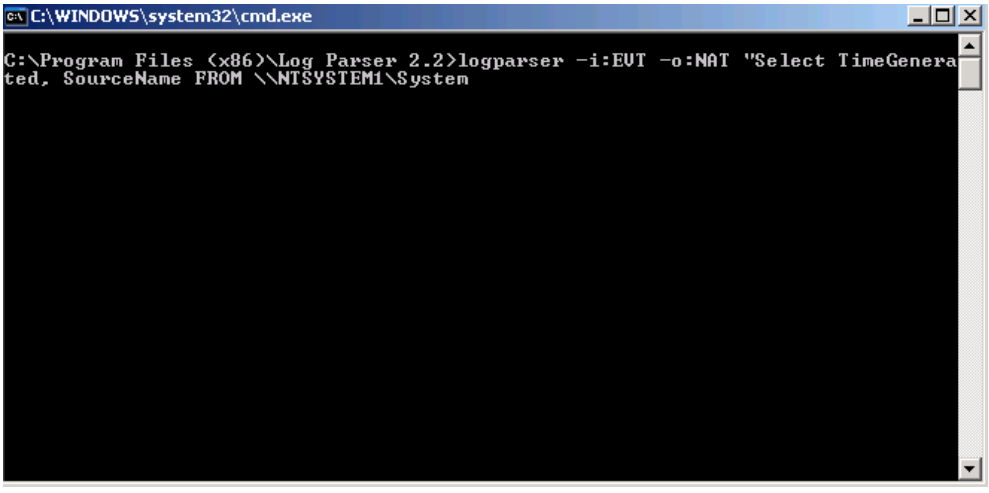

Figure 11: Logparser and execution on remote System

The command \\NTSYSTEM1\System queries the remote system NTSYSTEM1 and the System Event Log.

Additional commands

This article can't show you the whole Syntax of Logparser, but I will show you here some additional commands.

Show OWA users

The following Logparser command is a Microsoft Technet sample and shows you the OWA users of your Exchange Server.

"SELECT TO_STRING(time, 'HH') AS Hour, COUNT(*) AS Hits INTO hitPerSecond.jpg FROM ex*.log GROUP BY Hour ORDER BY Hour ASC" -i:IISW3C -o:CHART -chartType:ColumnClustered -chartTitle:"Hourly Hits" -groupSize:420x280

OWA usage

logparser file:owausage.sql -i:IISW3C -o:CHART -chartType:ColumnClustered -chartTitle:"owa.it-training-grote.de – Hits per Hour" -groupSize:420x280
-Start owausage.sql-
SELECT
 TO_STRING(time, 'HH') AS Hour,
 DIV(Sum(cs-bytes),1024) AS Incoming(K),
 DIV(Sum(sc-bytes),1024) AS Outgoing(K)
INTO %chartname%
FROM %source%
GROUP BY Hour
-End-

The Logparser Book

You can by the Logparser Book published by Syngress from the following website:
http://www.syngress.com/catalog/?pid=3110
This book is also available as a E-Book for less then 16$. If you will work closer with Logparser this book is my recommended reading for you.

Conclusion

Logparser is a great tool with many helpful functions and a powerful query language to analyze several different Log files from several different Data sources. Logparser is so powerful that you spend some time playing with this tool to be familiar with the complex syntax.

Related Links

The Unofficial Logparser Support Site
http://www.logparser.com
Download Logparser 2.2
http://www.microsoft.com/downloads/details.aspx?FamilyID=890cd06b-abf8-4c25-91b2-f8d975cf8c07&displaylang=en
Professor Windows - How Log Parser 2.2 Works
http://www.microsoft.com/technet/community/columns/profwin/pw0505.mspx
LogParser and RRDTool
http://geekswithblogs.net/woodenshoe/archive/2005/09/17/54194.aspx
Microsoft Technet LogParser Examples
http://www.microsoft.com/technet/scriptcenter/tools/logparser/lpexamples.mspx
Reporting for OWA Usage

http://www.msd2d.com/Content/Tip_viewitem_03NoAuth.aspx?id=d8f61600-172e-4ad4-a5b2-5e9526890cca&section=Exchange
Exchange Server ActiveSync Reporting with LogParser - COM object available
http://blogs.technet.com/exchange/archive/2006/03/03/421149.aspx
LogParser Commandline Creator
http://www.anonymoos.com/logparser.php