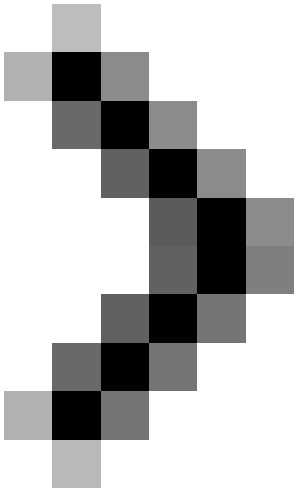
Managing log files of Exchange Server 2007 - Part 2

In this article, I will show you some other ways to get log information in Exchange Server 2007.



Managing log files of Exchange Server 2007 - Part 1
Anderson Patricio

In this article, I will show you some other ways to get log information in Exchange Server 2007.

Introduce

In the previous article of this series, I showed you how to debug in Exchange Server 2007 using the Set-EventLogLevel command. In this article, I will continue the configuration of the logs in Exchange Server 2007. Exchange Server 2007 allows debugging in a number of components, which are some of the components that we will cover. come in this second part:

- Internet Information Services (IIS)
- Message Records Management
- Agent Transport logs
- Message Tracking
- Send and Receive Connectors
- POP3 and IMAP4 protocols
- Connectivity Logs

You need to know where the above components are configured and capture the log information, which is really very useful in troubleshooting and reporting purposes.

Internet Information Services (IIS)

Exchange Server 2007 relies on IIS, we can use log files created by IIS to gather information about OWA, ActiveSync, Autodiscover, OAB, and the use of Web Services components as well as troubleshooting. Try the components when needed.

To validate log information, we can open **Internet Information Services (IIS) Manager** , this utility is located in the Administrative Tools menu, open **Web Sites,** then right-click on the selected website and click **Properties** (image 01). Make sure that *Enable Logging* option is *ticked* , then we can choose a format suitable for the logs, the default configuration is *W3C Extended Log File Format* .

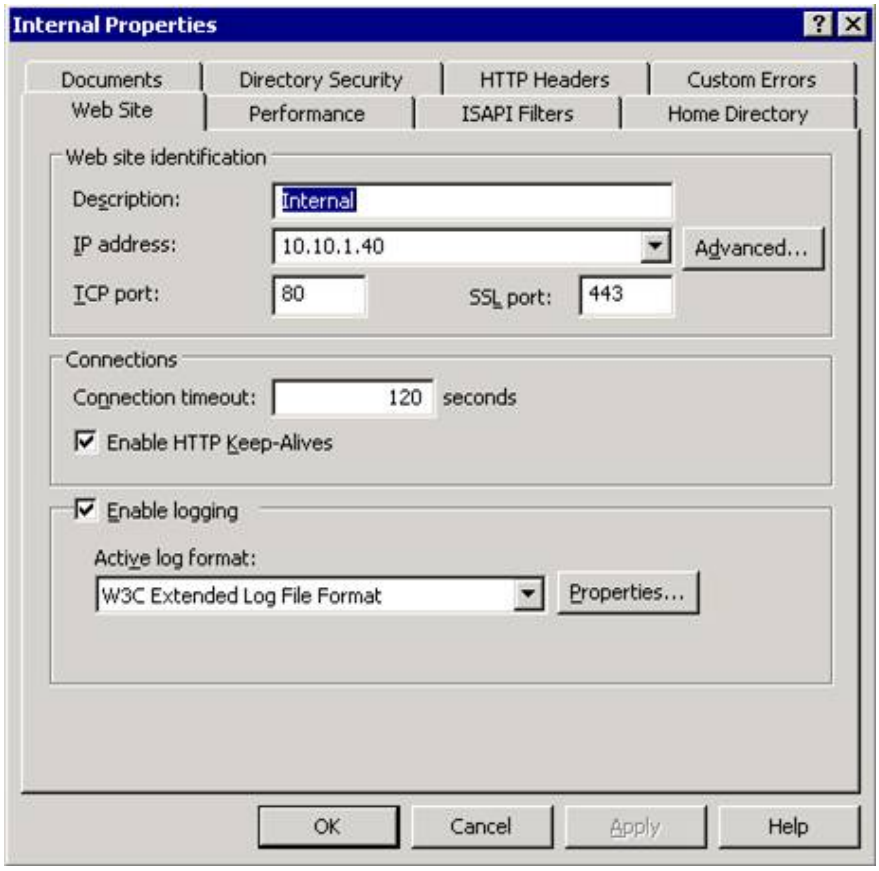


Figure 1

IIS log configuration is done at Website level, not Virtual Directory level. In the default exchange settings, we will have a website called *Default Web Site* and all Exchange Virtual folders located below it, such as: AutoDiscover, EWS, Exchange, OAB, UnifiedMessaging, . Even so Some companies do not use SAN (Subject Alternative Name) certificates when they choose multiple websites to provide the necessary certificates. In this case, each website will have a different log and location information to keep the log files.

If you click **Properties** in the Virtual Web Site main page, then two tabs will appear; *General* and *Advanced* . On the General tab (Figure 2) you can control how frequently the log files will be created (which can be daily as default) and you will have a file system location where all version files are The created record will be there, by default it will be C: windowssystem32Logfiles. When this is done, a small folder will be created based on the Virtual Web Site ID (Figure 2). In this example, the directory listed here is **W3SVC1.**

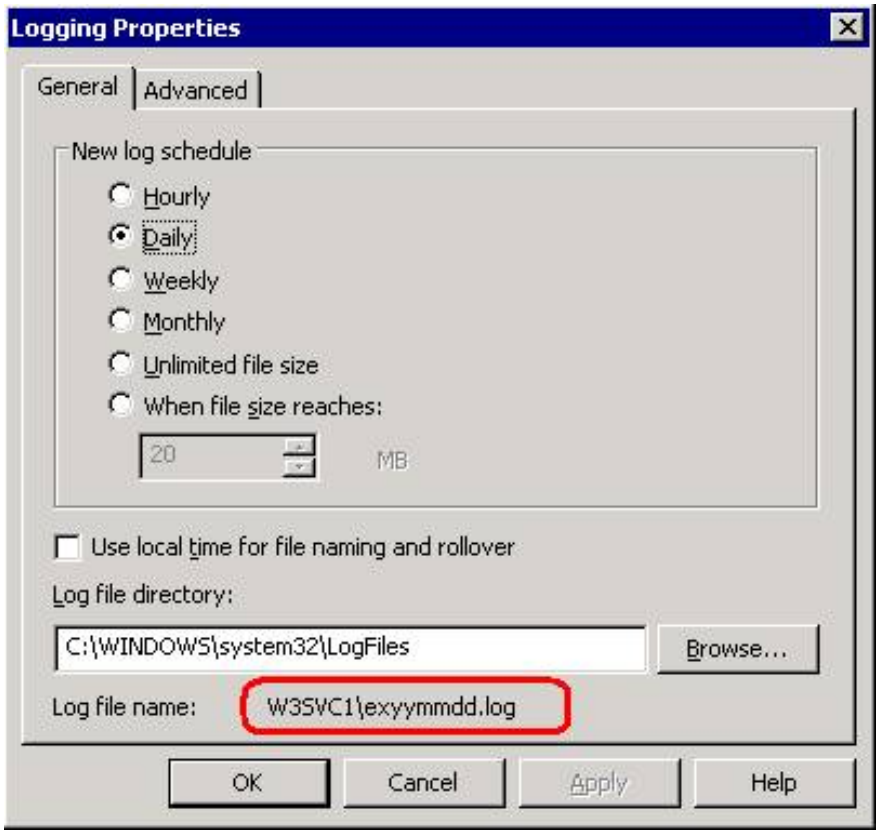


Figure 2

The *Advanced* tab allows you to select which fields will be recorded by IIS in the log files, as shown in Figure 3. You can use this page as a reference for the column names you will use with the utility. Log Parser in the next step.

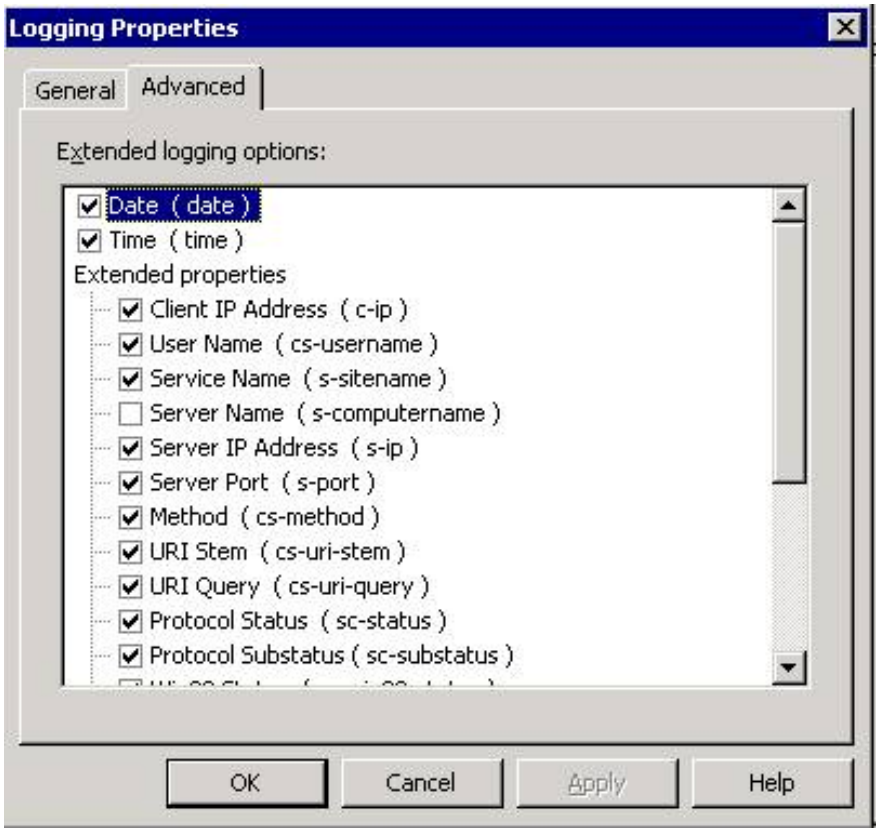


Figure 3

You can retrieve and troubleshoot from IIS log files with any editor, though we do it with a tool called Log Parser. This tool allows you to run queries using the SQL format to retrieve information from several different sources, such as CSV, EVT, IIS Log files, etc. The output will be in graphical form, text, html, .

How to use it?

Logparser is a command-line utility (logparser.exe) that we have some examples in the *Samples* and directories created during the installation of the tool. You can create your own queries with templates available or start completely new. However, you need to know that all fields used in queries come from the IIS field we selected in the previous image (Figure 3).

Besides, we also need to know the two basic parameters used by the tool, input and output. If you have any questions regarding the use of the tool, use *LogParser -h, and* there will be a summary of all the options displayed. Here are two basic command conversions that we will use:

- ' *-i:* ' - Here we can choose what output format is, in this case, it will be IISW3C.
- ' *-o:* ' - This is the data format to be displayed, in this case, we will use DataGrid to display the information in the GUI.

So if you open the *Samples* folder , then open the *Queries* subdirectory, you can choose the query you need here. In my case, we chose *Get authentication and authorization failures* where we could see the Http error code that the user is experiencing. Using the query that we copied from the –I and –o examples like we saw, you will get

the results shown in Figure 4.

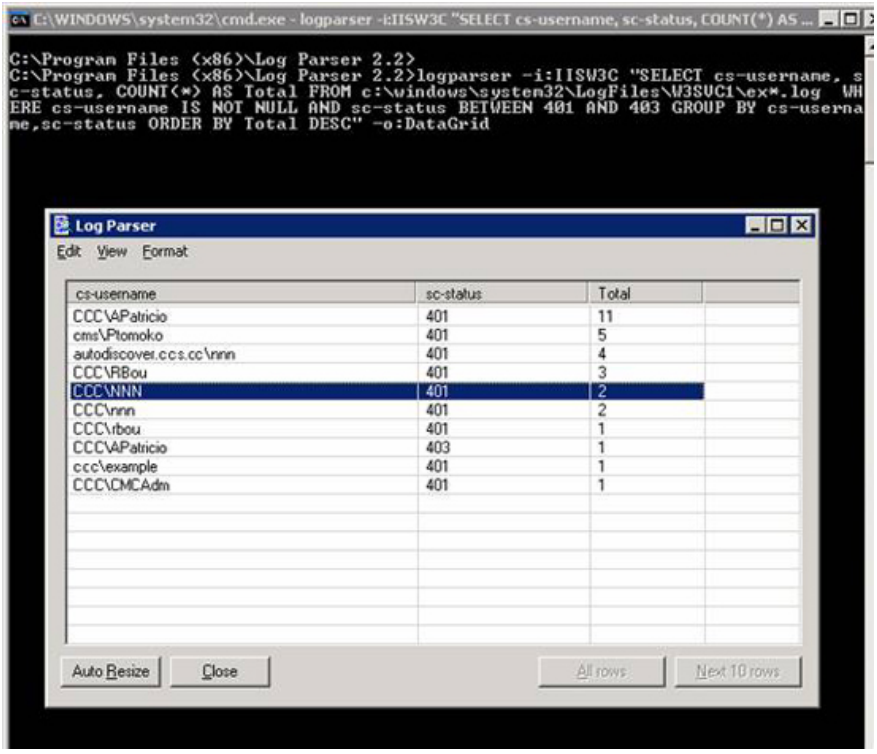


Figure 4

Note: To understand HTTP status code, we can collect more information in Microsoft Kbs below:

HTTP Status code for IIS 5.0 and 6.0, and IIS 7.

POP and IMAP protocols

By default, POP3 and IMAP4 services are disabled and *log features are* also disabled. If you enable one of these services in your environment and want to troubleshoot the client to connect and retrieve messages, you can manage the debugging information of these protocols by Change the files in the *Exchange ServerClientAccessPopImap* directory below:

- Microsoft.Exchange.Pop3.exe.config for POP3 service
- Microsoft.Exchange.IMAP4.exe.config for IMAP4 service

The log files have the same configuration in enabling or disabling, we just need to change the value of *ProtocolLog* parameter to *true* instead of *false* . All log files will be created on a led specified in the *LogPath* parameter, as shown in Figure 5.

Note: After enabling or disabling POP / IMAP login, you need to restart the service.

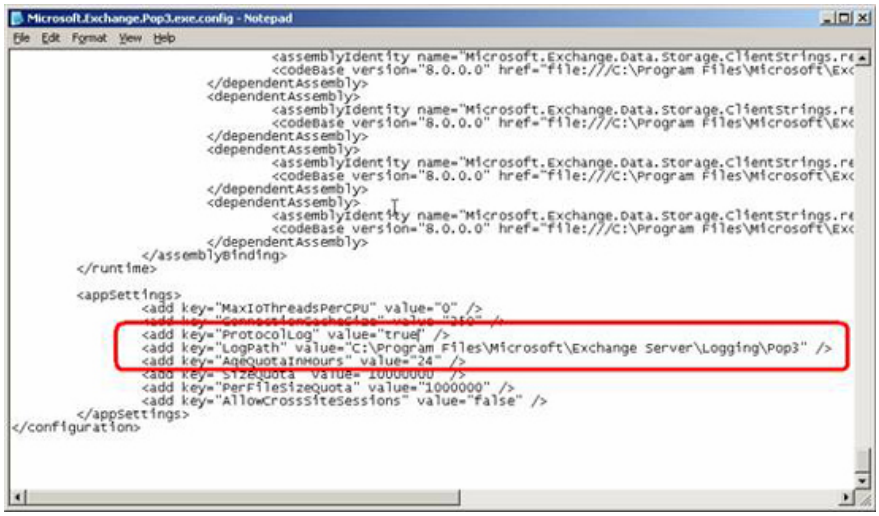


Figure 5

Now that we have activated the service and already know where the files were created, after connecting for the first time with POP / IMAP, we can open any log file and can absolutely validate the information stored on the server and other as shown in Figure 6 below.

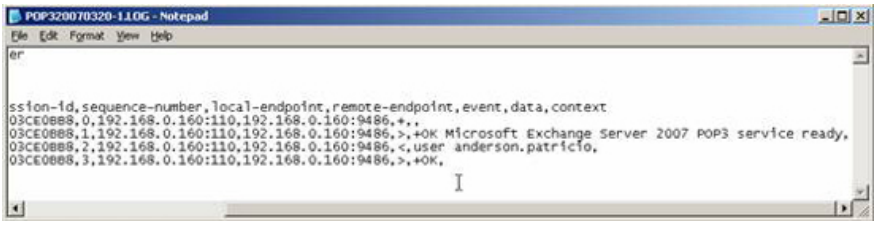


Figure 6

Conclude

In this article, I have discussed how to configure IIS logs and configure POP / IMAP logs in Exchange Server 2007.