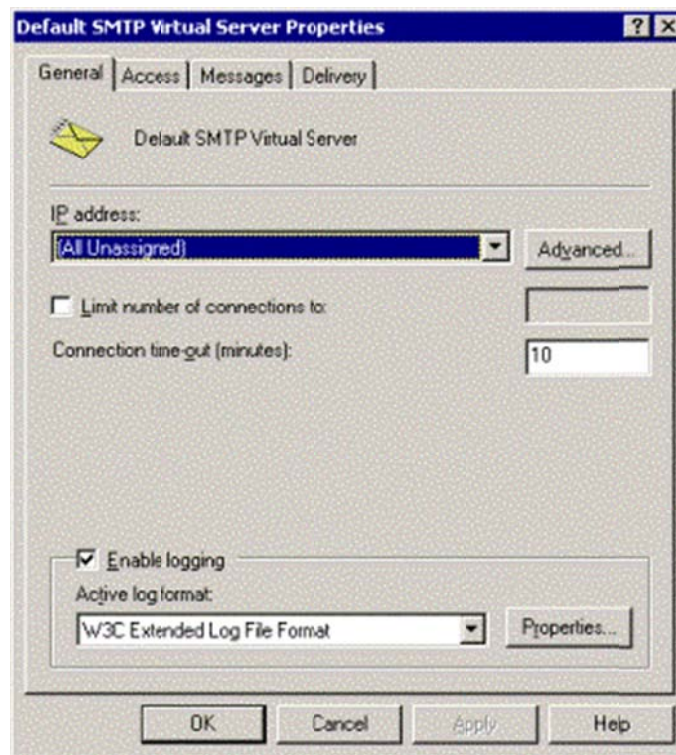


Logging the SMTP Service

Amit Zinman

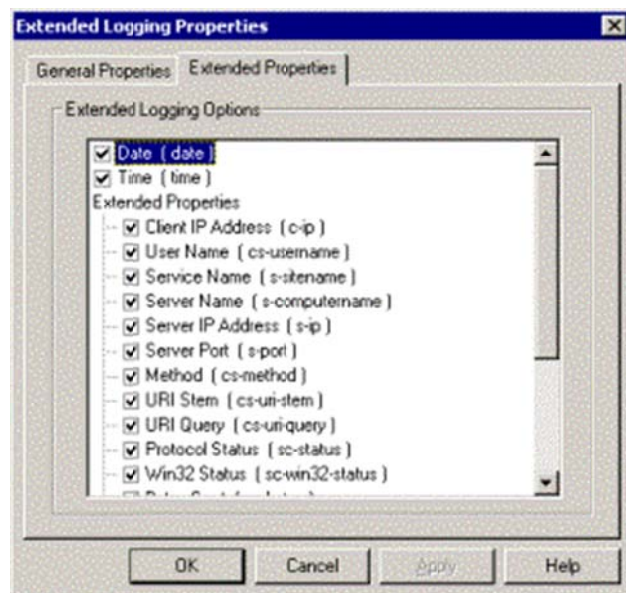
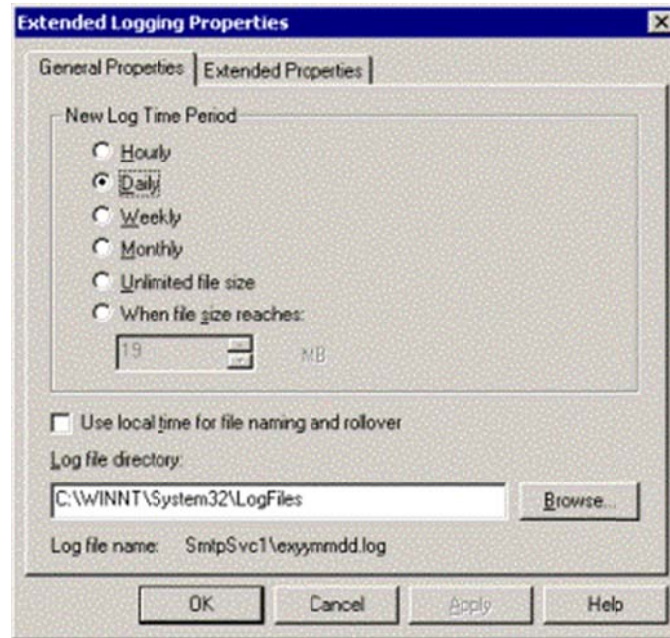
In Exchange 5.5, logging could be done using the Event Viewer. Thankfully, SMTP logging is now provided by IIS, the foundation to Exchange 2000/3 is now separate and writes the information to regular text-based log files. It can also write the log files to a SQL database using ODBC allowing integration of SMTP logging and general monitoring software.

To enable logging go to the SMTP virtual service property page General tab.



Logging the SMTP Service

Amit Zinman

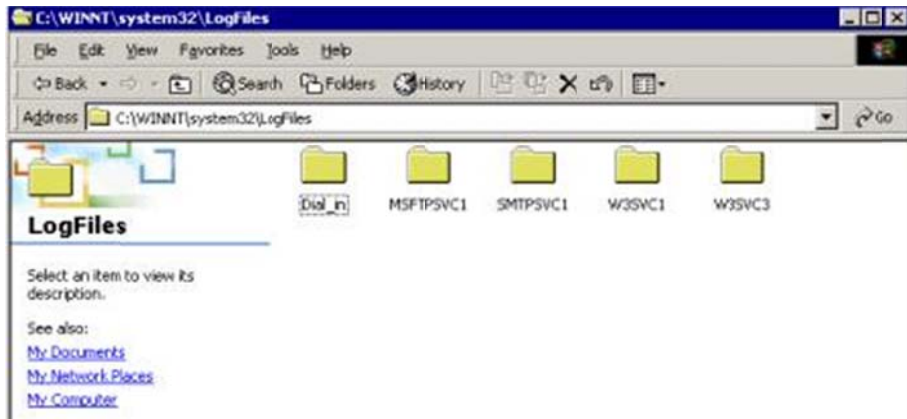


The logging as can be seen in these screen shots is general and intended also for protocols other than SMTP.

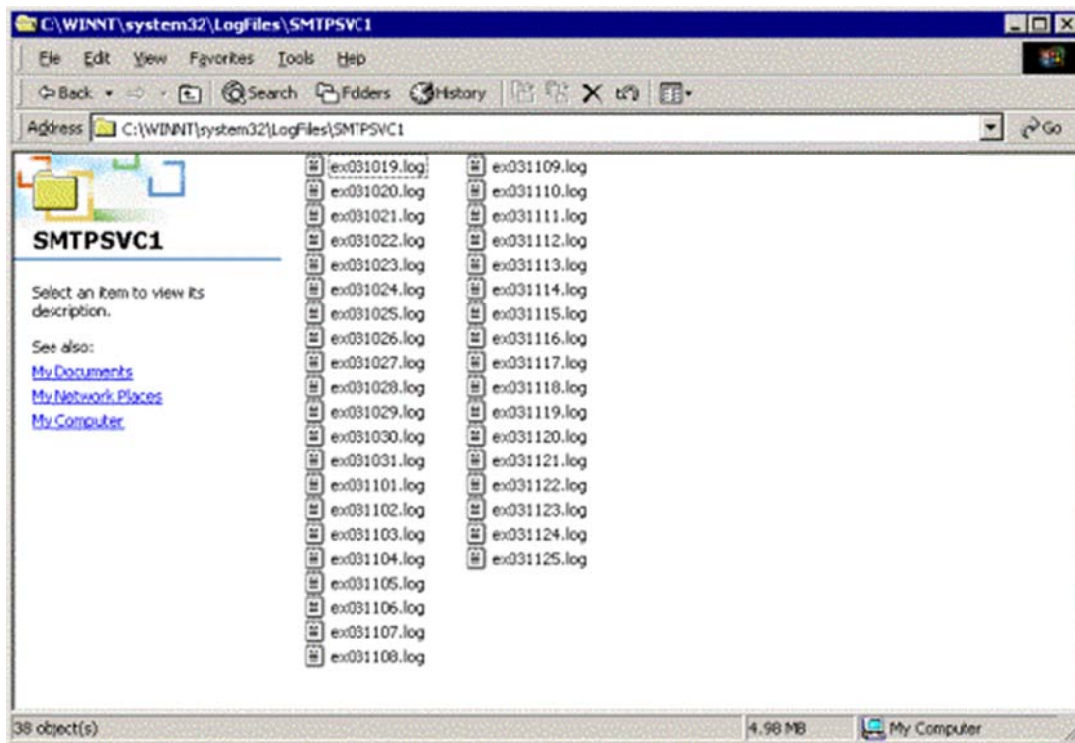
The log files are typically located under %systemroot%\system32\logfiles.

Logging the SMTP Service

Amit Zinman



As you can see from this screenshot my server logs all kinds of IIS activity. The Exchange log files are located under the SMTPSVC1 directory. The default file names for these logs include the date of creation.

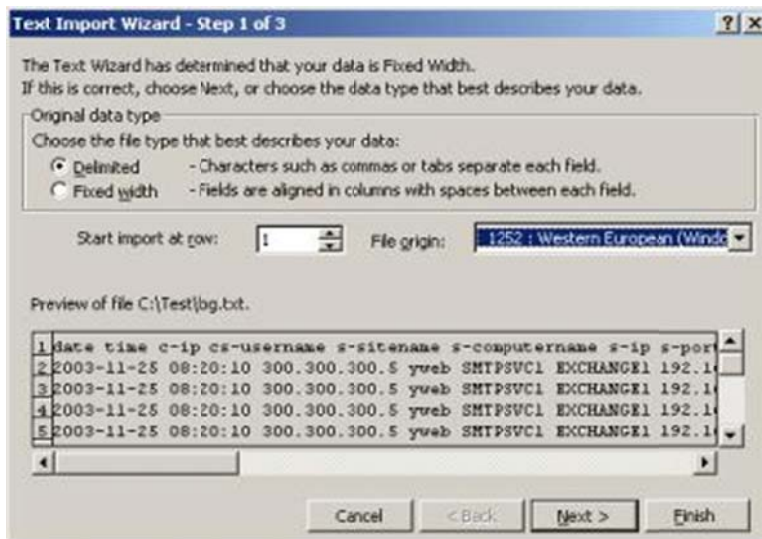
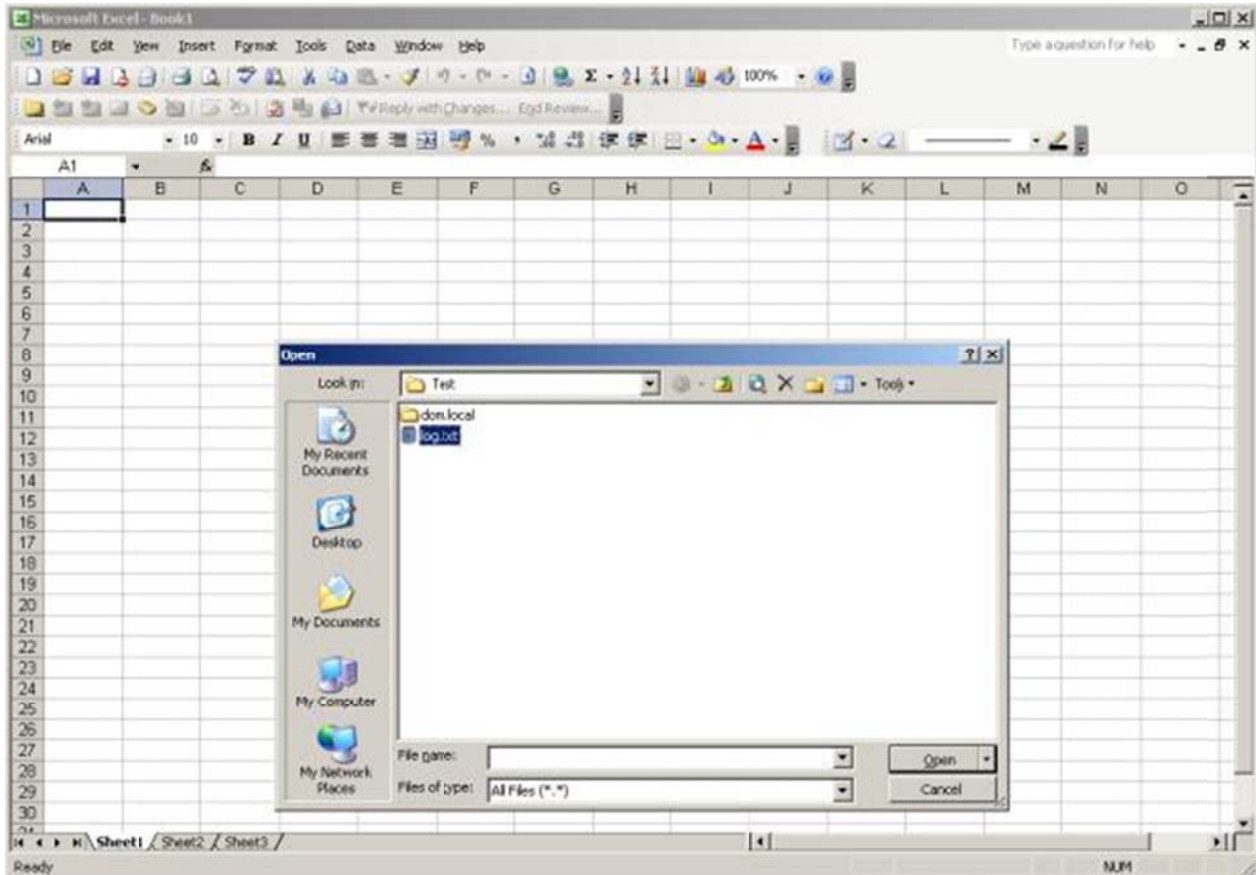


A typical log file would look like this:

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2003-11-25 08:20:10
#Fields: date time c-ip cs-username s-sitename s-computername s-ip s-port cs-
method cs-uri-stem cs-uri-query sc-status sc-win32-status sc-bytes cs-bytes
time-taken cs-version cs-host cs(User-Agent) cs(Cookie) cs(Referer)
2003-11-25 08:20:10 300.300.300.5 yweb SMTPSVC1 EXCHANGE1 192.168.1.100 0 EHLO -
+yweb 250 0 325 13 60 SMTP - - - -
2003-11-25 08:20:10 300.300.300.5 yweb SMTPSVC1 EXCHANGE1 192.168.1.100 0 MAIL -
```


Logging the SMTP Service

Amit Zinman



Logging the SMTP Service

Amit Zinman



Microsoft Excel - log.txt

	B	C	D	E	F	G	H	I	J
1	time	c-ip	cs-username	cs-method	cs-uri-query	sc-status	sc-bytes	cs-bytes	time-taken
2	08:20:10	300.300.300.5	yweb	EHLO	#NAME?	250	325	13	60
3	08:20:10	300.300.300.5	yweb	MAIL	+FROM:<nfcnews@hohohot.com>	250	46	33	20
4	08:20:10	300.300.300.5	yweb	RCPT	+TO:<dank@domain.com>	250	31	28	10
5	08:20:10	300.300.300.5	yweb	BDAT	+<YWEBWgtc2S6AAT0000b0ae@yweb>	250	76	101761	831
6	08:20:11	300.300.300.5	yweb	QUIT	yweb	240	66	4	0
7	08:22:17	100.100.100.5	OutboundConnectionResponse	-	220+mail.elpelp.com+SMTP,+Tue,+25+No	0	57	0	10665
8	08:22:17	100.100.100.5	OutboundConnectionCommand	EHLO	EXCHANGE1.domain.local	0	4	0	10665
9	08:22:17	100.100.100.5	OutboundConnectionResponse	-	250+mail.elpelp.com+Hello	0	25	0	10665
10	08:22:17	100.100.100.5	OutboundConnectionCommand	MAIL	FROM<haya@domain.com>	0	4	0	10826
11	08:22:17	100.100.100.5	OutboundConnectionResponse	-	250+<haya@domain.com>...+Sender+ok	0	37	0	10965
12	08:22:17	100.100.100.5	OutboundConnectionCommand	RCPT	TO:<zolpzolp@elpelp.com>	0	4	0	10965
13	08:22:17	100.100.100.5	OutboundConnectionResponse	-	250+<zolpzolp@elpelp.com>...+Recipient-	0	41	0	11005
14	08:22:17	100.100.100.5	OutboundConnectionCommand	DATA	-	0	4	0	11025
15	08:22:17	100.100.100.5	OutboundConnectionResponse	-	364+Enter+mail,+end+with+",""+on+a+line+by	0	48	0	11055
16	08:25:12	200.200.200.5	relay.mepmepmep.co.il	EHLO	-	324	0	SMTP	-

I've deleted some columns that are repetitive such as the Exchange server name and IP address, and the port used. What's left is the time that the connection was made, the IP address of the mail server from which the connection was made, the SMTP command also called verb), how many bytes were transferred and the time it took (in milliseconds).

Once the information is in Excel it is easier to view the information and use it to find out how much mail is coming in and out, who mails you the most (in some cases these is might not be friendly people) and you can be sure that you a certain mail item, even if a user or some virus protection program deleted this item.