

IBM ITSO Poughkeepsie
OS/390 in an e-business environment

**Logging, Reporting and
Accounting**



Roland Trauner
trauner@us.ibm.com

Logging, Reporting and Accounting



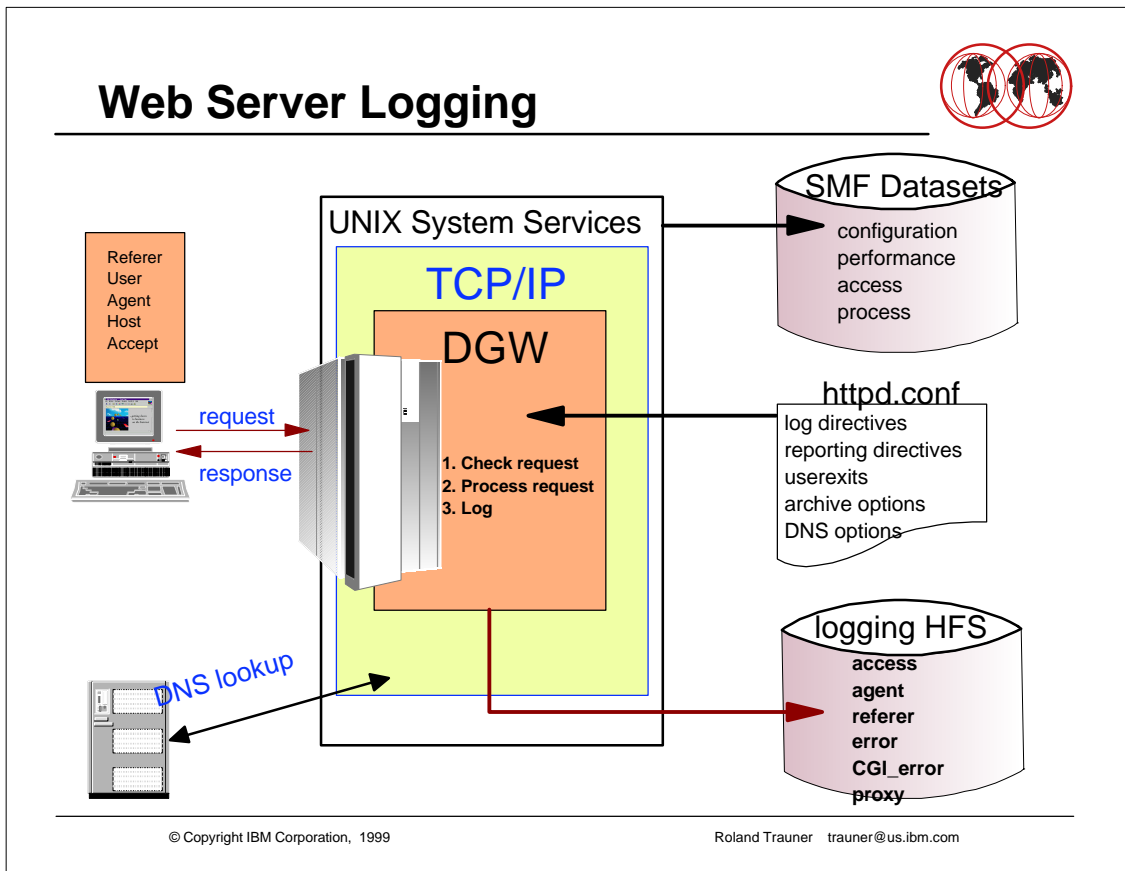
- **Logging**
- **Tracing**
- **Reporting**
- **Monitoring**
- **SMF Recording**

Web Server Logging



- **Where to find web server logging information?**

- ▶ Web server log files
- ▶ Syslog (especially security - RACF related messages)
- ▶ UNIX syslogd (TCP/IP information)
- ▶ SMF data (security and performance data)



Web Server Logging



- **Web Server Log Files**

- **Log file advantages**

- ▶ Useful to determine problems
- ▶ Input for Reporting Tools
- ▶ help to improve the web server
- ▶ find out "whats going on"

- **Log file disadvantages**

- ▶ Performance degradation
- ▶ If the HFS of the logs is full, web server slows down and uses up every available CPU
- ▶ If log HFS is full, you might not even be able to start the server

Web Server Logging



● Access Log

- ▶ AccessLog /web/apple/logs/httpd-log
- ▶ Main log file, records details about every request to the web server
- ▶ Format: NCF --- NCSA common log format (if LogFormat Common)
 - NCF is used by most web analysis tools
- ▶ Contains:
 - IP address or IP name of requester
 - Authenticated User or -
 - Date & Time (local server time)
 - Difference to GMT
 - Request string, request method and protocol
 - Return code of the request
 - 1xx Informational
 - 2xx Success
 - 3xx Redirection
 - 4xx Client Error
 - 5xx Server Error
 - File Size

Web Server Logging



● Agent Log

- ▶ AgentLog /web/apple/logs/agent-log
- ▶ Logs which web browser was used to access the web server
- ▶ Examples:
 - Mozilla/4.04 [en] (Win95; U) Netscape Communicator 4.04 US
 - Mozilla/4.05 [en] (Win95; I) Netscape Communicator 4.05 Internatl.
 - Microsoft Internet Explorer/4.40
 - HotJava/1.1.2 FCS

Web Server Logging



- **Cache Access Log**

- ▶ AgentLog /web/apple/logs/httpd-proxy
- ▶ Similar to the Access Log when using DGW as a Proxy Server
- ▶ Logs all requests for files served out of the proxy server's cache

- **CGI error log**

- ▶ CgiErrorLog /web/apple/logs/cgi-error
- ▶ All CGI output to stderr is logged here

Web Server Logging



● Error Log

- ▶ ErrorLog /web/apple/logs/httpd-errors
- ▶ Authentication errors, timeout and access problems are reported here
- ▶ The ErrorLog also contains information about start and restart of the webserver

▶ Examples:

```
-[23/Jan/1999:10:51:19 +0500] SIGHUP caught - waiting for threads to drain.  
-[23/Jan/1999:10:51:20 +0500] IMW0098E Restart succeeded.  
-[23/Jan/1999:10:51:20 +0500] IMW0235I Server is ready.  
-[23/Jan/1999:11:05:49 +0500] [IMW0194I OK-GATEWAY] [host: 9.12.2.145  
referer: http://virtualairport.lufthansa.com/english/mm/mm_0.htm] IMW2000E  
Proxy Error: Host name not recognized or host not found.  
-IBM WebSphere Application Server native plugin is shutting down :-(  
-IBM WebSphere Application Server native plugin initialization went OK :-)  
-[21/Jan/1999:13:37:18 +0500] Persist timer expired while waiting on client  
9.12.14.107  
-[28/Dec/1998:05:14:05 +0500] [IMW0196I NOT AUTHENTICATED] [host:  
9.184.167.64 referer: https://9.12.2.22:443/] /secl/secl.html  
-[19/Jan/1999:21:40:23 +0500] SSL support initialization failed, server will  
run only in non-secure mode without listening on ssl port
```

Web Server Logging



- **Proxy Access Log**

- ▶ `ProxyAccessLog /web/apple/logs/httpd-proxy`
- ▶ Logs requests through the proxy server excluding the ones that are served out of the proxy cache

- **Referer Log**

- ▶ `RefererLog /web/apple/logs/referer-log`
- ▶ Identifies the web page that referred (or linked to) the requested web page
- ▶ Helpful to identify misleading links
- ▶ Helpful to see "who is referring to me"

Web Server Logging



● Trace Log

- ▶ TraceLog /web/apple/logs/Trace-log
- ▶ Logs all trace data according to trace levels (-v -vv -mtv)
- ▶ If there is no TraceLog directive in httpd.conf, the trace data will be written to the SYSOUT DD of the web server started procedure
- ▶ Caution:
 - Use tracing only when necessary because it degrades the web server performance
 - Avoid tracing to HFS (another performance degradation)
 - No documentation about trace entries available

Logging, Reporting and Accounting



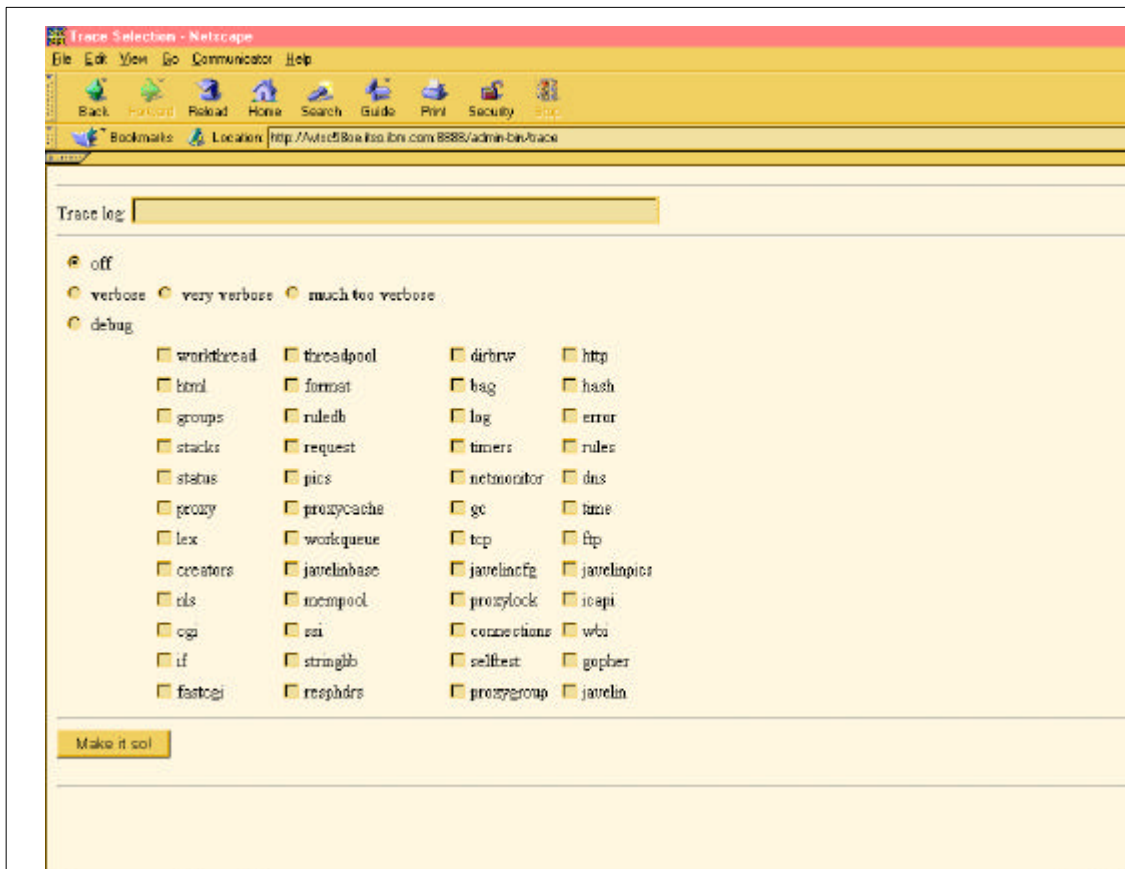
- Logging
- Tracing
- Reporting
- Monitoring
- SMF Recording

Tracing



● Tracing:

- ▶ Use -v -vv or -mtv option in the web server started procedure
 - Problem: Web server restart needed to enable changes in started procedure
- ▶ Use a command: F WEBAPPLE,appl=-v (-vv -mtv)
 - Problem: Command to start - no command to stop
- ▶ Use the trace service: /admin-bin/trace
 - Service statement needs to be activated in httpd.conf:
 - `service /admin-bin/trace* INTERNAL:TraceFn`
 - Allows to start and stop traces
 - Allows to debug special occasions



- ▶ Interactive ADMIN Trace Service
- ▶ Allows to start tracing -verbose -vv and -mtv and also to switch it off again what is not possible using the commands.
- ▶ It also allow to debug the components like proxy and proxycache



Tracing -vv trace

```
Client sez.. GET / HTTP/1.0
WorkQueue... no matching ApplEnv found, keeping work in current process.
Protocol version... 1.0
Client sez.. Host: 9.12.2.22:8700
Host..... 9.12.2.22
Client sez.. If-Modified-Since: Thu, 21 Jan 1999 17:06:55 GMT
Format..... Wkd, 00 Mon 0000 00:00:00 GMT
TimeZone.... 05 hours from GMT
Time string. Thu, 21 Jan 1999 17:06:55 GMT; offset = 0 seconds
Parsed..... to 916938415 seconds, Thu Jan 21 12:06:55 1999

Give only... if modified since (localtime) Thu Jan 21 12:06:55 1999
Client sez.. Pragma: no-cache
Pragma..... no-cache (force refresh)
Client sez.. Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,

Accept..... image/gif (q=1.00,mbx=0.0,mxs=0.0)
Accept..... image/x-xbitmap (q=1.00,mbx=0.0,mxs=0.0)
Accept..... image/jpeg (q=1.00,mbx=0.0,mxs=0.0)
Accept..... image/pjpeg (q=1.00,mbx=0.0,mxs=0.0)
Accept..... image/png (q=1.00,mbx=0.0,mxs=0.0)
Accept..... */* (q=1.00,mbx=0.0,mxs=0.0)
Client sez.. Accept-Language: en
Language.... en (q=1.00)
Client sez.. Accept-Charset: iso-8859-1,*,utf-8
Charset..... iso-8859-1 (q=1.00)
Charset..... * (q=1.00)
Charset..... utf-8 (q=1.00)
Client sez.. Via: HTTP/1.0 wtsc58oe.itso.ibm.com (Domino-Go-Webserver)
Client sez.. User-Agent: Mozilla/4.04 en (Win95; U)
User-Agent.. Mozilla/4.04 en (Win95; U)
HTSimplify.. simplifying '/'
HTSimplify.. nothing to do!
About..... to call preexit for "/.
CpConv..... converter NOT opened
CpConv..... converter NOT opened.
Using local address 9.12.2.22.
Protect..... /Docs/admin-bin/* did NOT match /.
```

Logging, Reporting and Accounting



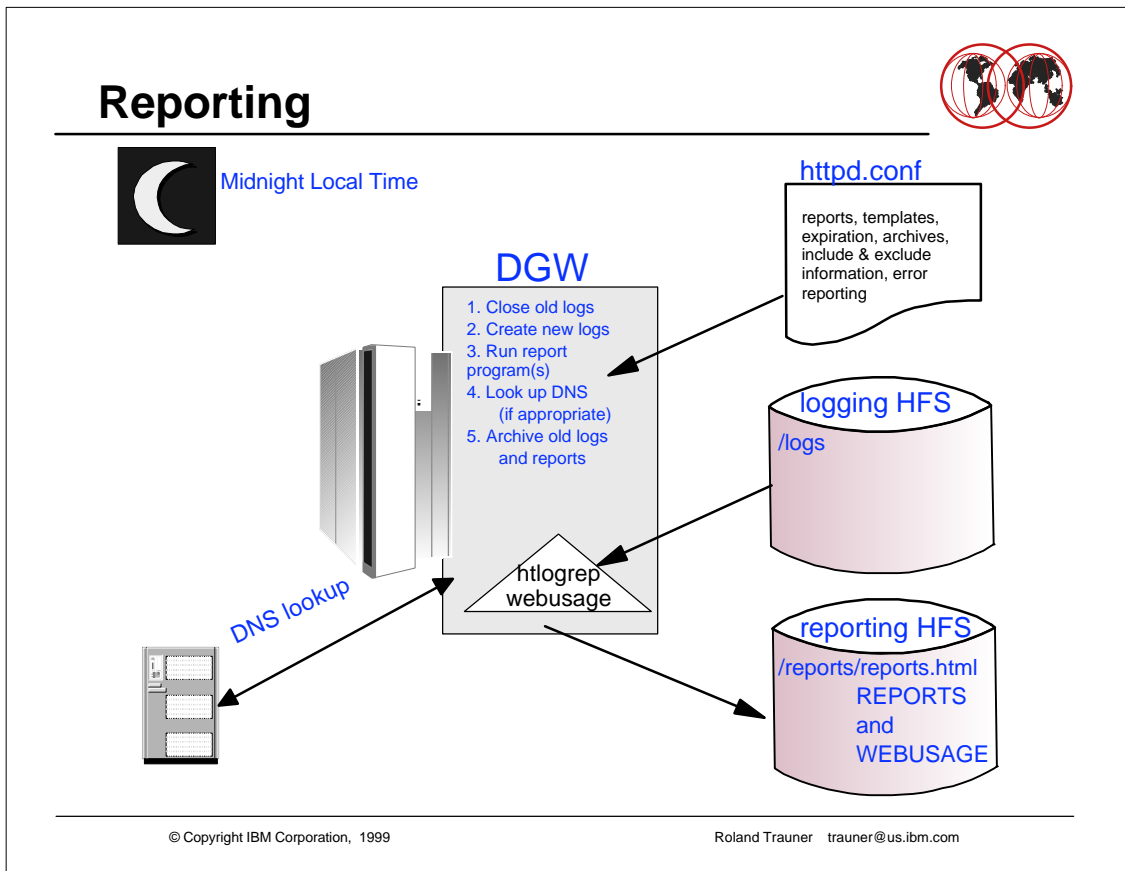
- Logging
- Tracing
- **Reporting**
- Monitoring
- SMF Recording

Reporting



- **DGW automatic report generation and log processing**

- ▶ Each midnight local time, logs are closed and new ones created
 - Midnight local time is a fixed time --- no way to change
- ▶ DNS lookups are created if `AccessReportDoDnsLookup` is activated
- ▶ Reports are created according to configuration directives
- ▶ Housekeeping of logs and reports will be processed




Reporting



- **DGW delivers 2 standard reporting tools:**

- ▶ htlogrep
 - technical oriented. For the webmaster to optimize the server
 - shows transfer counts, errors, hostnames etc.
 - Java applet - requires JVM 1.1.4 (or higher) enabled browser
- ▶ webusage
 - marketing oriented. Prove of the web content



Reporting

Template Load Panel

Template to Use: AccessStats Reload

Template Control Panel

Template: AccessStats
 Template Reports: URL Reports
 Initial Date: 5/20/98 6:18 AM
 Display

End Date: 1/11/99 6:53 AM

Template Description

Server access statistics

Template Data


URL's	Count	Bytes Xferred
/clearpixel.gif	938	22532
/	266	759278
/FISHREXX/GWAPI.RX/parml/parm2/parm3	258	881335
/reports/reports.html	253	102456
/admin-bin/webexec/cfgstart.html	246	325789
/SweetBackground.gif	211	226369
/BuiltByNOF.gif	175	147963
/LINKS_SweetButton.gif	144	472056
/FTP_SweetButton.gif	142	421452
/DGW-FISH_SweetButton0n.gif	131	392739
Total	Count: 8082	Bytes Xferred: 380221590

© Copyright IBM Corporation, 1999
Roland Trauner trauner@us.ibm.com

h
t
t
l
o
g
r
e
p

- ▶ HTLOGREP Example
- ▶ Shows server access statistics based on URL Reports
- ▶ Count of the most accessed item and how many bytes were transferred for it.

htlogrep details



Template <AccessStats> Report for </Admin/lotus(r).gif> URL from: 5/20/98 6:18 AM to: 1/11/99...

Url: </Admin/lotus(r).gif> for Template <AccessStats>

URL	Date	Bytes Xferred
socks5.raleigh.ibm.com	1/11/99 5:53 AM	1120
socks5.raleigh.ibm.com	8/15/98 4:08 PM	1120
socks5.raleigh.ibm.com	8/15/98 4:29 PM	0
socks5.raleigh.ibm.com	8/15/98 8:27 PM	0
socks5.raleigh.ibm.com	8/15/98 8:29 PM	0
socks5.raleigh.ibm.com	8/27/98 5:28 AM	1120
socks5.raleigh.ibm.com	8/27/98 5:32 AM	1120
socks5.raleigh.ibm.com	8/27/98 7:30 AM	1120
socks5.raleigh.ibm.com	8/27/98 12:18 PM	1120
socks5.raleigh.ibm.com	8/27/98 12:46 PM	1120
socks5.raleigh.ibm.com	9/18/98 7:00 AM	1120
ns.hamburg.de.ibm.com	6/22/98 7:13 AM	1108
ns.hamburg.de.ibm.com	6/22/98 8:31 AM	0
ns.hamburg.de.ibm.com	6/22/98 9:51 AM	1108
ns.hamburg.de.ibm.com	6/22/98 12:48 PM	1108

Total Bytes: 20040

Exit

Unsigned Java Applet Window

© Copyright IBM Corporation, 1999

Roland Trauner trauner@us.ibm.com

- ▶ HTLOGREP Details: One item have been accessed by whom and when

The screenshot shows a Netscape browser window with the title "Lotus Domino Go Webserver Logging Reports - Netscape". The address bar shows "http://93.12.2.22.8600/reports/reports.html". The page content includes a "Template Description" section, a "Template Data" table, and several links for further analysis.

URL's	Count	Bytes Xferred
/clearpixel.gif	938	22532
/	266	750278
/VISHREDDO/GWAPI.FX/param/param3	250	601335
/reports/reports.html	253	102488
/admin-bin/webexec/objstart.html	240	325709
/SweetBackground.gif	211	226369
/BuiltbyWUM.gif	175	147963
/LINK3_SweetButton.gif	144	472056
/FTF_SweetButton.gif	143	421452
/DOW-FIRE_SweetButton0a.gif	131	392739
Total	Count: 3082	Bytes Xferred: 380221590

Links at the bottom of the page:

- [Top10 WUM](#) --- Webusage Mining Reports for Template Top10
- [Top50 WUM](#) --- Webusage Mining Reports for Template Top50
- [400Errors WUM](#) --- Webusage Mining Reports for Template 400Errors
- [NoGifs WUM](#) --- Webusage Mining Reports for Template NoGifs
- [AccessStats WUM](#) --- Webusage Mining Reports for Template AccessStats



h
t
l
o
g
r
e
p
c
a
l
l
W
U
M

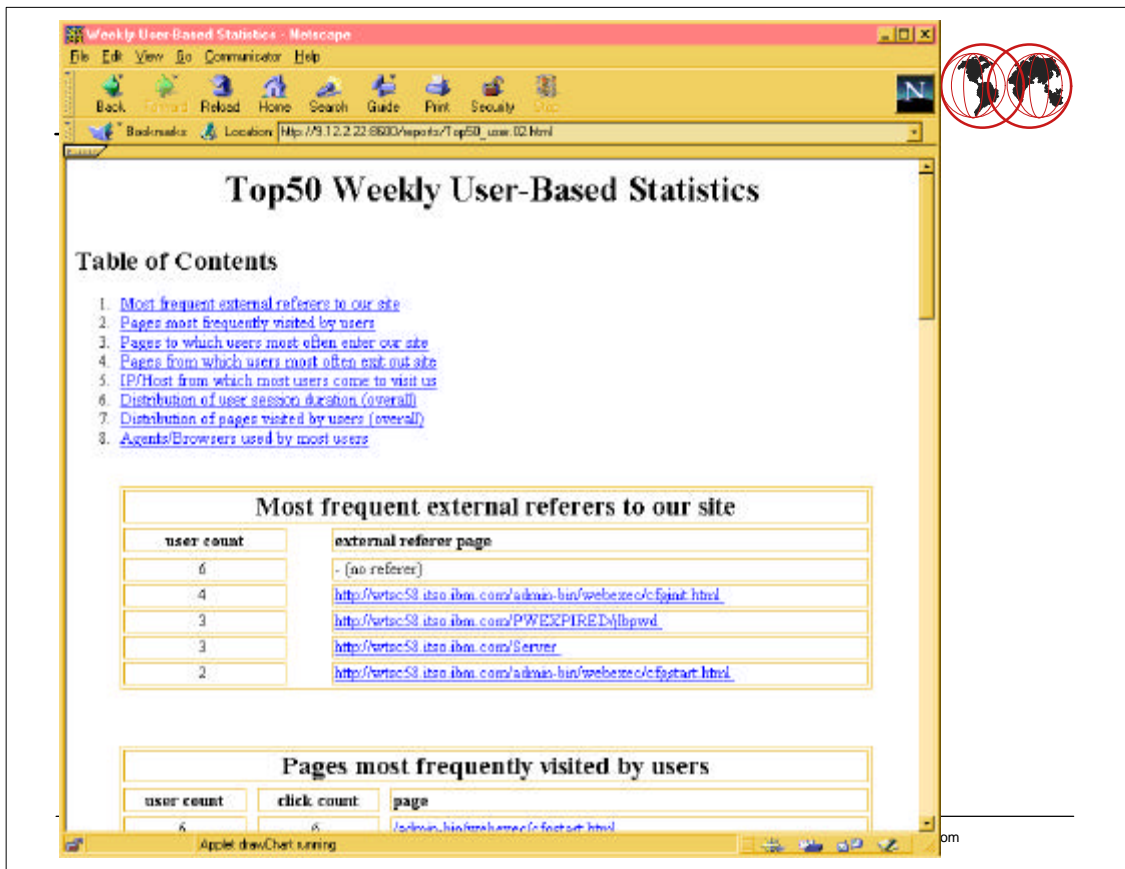
- ▶ Bottom of HTLOGREP page enables a link to WUM Reports
- ▶ Top10WUM --- Webusage Mining for Template Top10
- ▶ Top50WUM
- ▶ 400Errors WUM
- ▶ NoGifs WUM
- ▶ AccessStats WUM

Reporting - Web Usage Mining



- **WUM is a more marketing oriented report to verify the acceptance of the web server content**

- ▶ User based reports
 - Most frequent external referers to our site
 - Pages most frequently visited by users
 - Pages to which users most often enter our site
 - Pages from which users most often exit our site
 - Distribution of user session duration (overall)
 - Distribution of pages visited by users (overall)
 - Agents/browsers used by most users
- ▶ Path based reports
 - Most frequently visited paths with 1 link or n links
- ▶ Group based reports
 - Most frequently visited groups consisting of 2 or more pages



- ▶ Top50 Weekly User-Based Statistics
- ▶ Most frequent external referers to our site
- ▶ Pages most frequently visited by users
- ▶ Pages to which users most often enter our site
- ▶ IP/Host from which most users come to visit us
- ▶ Distribution of user session duration (overall)
- ▶ Distribution of pages visited by users (overall)
- ▶ Agents/Browsers used by most users
- ▶

Reporting



- **Do your own reporting**

- ▶ If you like to include other reporting programs into the automatic midnight processing, you will need to write a small support program:

- ▶ **Example:** REXX exec called logexit.rexx

```
/* REXX */
confvar = '_CEE_ENVFILE'
confval = 'n/a'
do n = 1 to __environment.0
  parse var __environment.n varname '=' confval
  if varname = confvar then signal FOUND
end
NOTFOUND:
say 'Variable' confvar 'is not set. Logexit aborted'
exit 999
FOUND:
'htlogrep -c' confval
'webusage -c' confval
exit
```

- ▶ **Activate it:** define httpd.conf

```
LoggingReportingProgram /web/apple/logexit.rexx
```

Reporting



● Other Reporting Tools

- ▶ There are several other reporting tools available
 - See:
http://dir.yahoo.com/Computers_and_Internet/Software/Internet/World_Wide_Web/Servers/Log_Analysis_Tools/
- ▶ You may select a tool written in PERL and port it to OS/390
 - Example: <http://www.ics.uci.edu/pub/websoft/wwwstat/>
 - wwwstat is a nice log statistic tool
 - Freeware from the University of California



Reporting --- Port wwwstat



● How to port wwwstat

- ▶ Use a **PERL** interpreter for OS/390
 - <http://www.mks.com/s390/gnu>
- ▶ Put it into a HFS like `/usr/lpp/perl/source/perl5.trz`
- ▶ Unpack the archive file to another directory like `/usr/lpp/perl/bin`
 - use the `tar -xzf perl5.trz` command
- ▶ Add `/usr/lpp/perl/bin` to the end of the path statement of `httpd_envvars`
- ▶ Get the log analyzer and put it into another HFS like `/usr/lpp/wwwstat/source/wwwstat-2.0.tar.gz`
 - Since the file is gzipped, you might need another utility to unzip the file
 - Get **gzip** from <http://www.s390.ibm.com/oe>
- ▶ Unzip the file to the same source directory
- ▶ Untar the file to `/usr/lpp/wwwstat/bin`
 - `pax -o from=ISO8895-1,to=IBM-1047 -rf wwwstat.tar`
- ▶ Read the **INSTALL** documentation or get the **wwwstat** handbook out of their web site.

Reporting --- Port wwwstat cont.



● How to port wwwstat - cont.

- ▶ Install the log analyzer according to its installation guidelines
- ▶ Edit the code --- insert the following 2 lines before the first line of the original code:

```
eval 'exec perl -S $0 ${1+"$@"}'      <-- add this
if 0;                                <-- add this
# =====
$Version = 'wwwstat-2.0';
#
# Copyright (c) 1994, 1996 Regents of the University of California.
#
```

- ▶ Start this analyzer manually --- or let DGW do it automatically at night
- ▶ For the automatic: See the LoggingReportingProgram definition
- ▶ Manually: Add a html link to your administrator homepage like the following example:

```
<form action="/perl/wwwstat.perl" METHOD="POST">
```

Reporting --- Port wwwstat cont.



- **How to port wwwstat - cont.**
 - ▶ There is a little more you need to do.
 - ▶ Most web servers (including Apache) are keeping only one logfile. This means that most freeware log analyzers omit to scan the directory.
 - ▶ This means a little more programming --- a nice little REXX clist will do.
- **Don't worry about all this freeware etc.**
- **We're doing UNIX now - remember ?**

Logging, Reporting and Accounting



- Logging
- Tracing
- Reporting
- **Monitoring**
- SMF Recording

Monitoring

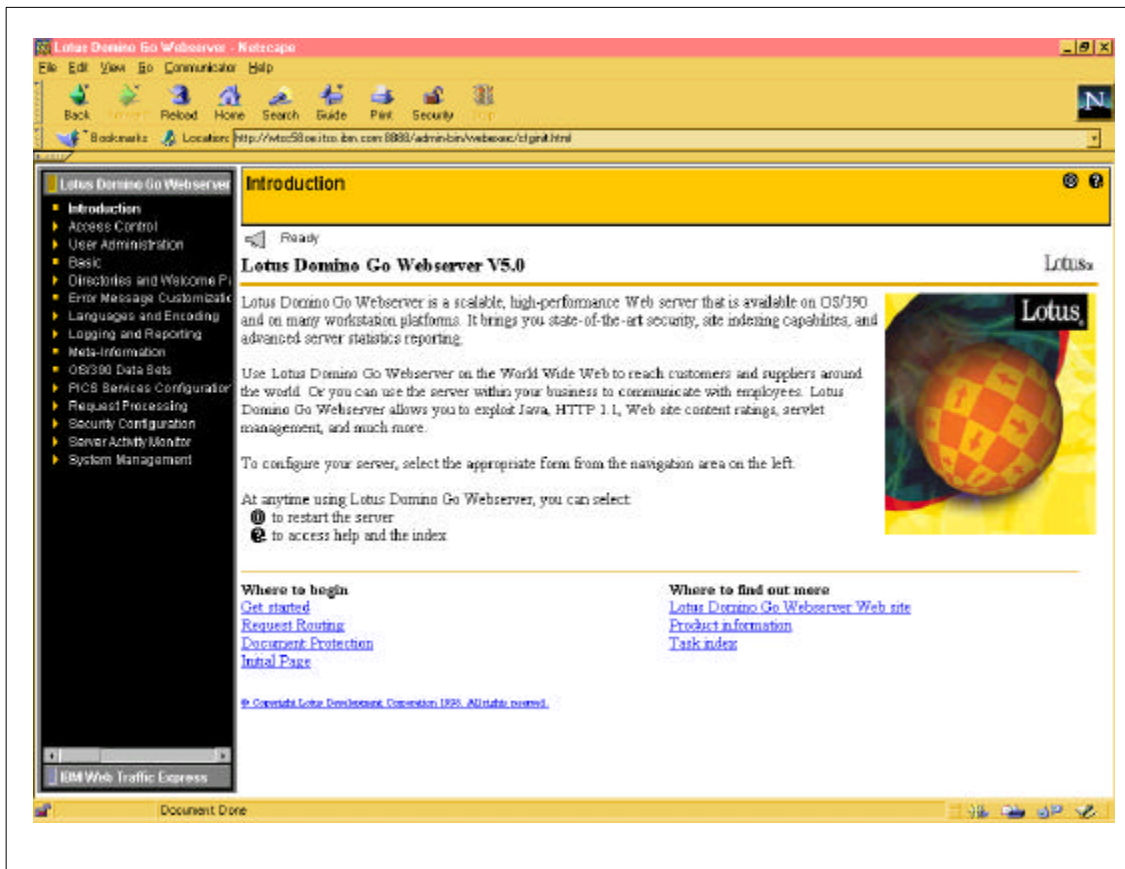


- **Domino Go Webserver allows to do snapshots of web server events**
 - ▶ Monitor the web server activity
 -/Usage/Initial
 - ▶ Monitor the proxy activity
 -/Usage/proxylog
 - ▶ Browse the access log dynamically
 -/Usage/Logs
 - ▶ Monitor the Network statistic
 -/Usage/Netstat
 - ▶ Monitor the proxy cache
 -/Usage/Cache
 - ▶ Monitor the garbage collection
 -/Usage/gcsmry

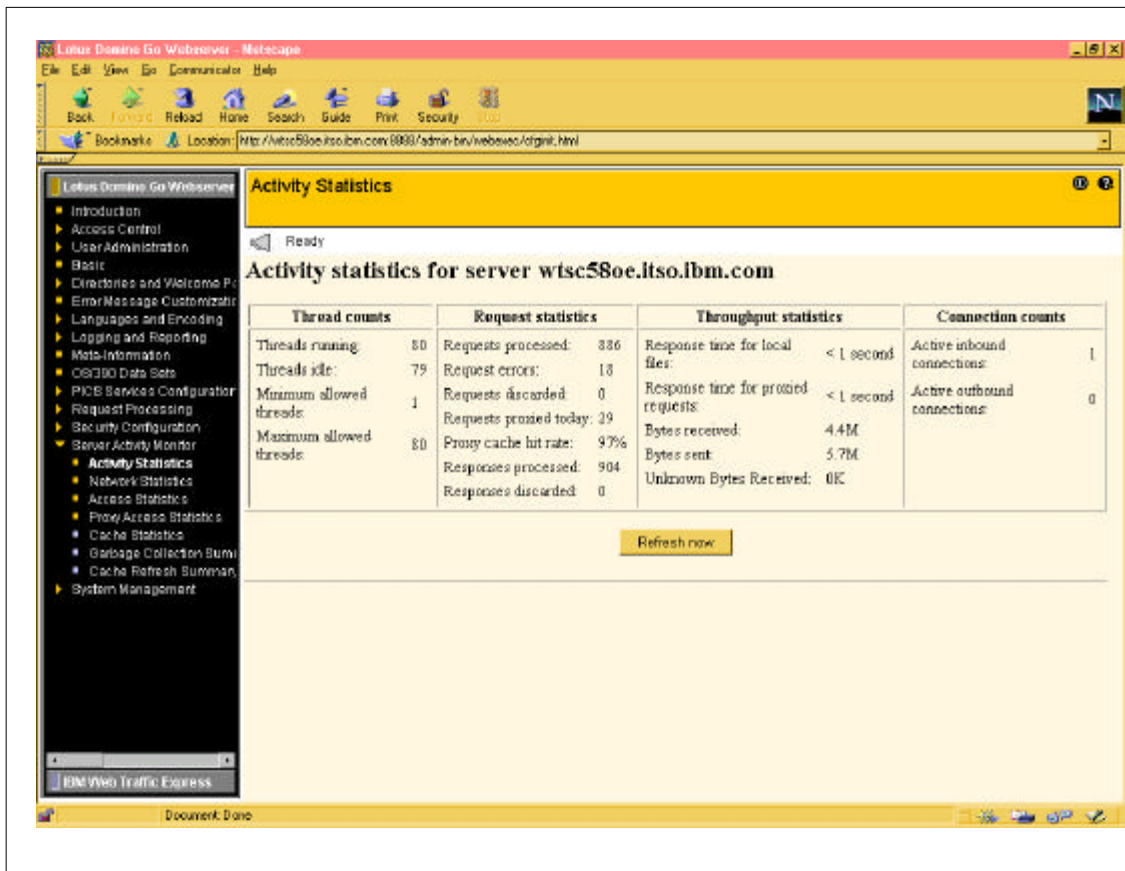
Monitoring



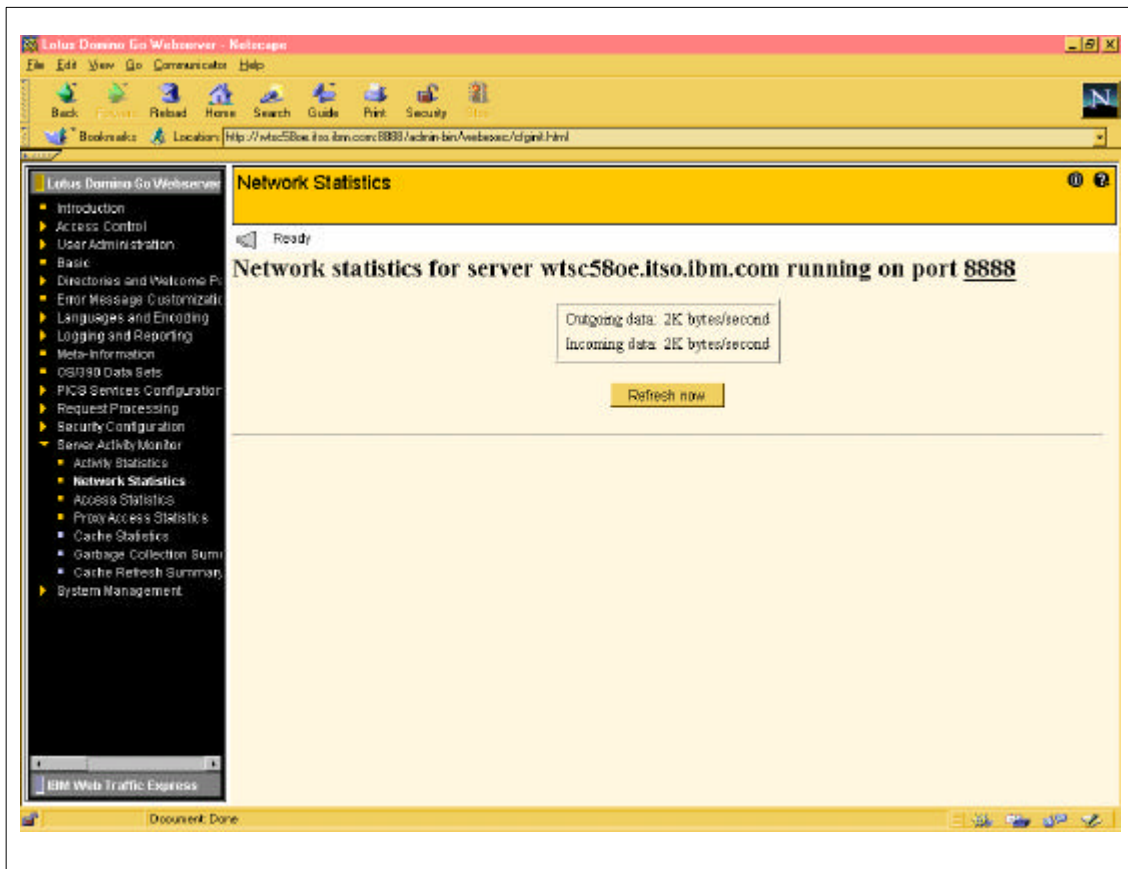
- **Use the server Administration Forms to monitor the system or create your own Admin homepage**
 - ▶/admin-bin/webexec/cfginit.html
- **Be sure to have the monitor activated (httpd.conf)**
 - ▶ service /Usage* INTERNAL:UsageFn



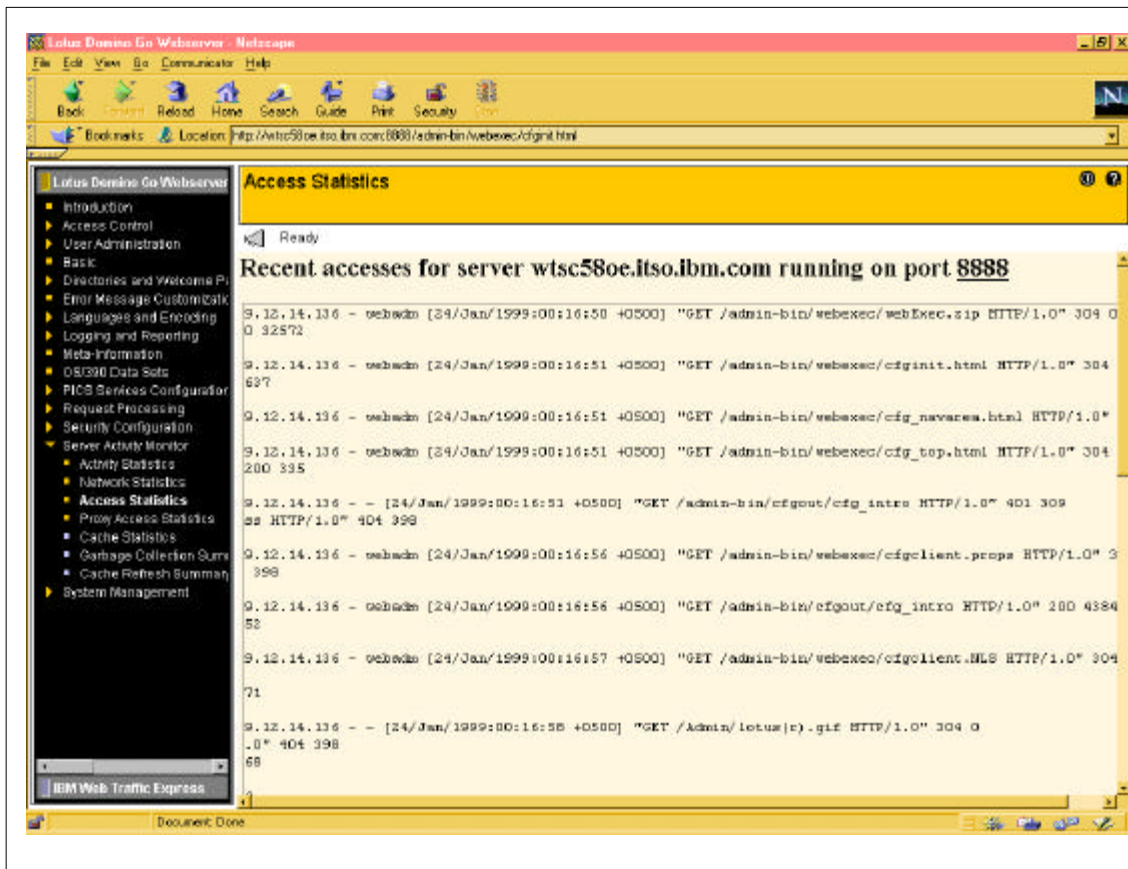
► Admin Interface Main Configuration Page



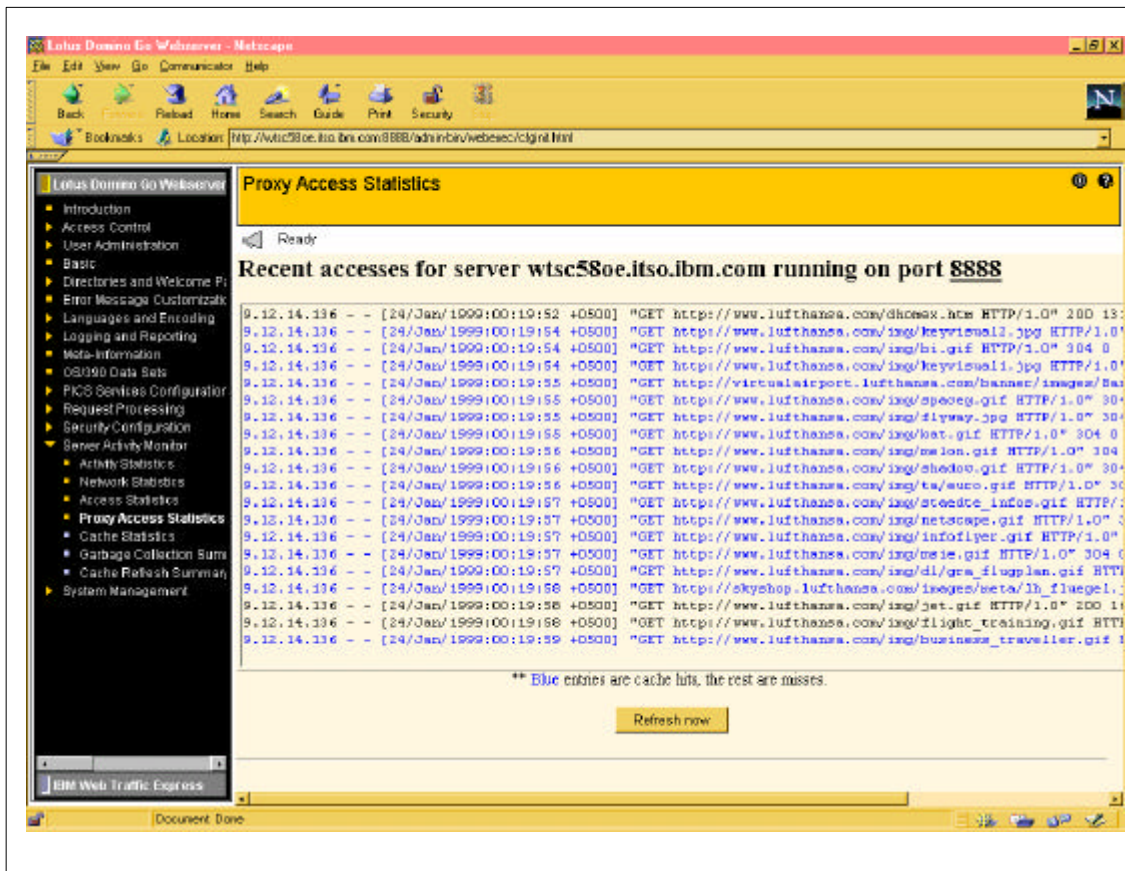
- ▶ Activity Statistics
- ▶ Thread counts
- ▶ Request statistics
- ▶ Throughput statistics
- ▶ Connection counts



- ▶ Network Statistics
- ▶ Incoming and outgoing data bytes/second



► Browse recent access log



► Recent PROXY access statistics

Cache Statistics

Ready

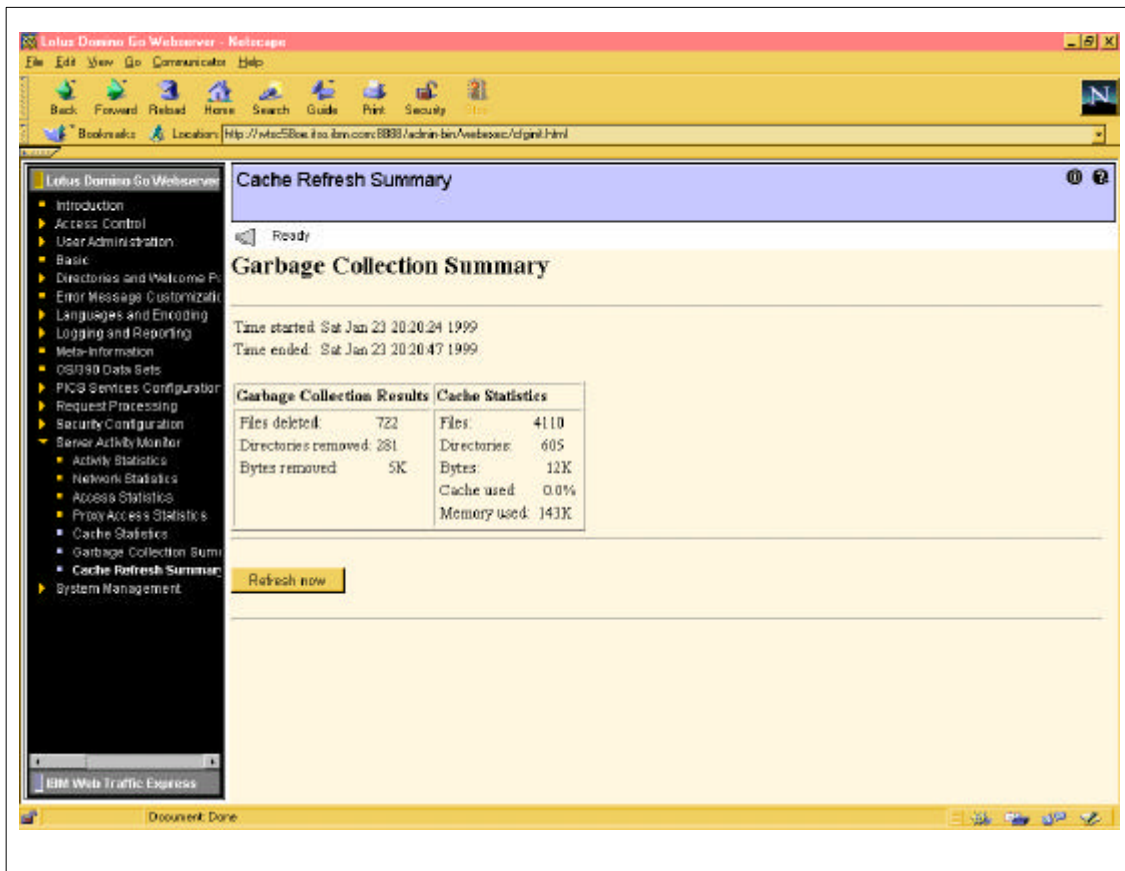
Cache operational

The proxy cache is in normal operation.

The cache is managed as 17 subcaches. The following table shows how much content is in each subcache:

Table	Content Bytes	Number of Files	Index size
0	188K	39	5K
1	196K	37	5K
2	292K	50	7K
3	324K	46	6K
4	260K	39	5K
5	266K	48	6K
6	228K	36	5K
7	316K	49	6K
8	346K	53	7K
9	256K	42	5K
10	224K	39	5K
11	256K	40	5K
12	264K	42	5K
13	812K	38	5K
14	260K	43	6K
15	256K	40	5K
16	360K	54	7K

► Proxy cache stats



- ▶ Cache refresh summary (garbage collection)

Logging, Reporting and Accounting



- Logging
- Tracing
- Reporting
- Monitoring
- SMF Recording

SMF Recording



- **DGW configuration and performance data can be written to SMF (Record 103)**
- **RACF writes audit records for UNIX events to SMF (Record 80)**
 - ▶ Directory searches DIRSRCH
 - ▶ Directory access check DIRACC
 - ▶ File and directory checks FSOBJ
 - ▶ Filesystem security changes FSSEC
 - ▶ Object access IPCOBJ
 - ▶ Change to UIDs and GIDs of processes PROCESS
 - ▶ Access other processes PROCACT
 - Needs to be activated
 - Example: SETR LOGOPTIONS(FAILURES(DIRSRCH,DIRACC)) and SETR
AUDIT(FSOBJ,PROCESS)

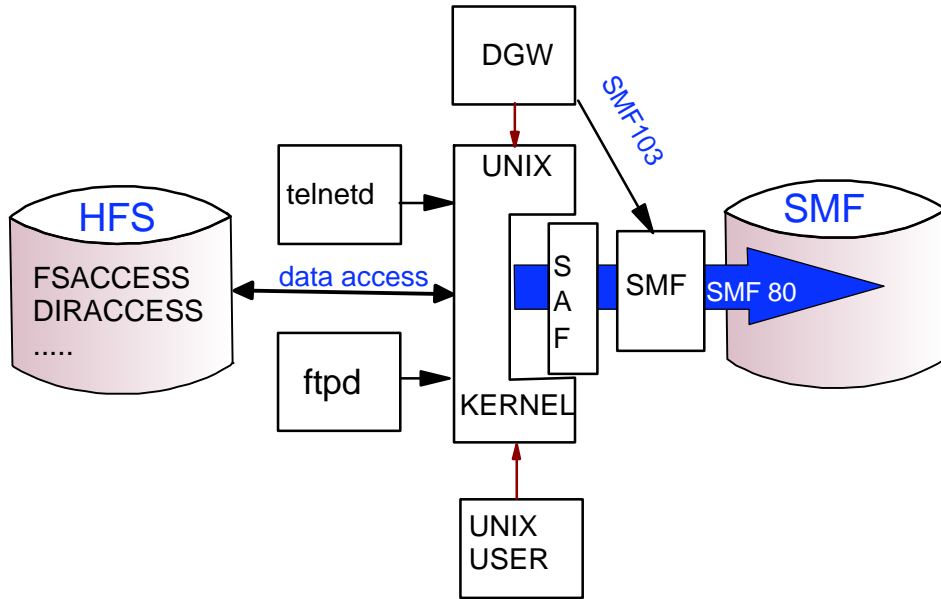
SMF Recording



- **Other useful SMF records:**

- ▶ 030 - address space work record
- ▶ 042 - HFS activity and caching
- ▶ 07x - UNIX System Services measurement for RMF and kernel activity
- ▶ 092 - mounted file system data
- ▶ 118 - TCP/IP daemon relevant data

SMF Recording



© Copyright IBM Corporation, 1999

Roland Trauner trauner@us.ibm.com



SMF Recording

- **Webserver needs to be authorized to write to SMF**

- ▶ RDEFINE FACILITY BPX.SMF UACC(NONE)
- ▶ PERMIT BPX.SMF CLASS(FACILITY) ID(WEBSRV) ACC(READ)
- ▶ SETR RACLIST(FACILITY) REFRESH

- **Define the SMF Types in SYS1.PARMLIB (SMFPRMxx)**

```
SMFPRMxx
...
SYS(TYPE(30,42,74,80,81,83,92,103),EXITS(IEFU83, IEFU84,
    IEFU85, IEFACRTR, IEFUJV, IEFUSI, IEFUJP,
    IEFUSO, IEFUTL, IEFUAV),
    INTERVAL(SMF,SYNC),DETAIL)
```

- **Enable changed SMF recording**

- ▶ T SMF=xx xx = SMFPRMxx

SMF Recording



- **Enable Domino Go Webserver to do SMF recording**
- **Modify httpd.conf**
 - ▶ SMF ALL
 - ▶ SMFRecordingInterval 00:12
- **or via command**
 - ▶ F WEBAPPLE,APPL=-smf
- **Several tools available to analyze SMF records**
- **TME 10 Performance Reporter for OS/390**
 - ▶ offers DGW reports
- **SMF Record 103**
 - ▶ Described in Webmasters Guide "Managing your Webserver"
 - ▶ Additional Description in redbook SG24-2074-01