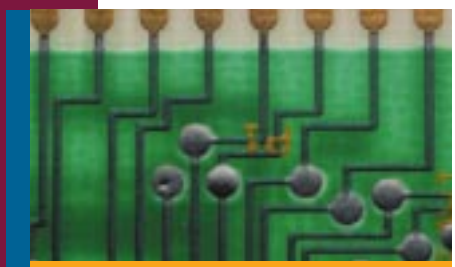

BY PATRICK RENARD

Implementing a Web Server on OS/390: Part II ICSS Functions

Now that you've established how to set up and operate a web server on the OS/390 platform, the next step is using this server to implement your business applications.

LAST month, Part I of this series examined installation and operation of an "empty" ICSS server on OS/390. This article presents some interesting ICSS functions to implement web applications on this platform. First, we will examine some basic functions: the "Web Hotel" concept and how to use a single physical server to manage several logical web applications, the RACF interface and how it can be used to protect your server applications, and then, how to use page access counters.

Secondly, I will present some advanced concepts including IBM Host On-Demand and how to access 3270 applications from the Internet and Secure Socket Layer (SSL), and how to secure your Internet traffic.

IMPLEMENTING A WEB HOTEL

A Web Hotel is a single "physical" web server that is able to serve different "logical" web servers. This can be useful for service providers who need to set up another web server image without having to physically build another server. As long as web serving capacity requirements do not exceed the capacity of a single physical server, the Web Hotel concept is ideal. One possible implementation is to use HTTP/1.1 enhancements, which allow a single host server to be known with different hostnames. This method, which is called virtual host using a single IP address, can only be used with a web browser implementing HTTP/1.1. In that case, the browser sends a header that contains the hostname portion of the URL. This allows the web server to distinguish requests based on the original hostname entered by the client. Figure 1 presents an overview of this concept. The process involves several steps:

- **Step 1:** The client enters a request containing a hostname.
- **Step 2:** The IP address is resolved by a Domain Name Server.
- **Step 3:** The server receives the request.
- **Step 4:** The server determines the content to send based on the hostname specified by the client browser.

To implement this configuration, you need to update your httpd.conf file to use specific directories for each "logical" server. See Figure 2. For each "logical" server, you can set up the type of directory architecture to store its objects as shown in Figure 3.

PROTECTING ACCESS TO SPECIFIC URLS WITH RACF

When ICSS serves a request from a browser, it starts an OpenEdition process. This process needs a RACF userid. To set up this userid you can force users to sign on with their own userid (in this case, all users who access the server need an MVS userid with an OpenEdition profile) or you can decide to use a default surrogate userid such as PUBLIC for all users.

All access controls will be established using this userid: UNIX checks will be based on UID/GID and MVS checks will be based on the userid. To set up a default userid, you need to add the following directive in the httpd.conf file:

```
UserId          PUBLIC
```

To force users to sign on with their own userid before accessing specific URLs

(administration panels), you need to code the directives shown in Figure 4.

ACCESSING MVS SEQUENTIAL DATASETS

With ICSS, you can retrieve web data from MVS physical sequential datasets (PS) or partitioned datasets (PO). To avoid data duplication, it can be useful to access data directly from ICSS MVS datasets. It is often even faster to access MVS datasets than HFS. ICSS implements this function using an ICAPI (Internet Connection API) service: mvsds.so DLL program. You need to code directives in httpd.conf to define this service. See Figure 5. The server will match URLs starting with /MVSDS* to load the required dataset. Figure 6 shows how to use this service to browse some SYS1.PARMLIB members. The RACF userid (either a private or surrogate userid such as PUBLIC), which will be used by ICSS to serve these requests, must have read access on MVS datasets. To achieve better performance, you can pre-load, in memory, one or more datasets at server initialization using mvsds.conf file, as shown in Figure 7.

PAGE ACCESS COUNTING

A very common facility provided by a web server is to count the number of visitors that have accessed a particular page. ICSS provides a counter program that displays page access count. This function is implemented by three services:

- service /cgi-bin/apicounter* /usr/lpp/internet/bin/htcounter.so:HTCounter*
- service /cgi-bin/datetime* /usr/lpp/internet/bin/htcounter.so:HTCounter*
- service /cgi-bin/text2gif* /usr/lpp/internet/bin/htcounter.so:HTCounter*

To use this facility, you have to code the tags shown in Figure 8 in your HTML document. The counter program writes counter values in files stored in server_root/Counters, in our case /u/imwebsrv/Counters, as shown in Figure 9. Before using the counter, you must create and initialize the counter file as shown in Figure 10. The counter program needs access to some Font files located in server_root/Counters/Fonts/. Theses files are normally installed in /usr/lpp/internet/server_root/Counters/Fonts/. However, because our server_root is /u/imwebsrv, we had to

Figure 1: Web Hotel Overview

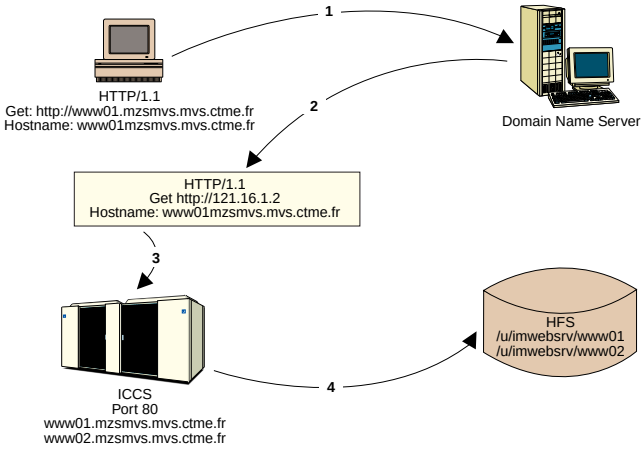

Figure 2: httpd.conf Updates to Implement "Logical" Servers

```
ℓ
ℓ directories for www01 server
ℓ
Pass    /*              /u/imwebsrv/www01/*       www01.mzsmvs.mvs.ctrne.fr
ℓ
ℓ
ℓ directories www02 server
ℓ
Exec    /cgi/*          /u/imwebsrv/www02/cgi/*   www02.mzsmvs.mvs.ctrne.fr
Exec    /java/*         /u/imwebsrv/www02/java/*  www02.mzsmvs.mvs.ctrne.fr
Pass    /*              /u/imwebsrv/www02/*       www02.mzsmvs.mvs.ctrne.fr
ℓ
```

Figure 3: "Logical" Server Directories Structure

```
                                Directory List

/u/imwebsrv/www02/
Select one or more files with / or action codes.

  Type    Perm    Changed (GMT)         Owner      Size     Fil       Row 1 of 8
_ Dir     755     02/19/1998 11:22      I990557    0        .
_ Dir     755     01/30/1998 14:41      WEBADM     0        ..
_ Dir     755     02/11/1998 18:38      I990557    0        cgi
_ File    755     02/13/1998 16:24      I990557    1752     Frntpage.shtml
_ Dir     755     02/13/1998 16:29      I990557    0        gif
_ Dir     755     02/13/1998 16:27      I990557    0        html
_ Dir     755     02/09/1998 17:25      I990557    0        java
_ Dir     755     11/28/1997 13:41      I990557    0        jpeg
```

Figure 4: Forcing Users to Sign on to Access Administration Forms

```
Protection IMW_ADMIN {
       PasswdFile          %%SAF%%
       UserId              %%CLIENT%%
       Mask                All
                  }
Protect /admin-bin/*                                IMW_ADMIN
```

Figure 5: httpd.conf Directives for MVSDS Service

```
£
£ MVSDS service
£
ServerInit /usr/lpp/internet/bin/mvsds.so:mvsdsInit /u/imwebsrv/config/
Service    /MVSDS*  /usr/lpp/internet/bin/mvsds.so:mvsdsGet*
ServerTerm /usr/lpp/internet/bin/mvsds.so:mvsdsTerm
£
```

build a symbolic link from /u/imwebsrv/Counters/Fonts to /usr/lpp/internet/server_root/Counters/Fonts/. You can create that link using the shell command shown in Figure 11.

HOST ON-DEMAND

IBM Host On-Demand is an Internet-to-SNA connectivity solution that provides 3270 access from a web browser. Host On-Demand is available at no additional charge as an added feature of IBM Communications Server (TCP/IP Feature: 6046). You can obtain additional information on the OS/390 feature on the web at www.networking.ibm.com/hex/hex390.html.

Host On-Demand uses a Java environment and TN3270 protocols to provide platform-independent host access from a web browser. With Host On-Demand TN3270 Java applets, you don't need any additional software on your PC to access 3270 applications. When you click on the Host On-Demand hyperlink, the applet is dynamically downloaded and started on your computer.

Host On-Demand is installed using SMP/E (FMID: JTCP32H). The product is composed of several MVS datasets and one OpenEdition filesystem (mounted on /usr/lpp/he). Following installation you should update httpd.conf to add a Pass directive to locate Host On-Demand objects. Figure 12 demonstrates how to update this configuration file. To begin using Host On-Demand, establish a hyperlink to he3270en.htm and immediately begin using Host On-Demand through this link as shown in Figure 13.

THE SECURE SOCKET LAYER (SSL)

The Internet was not initially designed to protect confidential or sensitive information. Internet users and providers are not regulated; anyone can use the Internet or become an Internet provider. Thus, unless some form of security is used information being communicated is unprotected from mischief, malice or inadvertent misuse.

Secure Socket Layer (SSL), developed by Netscape Communications Corporation, is a security protocol that encrypts data sent by an application using a TCP/IP sockets interface. HTTPS is the unique protocol that combines SSL with HTTP. It allows clients and servers to communicate confidential data through the Internet or an Intranet.

SSL is composed of two protocols, record protocol and handshake protocol:

Figure 6: Sample HTML Code Using MVSDS Service

```
Browse SYS1.PARMLIB members.
<ul>
 <li>
   <A HREF="http:/MVSDS/'SYS1.PARMLIB(IEASYS00)'">
   I<FONT SIZE=-1>EASYS00</FONT></a>
 <li>
   <A HREF="http:/MVSDS/'SYS1.PARMLIB(IEFSSN00)'">
   I<FONT SIZE=-1>EFSSN00</FONT></a>
 <li>
   <A HREF="http:/MVSDS/'SYS1.PARMLIB(SMFPRM00)'">
   S<FONT SIZE=-1>MFPRM00</FONT></a>
</ul>
```

Figure 7: Sample mvsds.conf Configuration File

```
BROWSE – /u/imwebsrv/config/mvsds.conf ———— Line 00000000 Col 001 043
******************************** Top of Data ********************************
LOAD 'SYS1.PARMLIB(IEASYS00)'
LOAD 'SYS1.PARMLIB(IEFSSN00)'
LOAD 'SYS1.PARMLIB(SMFPRM00)'
******************************** Bottom of Data *****************************
```

Figure 8: Sample HTML Code to Use Page Access Count Facility

```
<P>You are visitor number:
<img src="/cgi-
bin/apicounter/count01.cnt?FontName=LCD&FontSize=9x13&Format=%%010d&BG=000000&FG=00FF00">
<P>Enjoy your visit.
```

Figure 9: Counters Files Directory

```
                                Directory List

/u/imwebsrv/Counters/
Select one or more files with / or action codes.

  Type    Perm    Changed (GMT)         Owner      Size     Fil       Row 1 of 9
_ Dir     755     01/30/1998 14:59      I990557    0        .
_ Dir     755     01/30/1998 14:41      WEBADM     0        ..
_ File    777     02/17/1998 09:48      I990557    2        count01.cnt
_ Syml    777     01/30/1998 14:59      I990557    44       Fonts
_ File    777     01/30/1998 18:00      I990557    3        icssamp1.cnt
_ File    644     01/30/1998 14:52      I990557    3        icssamp2.cnt
_ File    644     01/30/1998 14:52      I990557    57       icssamp3.cnt
_ File    644     01/30/1998 14:53      I990557    3        icssamp4.cnt
_ File    644     01/30/1998 14:53      I990557    3        sample.cnt
```

Figure 10: Initialize Counter File With 0

```
BROWSE – /u/imwebsrv/Counters/count01.cnt ———— Line 00000000 Col 001 002
******************************** Top of Data ********************************
0
******************************** Bottom of Data *****************************
```

Figure 11: Building a Symbolic Link to Fonts Directory

```
ln -s /usr/lpp/internet/server_root/Counters/Fonts/ /u/imwebsrv/Counters/Fonts
```

Figure 12: httpd.conf updates for Host On-Demand

```
£ Host on Demand
£
Pass            /hod/*          /usr/lpp/he/*
£
```

Figure 13: HTML Sample Code to Call Host On-Demand

```
<DT>
<A HREF="/hod/he3270en.htm">
   <img src="/Admin/skycfg.gif" align="bottom" alt=" ">
   H<FONT SIZE=-1>OST ON DEMAND</FONT></A>
<DD>
Telnet 3270 Client.
```

Figure 14: SSL Security Keys

```
                                Directory List

/u/imwebsrv/security/
Select one or more files with / or action codes.

   Type    Perm   Changed  (GMT)         Owner      Size     Fil       Row 1 of 6
_ Dir     755    02/24/1998 18:43       I990557    0        .
_ Dir     755    02/24/1998 18:23       WEBADM     0        ..
_ File    600    02/24/1998 18:25       I990557    3474     ca.kyr
_ File    600    02/24/1998 18:43       I990557    129      ca.sth
_ File    600    02/24/1998 18:25       I990557    4133     server.kyr
_ File    600    02/24/1998 18:43       I990557    129      server.sth
```

Figure 15: httpd.conf Updates to Implement SSL Support

```
sslmode     on
sslport     443
SSLClientAuth   Off
normalmode on
keyfile /u/imwebsrv/security/ca.kyr
keyfile /u/imwebsrv/security/server.kyr
```

Figure 16: httpd.conf Updates to Use SSL

```
£ www01 server
£
Redirect   /secure/*   https://www01.mzsmvs.mvs.ctrne.fr/*    www01.mzsmvs.mvs.ctrne.fr
Pass       /*          /u/imwebsrv/www01/*                   www01.mzmvs.mvs.ctrne.fr
```

Figure 17: Sample HTML Coding to Use SSL

```
<DT>
 <img src="/Admin/skycfg.gif" align="bottom" alt=" ">
 P<FONT SIZE=-1>HONE DIRECTORY</FONT>
<DD>
     <ul>
       <li>
       <A HREF="/secure/html/d8ct.htmls">
        <img src="/gif/sslon.gif" align="bottom" alt=" "> </A>
        Access CTR Phone directory using data encryption.
     <li>
       <A HREF="/html/d8ct.htmls">
        <img src="/gif/ssloff.gif" align="bottom" alt=" "> </A>
        Access CTR Phone directory without data encryption.
     </ul>
```

Record Protocol: This protocol is based on cryptography and can be used to ensure privacy and integrity of data over a non-secure network. This protocol is implemented using a symmetric encryption key scheme.

Handshake Protocol: This protocol allows the receiver of a document to check the identity of the sender using an asymmetric encryption scheme. This handshake is based on "certificates," which are electronic proofs of identity. These certificates are delivered by a trusted third party.

SSL IMPLEMENTATION WITH ICSS

Because HTTP and HTTPS are different protocols that use TCP/IP ports 80 and 443 respectively, you can run both SSL and non-SSL requests at the same time. So, you can choose to provide general information to all users using no security and specific information only to browsers that make secure requests.

You must first decide what type of certificate will be used to authenticate your server. To get started with SSL, you will probably use a self certificate. The *Webmaster's Guide* provides information on how to generate your own certificate.

Once you've generated your SSL certificate, you must store it in the security directory of your server as shown in Figure 14. Note: A certificate can be delivered by an official external organization or, for testing purposes only, a certificate you created yourself. Figure 15 demonstrates how to update the httpd.conf configuration file, which you must do to activate SSL support (you must stop and start ICSS to implement these changes). Before using SSL, you need to update your Pass directives to "redirect" specific requests to HTTPS instead of HTTP. This is done adding a redirect directive in httpd.conf as shown in Figure 16. Next, you are ready to code HTML documents referencing your "secure" server as shown in Figure 17. Note that you will need to specify https:// as an anchor in HTML documents that link to SSL protected documents.

SSL PERFORMANCE IMPACT

Cryptography does have an associated system cost. Each incoming and outgoing transaction that requires this level of security must be encrypted and decrypted. This operation is generally performed in software that will have an impact on processor performance. However, new CMOS servers G3 and G4 address this challenge by performing hardware cryptographic functions using a specialized Cryptographic Coprocessor.

CONCLUSION

Now that the environmental characteristics of implementing an ICSS server on OS/390 have been discussed, a foundation is in place for Part III of this series. Part III will discuss how to write Common Gateway Interfaces (CGIs) on OS/390 to dynamically build Web pages. In this article, I will examine REXX and C/C++ programming techniques and also look at how to install and run Java CGIs and applets on OS/390. ts

NaSPA member Patrick Renard has been an MVS systems programmer for eight years. His experience includes DB2 Data Sharing and Parallel Sysplex implementation. He can be reached at renard@mygale.com.