IBM HTTP Server V7 and the RACF Auto-Registration Application

This document can be found on the web, www.ibm.com/support/techdocs
Document ID: PRS4791

October 14, 2011
Mike Kearney
Overview

In 1996, IBM released a web server for the OS/390 operating system. Based on the CERN web server, it was quickly adopted by IT shops to expand the role of the mainframe as a data and application server. Initially known as the IBM Internet Connection Secure Server, then as the Domino Go Webserver, it continues to be available and supported today as the IBM HTTP Server for z/OS 5.3. It's become an important part of the web infrastructure for many System z users.

Over the years, IBM customers have also expressed interest in a port of the Apache web server to z/OS. Of course it must be optimized to the z/OS operating system, taking advantage of the SAF interface and the use of System z cryptographic hardware. Initially available only to licensed WebSphere Application Server for z/OS V6.1 customers, in IBM United States Software Announcement 208-391, dated November 18, 2008, IBM announced the availability of the IBM HTTP Server V7.0 as part of the unpriced IBM Ported Tools for z/OS licensed program.

Today IBM z/OS users have a choice between a CERN-based web server and an Apache-based one. One frequently asked question is whether the Apache-based IBM HTTP Server V7.0 can replace all of the functions of the old reliable CERN-based IBM HTTP Server for z/OS 5.3. In general the answer is yes, although there remain a few functions that haven't been provided, or haven't been tested.

This paper focuses on one example, the RACF Auto-Registration application sample code released for the Domino Go WebServer in 1998, and described in Redbook SG24-5158. Properly configured, the IBM HTTP Server V7 is able to run the RACF Auto-Registration application sample code released in 1998. If you still use the RACF Auto-Registration application with your IBM HTTP Server for z/OS 5.3, you might like to use it on the IBM HTTP Server V7. If you have no prior experience with the IBM HTTP Server V7, this is an excellent opportunity to get acquainted with it.

An overview of the steps:

1. (Optional) Configure the RACF Auto-Registration application with the IBM HTTP Server for z/OS 5.3.
2. Build an IBM HTTP Server V7 on your z/OS system.
3. Define directories and copy the RACF Auto-Registration sample materials.
4. Make necessary modifications to the RACF Auto-Registration sample materials.
5. Modify your httpd.conf file to support the RACF Auto-Registration application.
6. RACF commands and permissions.
7. Test the RACF Auto-Registration application.

The remainder of this document describes the above steps in detail.
1. (Optional) Configure the RACF Auto-Registration application with the IBM HTTP Server for z/OS 5.3.

Although the subject of this Techdoc is configuring the RACF Auto-Registration application with the IBM HTTP Server V7, you might be interested in the original RACF Auto-Registration application. In preparation for testing RACF Auto-Registration on the IBM HTTP Server V7, we downloaded the original materials and set it up on an IBM HTTP Server for z/OS 5.3, so we could see how it works. It served as a valuable guide and reference to ensure that when the RACF Auto-Registration application was configured on the IBM HTTP Server V7, it operated correctly, especially in prompting for a client certificate and basic authentication.

Documentation for the original RACF Auto-Registration application for the Domino Go Webserver is still available in Redbook SG24-5158 online at: http://www.redbooks.ibm.com/redbooks/pdfs/sg245158.pdf

The original sample code for the RACF Auto-Registration application is still available at: ftp://www.redbooks.ibm.com/redbooks/SG245158

Pages 131-138 of the above Redbook describe the RACF Auto-Registration application and how to install the sample code, and the instructions are still mostly applicable to the IBM HTTP Server for z/OS 5.3.

A few comments are offered here on the instructions in the Redbook:

The Redbook used "SSLCLIENTAUTH ON". This is not a supported option for SSLClientAuth in the IBM HTTP Server for z/OS 5.3. In testing we used "SSLClientAuth Local" and it behaved as required, prompting all clients for a certificate.

Although not well documented, IBM HTTP Server for z/OS 5.3 directives, subdirectives and their values are often case-sensitive. With that in mind, from our httpd.conf file, here are the directives that we used that are related to the RACF Auto-Registration application:

SSLMode on
SSLPort 7543
SSLClientAuth Local
keyfile MyTestKeyring SAF

Protection Public_Pages {
  ServerId HTTP_Server
  AuthType Basic
  UserId %%SERVER%%
}
Note that port 443 is the standard SSL port. We chose port 7543 in our testing simply because port 443 was in use by another server.

RACF keyrings were still new in 1998. The Redbook used a keyfile. In our testing we used a RACF keyring and certs for the server and client. The correct format for a keyfile directive when using a RACF keyring is:

```
keyfile MyTestKeyring SAF
```

As the Redbook didn't use RACF keyrings or certs, the following RACF commands are offered as a sample of commands needed to build the RACF keyring and certs used in our testing of the RACF Auto-Registration application with the IBM HTTP Server for z/OS 5.3.

```
RACDCERT CERTAUTH DELETE (LABEL('IMWEBSRK CA'))
RACDCERT ID(WEBSERV) DELETE (LABEL('webserv'))
RACDCERT ID(WEBSERV) DELRING(MyTestKeyring)
RACDCERT ID(CLIENT) DELETE (LABEL('ClientCert'))
SETR RACLST('DIGTCERT') REFRESH
RACDCERT ID(WEBSERV) ADDRING(MyTestKeyring)
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('IMWEBSRK CA') -
O('IBM') OU('ATS') C('US')) WITHLABEL('IMWEBSRK CA') -
TRUST NOTAFTER(DATE(2020/12/31)) -
NOTBEFORE(DATE(2010/01/01))
RACDCERT ID(WEBSERV) GENCERT SUBJECTSDN(CN('your.host.name') -
O('ATS') OU('WEBSERV')) WITHLABEL('webserv') -
SIGNWITH(CERTAUTH LABEL('IMWEBSRK CA')) -
```
NOTAFTER(DATE(2020/12/30)) –
NOTBEFORE(DATE(2011/01/01))
RACDCERT ID(WEBSERV) CONNECT (RING(MyTestKeyring) –
LABEL('IMWEBSRK CA') CERTAUTH)
RACDCERT ID(WEBSERV) CONNECT (LABEL('webserv') –
RING(MyTestKeyring) DEFAULT
RACDCERT ID(CLIENT) GENCERT SUBJECTSDN –
(CN('Client User') –
OU('ATS') O('IBM') C('US')) WITHLABEL('ClientCert')
SIGNWITH(CERTAUTH –
LABEL('IMWEBSRK CA')) –
TRUST NOTAFTER(DATE(2015/12/31)) –
NOTBEFORE(DATE(2011/01/01))
RACDCERT ID(CLIENT) EXPORT(LABEL('ClientCert')) –
DSN('CLIENT.CERT') FORMAT(PKCS12DER) PASSWORD('secret')
RACDCERT CERTAUTH EXPORT (LABEL('IMWEBSRK CA')) –
DSN('CLIENT.WEBSRKCA.DER') FORMAT(CERTDER)
SETR RACLST(DIGTCERT) REFRESH

In the above sample commands, WEBSERV is the existing userid that the IBM HTTP
Server for z/OS 5.3 started procedure runs under. CLIENT is the existing userid used for
testing the registration of a client certificate using the RACF Auto-Registration
application.

Again, all of the above is optional, and none of it is prerequisite to running the RACF
Auto-Registration application with the IBM HTTP Server V7. It's included primarily to
enable you to do a side-by-side comparison of the two servers running the same
application.

2. Build an IBM HTTP Server V7 on your z/OS system.

It is beyond the scope of this paper to describe the installation and building of an IBM
HTTP Server V7, other than to provide links to more information.

As mentioned, the IBM HTTP Server V7.0 is packaged with the IBM Ported Tools for
z/OS licensed program. For more information on the IBM Ported Tools for z/OS,
including the IBM HTTP Server V7.0 Feature and ordering information:

The IBM HTTP Server V7.0 is also packaged with the IBM WebSphere Application
Server for z/OS V7. If you have the IBM WebSphere Application Server for z/OS V7, it's
not necessary to order the IBM Ported Tools for z/OS licensed product. However, the
IBM Ported Tools for z/OS includes a number of features that make it worthwhile in
addition to the IBM HTTP Server V7.0.
The Program Directory for IBM HTTP Server V7.0:

The pdf copy of the IBM HTTP Server V7 book:

The IBM HTTP Server V7.0 Infocenter, for general product documentation:
http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?
topic=/com.ibm.websphere.ihs.doc/info/welcome_ihs.html

The IBM HTTP Server V7.0 Infocenter is shared with the IBM WebSphere Application
Server V7 Infocenter. To use the Infocenter to search only the HTTP Server V7.0
content, you can customize the Search Scope of the Infocenter. To do this:
  • go to the IBM HTTP Server V7.0 Infocenter link mentioned above.
  • At the top of the page, click on the blue link labeled "Scope":
  • At the popup, click the radio button labeled "Show only the following topics":
    • Click New.
    • At the next popup, for "List name", type "HTTP Server V7".
    • Under "Topics:" , click only the topic for the IBM HTTP Server.
    • Click OK, then OK again to save.
    • Now the Scope will include only the IBM HTTP Server V7 book, which will be
      the only book listed under Contents.
    • To change the Scope later, just click on the link labeled "Scope":

The IBM HTTP Server V7.0 used in the testing for this paper was built using the
information in the Infocenter referenced above, in the topics "Migrating and installing
IBM HTTP Server on z/OS systems" and "Installing IBM HTTP Server". The server was
built using the using the installer program install_ihs, which greatly simplified the
process.

Once you have an IBM HTTP Server V7 running on your z/OS system, you are ready to
proceed to step 3.

3. Define directories and copy the RACF Auto-
Registration sample materials.

The RACF Auto-Registration sample materials are contained in a zip file located in the
Techdocs entry for this paper, PRS4791. The file is “HTTP Server V7 RAR.zip”.

The HTTP Server V7 RAR.zip file contains all of the same files as the original RACF
Auto-Registration sample materials released in 1998, with the exception of the original
selfreg.rexx. The original selfreg.rexx file was updated to make it work with
IBM HTTP Server V7, and the modified selfreg.rexx file is included in the HTTP Server
V7 RAR.zip.
Download the “HTTP Server V7 RAR.zip” file from the Techdocs site and unzip the file to a folder on your PC.

The IBM HTTP Server V7 built for the testing of the RACF Auto-Registration application uses a server root directory of /etc/websrv1/. The document root directory is /etc/websrv1/htdocs.

Two directories are required to hold the materials for the RACF Auto-Registration application. Create one new directory in the directory indicated by the DocumentRoot directive of your httpd.conf file. In our server, the DocumentRoot directive is "/etc/websrv1/htdocs", so we created a new directory /etc/websrv1/htdocs/RAR. In this directory we created our second directory, /etc/websrv1/htdocs/RAR/REXX.

The /etc/websrv1/htdocs/RAR/ directory holds the RACF Auto-Registration application html, gif and jpeg files.

The /etc/websrv1/htdocs/RAR/REXX/ directory holds just the selfreg.rexx.

It is important that the directory that holds the selfreg.rexx be a subdirectory of the directory that holds the RACF Auto-Registration application html, gifs and jpegs, because selfreg.rexx refers to jpegs and gifs located in the relative directory one level above where selfreg.rexx is located.

After defining the two directories, FTP the RACF Auto-Registration sample materials extracted from the zip file on your PC to the appropriate directories you allocated above. Remember to transfer the html and rexx files in ascii mode, and the gifs and jpegs in binary mode. To avoid access problems later, make the server's userid (we used WEBSRV1) the owner of the files.

A sample IBM HTTP Server V7.0 httpd.conf is also included in the HTTP Server V7 RAR.zip file, but it is for reference only and is not meant to replace the httpd.conf file used by your server, so there's no need to FTP it to the server.

4. Make necessary modifications to the RACF Auto-Registration sample materials.

Two of the files in the HTTP Server V7 RAR.zip file must be updated to reflect your configuration. They are the selfreg.html and selfreg.rexx files.

In the selfreg.html file, locate the ACTION value and replace the url with the https url for the selfreg.rexx on your server.

For example, we changed the line:
to the url of the selfreg.rexx exec on our server:

In the selfreg.rexx file, there are several changes. Locate the lines near the top where the values for tlrfile and hdrfile are assigned, and replace the values with the location that you FTP'ed the selfrgft.html and selfrghd.html files to.

For example, we set the values to:

tlrfile = '/etc/websrv1/htdocs/RAR/selfrgft.html'
hdrfile = '/etc/websrv1/htdocs/RAR/selfrghd.html'

Also in the selfreg.rexx file, locate the ACTION value and replace the url with the https url for the selfreg.rexx on your server.

For example, we set the value to:

5. Modify your httpd.conf file to support the RACF Auto-Registration application.

A sample IBM HTTP Server V7.0 httpd.conf file used in our testing of the the RACF Auto-Registration application is included in the HTTP Server V7 RAR.zip file. It is for reference and is not meant to replace the httpd.conf for your server. However, bits and pieces of it will serve as examples for enabling your IBM HTTP Server V7 to support the RACF Auto-Registration application. The sample httpd.conf has all the self-documentation comments removed to make it smaller and easier to read.

There are a number of modifications that must be made to your httpd.conf. In no particular order:

LoadModules for SAF authorization and the use of SSL:

LoadModule auth_basic_module modules/mod_auth_basic.so
LoadModule authnz_saf_module modules/mod_authnz_saf.so
LoadModule authz_default_module modules/mod_authz_default.so
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so

Directory statement protecting the selfreg.rexx exec, requiring basic authentication:

```
<Directory "/etc/websrv1/htdocs/RAR/REXX/" >
  SetHandler cgi-script
```
Options ExecCGI
AuthName SELFREG
AuthType Basic
AuthBasicProvider saf
Require valid-user
SAFRunAs %CLIENT%%
</Directory>

Directory statement making the rest of the RACF Auto-Registration application public:
<Directory "/etc/websrv1/htdocs">
   Options FollowSymLinks
   AllowOverride None
   Order allow,deny
   Allow from all
</Directory>

AddType to recognize rexx execs as executables:
AddType application/x-httpd-rexx-script .rex .rexx

Changes to enable SSL, specify an SSL port, require a client cert and use a RACF keyring:
<IfModule mod_ibm_ssl.c>
   Listen 3543
   <VirtualHost *:3543>
      SSLEnable
      SSLClientAuth Required
   </VirtualHost>
</IfModule>
SSLDisable
KeyFile /saf MyTestKeyring

Note that port 443 is the standard SSL port. We chose port 3543 in our testing simply because port 443 was in use by another server.

Information on the various httpd.conf directives can be found in the IBM HTTP Server V7.0 Infocenter:

6. RACF commands and permissions.

In addition to the RACF commands you will have run in the process of building your IBM HTTP Server V7, commands are necessary to enable the RACF Auto-Registration application.
Your server will need a keyring (or a keyfile) in order to support the RACF Auto-Registration application. In the sample directives above, the keyring was MyTestKeyring, owned by the server which ran as user WEBSRV1.

Below are sample RACF commands to build a keyring and certificates for your IBM HTTP Server V7, and a client certificate for testing the RACF Auto-Registration application.

```
RACDCERT CERTAUTH DELETE (LABEL('WEBSRV1 CA'))
RACDCERT ID(WEBSRV1) DELETE (LABEL('websrv1'))
RACDCERT ID(WEBSRV1) DELRING(MyTestKeyring)
RACDCERT ID(CLIENT) DELETE (LABEL('ClientCert1'))
SETR RACLST(DIGTCERT) REFRESH
RACDCERT ID(WEBSRV1) ADDRING(MyTestKeyring)
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('WEBSRV1 CA') - O('IBM') OU('ATS') C('US')) WITHLABEL('WEBSRV1 CA') - TRUST NOTAFTER(DATE(2020/12/31)) - NOTBEFORE(DATE(2010/01/01))
RACDCERT ID(WEBSRV1) GENCERT -
SUBJECTSDN(CN('your.host.name') - O('ATS') OU('WEBSRV1') C('US')) - SIGNWITH(CERTAUTH LABEL('WEBSRV1 CA')) - TRUST NOTAFTER(DATE(2020/12/30)) - NOTBEFORE(DATE(2011/01/01))
RACDCERT ID(WEBSRV1) CONNECT (RING(MyTestKeyring) - LABEL('WEBSRV1 CA') CERTAUTH)
RACDCERT ID(WEBSRV1) CONNECT (LABEL('websrv1')) - RING(MyTestKeyring) DEFAULT
RACDCERT ID(CLIENT) GENCERT SUBJECTSDN - (CN('Client User') OU('ATS') O('WEBSRV1') C('US')) - WITHLABEL('ClientCert1') SIGNWITH(CERTAUTH - LABEL('WEBSRV1 CA')) - TRUST NOTAFTER(DATE(2015/12/31)) - NOTBEFORE(DATE(2011/01/01))
RACDCERT ID(CLIENT) EXPORT(LABEL('ClientCert1')) - DSN('CLIENT.CERT1') FORMAT(PKCS12DER) PASSWORD('secret')
RACDCERT CERTAUTH EXPORT (LABEL('WEBSRV1 CA')) - DSN('CLIENT.WEBSRV1.DER') FORMAT(CERTDER)
SETR RACLST(DIGTCERT) REFRESH
```

In the above sample commands, WEBSRV1 is the existing userid that the IBM HTTP Server V7 started procedure runs under. CLIENT is the existing userid used for testing the registration of a client certificate using the RACF Auto-Registration application.

The server userid will need Permission to use its cert and keyring:
PE IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(WEBSRV1) - ACCESS(READ)
The server userid will need authority to establish thread-level security, necessary for the client to register their certificate to their RACF userid.

Clients who will be adding or removing their certificates from RACF will need authority.

or alternately, set the UACC of the profiles to READ:

7. Test the RACF Auto-Registration application.

To prepare your browser to test the RACF Auto-Registration application you'll need a client certificate. The RACF commands in step 6 above created a client certificate for use in testing.

FTP, in binary format, the dataset 'CLIENT.WEBSRV1.DER' to your PC and save it as file WEBSRV1.CRT. Double-click on the file to start the certificate wizard, which will install the certificate in Microsoft Internet Explorer as a trusted signer.

FTP, in binary format, the dataset 'CLIENT.CERT1' to your PC and save it as file CLIENT.P12. Double-click on the file to start the certificate wizard, which will install the certificate in Microsoft Internet Explorer as a personal certificate. You will be prompted for a password for the certificate. The password is: secret

For other browsers you can use the browser tools or options to install the certificates. Installing the certificates in Microsoft Internet Explorer does not make them available to other browsers you may have installed.

To test the RACF Auto-Registration application, point your browser to the location of the selfreg.html.

On our server, the url is:
You should see a browser popup requesting you to select a certificate for authentication to the server.

When you have selected your certificate, you should see the "Register Personal Certificate with RACF" page. (Since you are using the original RACF Auto-Registration sample materials, it will have the Domino Go WebServer 4.6 and Powered by S/390 icons from 1998.)

Click "Verify Personal Certificate", and a browser basic authentication popup should appear. Enter your RACF userid and password and click Log In.

You should see the "Verify your Certificate Information" page, where the contents of your certificate and your RACF userid will appear. You have the choice of "Register Personal Certificate" or "Deregister Personal Certificate".

If you click "Register Personal Certificate", the displayed certificate will be added to RACF with you as the owner, and the message “Your Certificate was successfully registered with RACF” will appear.

If you click "Deregister Personal Certificate", the displayed certificate will be removed from your id in RACF, and the message “Your Certificate was successfully deregistered with RACF" will appear.

References:

IBM United States Software Announcement 208-391:

Redbook SG24-5158:

RACF Auto-Registration 1998 sample code rar.zip:
ftp://www.redbooks.ibm.com/redbooks/SG245158

Information on the IBM Ported Tools for z/OS, including the IBM HTTP Server V7.0 Feature and ordering information:

The Program Directory for IBM HTTP Server V7.0:

The pdf copy of the IBM HTTP Server V7 book:
The IBM HTTP Server V7.0 Infocenter, for general product documentation:
http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?
topic=/com.ibm.websphere.ihs.doc/info/welcome_ihs.html

RACF manuals, including the Command Language Reference:
http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/Shelves/EZ2ZBK0K?
filter=RACF&SUBMIT=Search+titles

**Trademarks**
A full list of U.S. trademarks owned by IBM may be found at:

**Feedback**
Please send comments or suggestions for changes to kearney@us.ibm.com.

**Acknowledgements**
The author would like to thank Gregory Ames and Eric Covener for their assistance and support of the IBM HTTP Server V7.