IBM HTTP Server - Certificates and the Secure Sockets Layer (SSL) - session#3

Robert Boretti
Advisory Software Engineer

Today's Agenda

- Explore How to..
  - **troubleshoot** and **debug** SSL *configuration* and *handshake* problems within the IBM HTTP Server

- Specifically, Learn how to..
  - **enable** SSL, HTTP plug-in and Gskit *Tracing*
  - **log** SSL related information in the web server's *access log*

Today’s Agenda (continued..)

- **analyze** SSL messages in the web server’s *error log*
- **analyze** SSL messages in the HTTP plug-in’s *http_plugin.log*
- **identify** the certificate *passed* by the web server to the browser
- **bypass** the *HTTP plug-in* and hit the *WebSphere application server* directly to Identify the *certificate* passed by WebSphere

First Things First..

- What are the minimum Global Security Kit supported versions?

- What files are needed to troubleshoot and debug SSL in the IBM HTTP Server?

What are the minimum Global Security Kit supported versions?

- **IBM® HTTP Server V2.0.47 releases**
  *Supports Global Security Kit Version 7 only!

  2.0.47.0 ....**7.0.1.10** (or **higher**)
  2.0.47.1 ....**7.0.1.16** (" ")

- **IBM HTTP Server V6.0 releases**
  *Supports Global Security Kit Version 7 only!

  V6.0.0.0 ....**7.0.3.6** (or **higher**)

- **IBM HTTP Server V6.1 releases**
  *Supports Global Security Kit Version 7 only!

  V6.1.0.0 ....**7.0.3.20** (or **higher**)

What files are needed to troubleshoot and SSL debug the IBM HTTP Server?

- httpd.conf
- error_log
- access_log
- key.kdb, key.sth, key.rdb, key.crl
- gsktrace.log
- servercert.cer, ca.cer, etc..
- ldaptrace.log
- ldap.prop
- plugin-cfg.xml
- http_plugin.log
- plugin-key.kdb, plugin-key.sth

Next, Let’s Get Busy

- What should I immediately check first?
- What tracing is useful to debug SSL problems?
- What information can I log in the access log that can help me troubleshoot SSL?
- What does a particular SSL message in the web server’s error log mean?
- What does a particular SSL message in the HTTP plug-in log mean?
- How can I confirm what certificate is being used?

What should I immediately check first?

- **Netstat –na** to see if the IBM HTTP Server is listening on the SSL port

```
C:\Documents and Settings\Administrator>netstat -na

Active Connections

Proto  Local Address          Foreign Address        State
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
TCP    0.0.0.0:2967           0.0.0.0:0              LISTENING
TCP    0.0.0.0:59449          0.0.0.0:0              LISTENING
TCP    9.27.165.141:80        0.0.0.0:0              LISTENING
TCP    9.27.165.141:139       0.0.0.0:0              LISTENING
TCP    9.27.165.141:443       0.0.0.0:0              LISTENING
```

(continued..)

- Try both https://hostname/uri and https://ipaddress/uri

- Check the web server’s *error_log* for any SSL “**Initialization**” errors. These normally will be recorded on web server startup

- Check ***IBM HTTP Server* version** and then ***gskit* version** to confirm the proper gskit version is installed (see next slide)

(continued..)

- to check the **IBM HTTP Server** version
  - *windows*® - /ihs_root/bin/apache –V
  - *Unix*® - /ihs_root/bin/apachectl –V

example:

```
C:\Program Files\IBM HTTP Server6.0\bin>apache -V
Server version: IBM_HTTP_Server/6.0.2.15 Apache/2.0.47
Server built:   Aug  9 2006 14:27:54
```

(continued..)

- to check the **gskit** version
  - *Windows* - /gsk_root/bin/gsk7ver.exe
  - *Unix* - /gsk_root/bin/gsk7ver

example:

- @(#)CompanyName: IBM Corporation
- @(#)LegalTrademarks: IBM
- @(#)FileDescription: IBM Global Security Toolkit
- **@(#)FileVersion: 7.0.3.20**

(continued..)

- Another thing to check right away.. Is whether **non-ssl requests** can be *served* from the web server?

- **Comment out** the *WebSphere HTTP plugin* lines and then test to see if any SSL requests work for just **static** content

```
#LoadModule was_ap20_module D:/plugintestmodule/bin/mod_was_ap20_http.dll
#WebSpherePluginConfig D:/plugintestconfig/plugin-cfg.xml
```

- Check the SSL **configuration** in the IBM HTTP Server's *httpd.conf* file. Note: most *SSL problems* are due to an **incorrect** configuration

(continued..)

- When in doubt about the configuration
  - refer to the..

“Guide to properly setting up SSL within the IBM HTTP Server”

http://www-1.ibm.com/support/docview.wss?uid=swg21179559

What tracing is useful to debug SSL problems?

- There are **two main** traces which are useful when debugging IBM HTTP Server SSL issues..

  - **SSLTrace** directive (requires loglevel debug)

    provides additional information in the web server's error_log related to SSL *I/O reads and writes* of data bytes

    example:

    ```
    [Tue Jan 15 14:10:43 2008] [debug] [client 9.27.165.141]
    [9392d8] SSL read end bytes [70] err [0] to [0] eof [0]

    [Tue Jan 15 14:10:43 2008] [debug] [client 9.27.165.141]
    [9392d8] SSL write begin bytes [584] timeout
    [300000000]
    ```

(continued..)

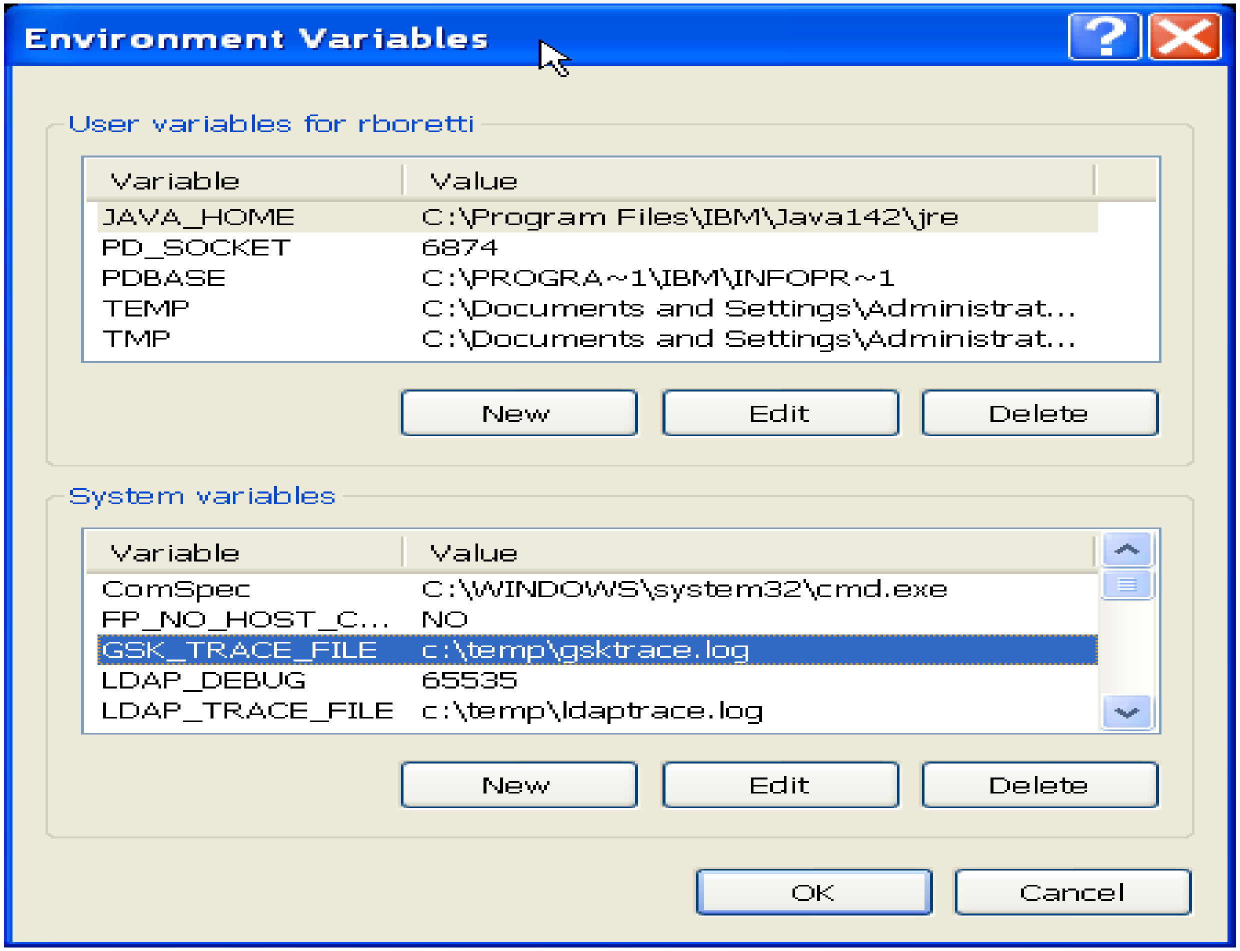
- **Gskit** Tracing
  - ***For Windows:***

    create the following *system variable*:

    GSK_TRACE_FILE

    set the value with the name for the log file (for example: c:\temp\gsktrace.log)

(continued..)



Variable	Value
JAVA_HOME	C:\Program Files\IBM\Java142\jre
PD_SOCKET	6874
PDBASE	C:\PROGRA~1\IBM\INFOPR~1
TEMP	C:\Documents and Settings\Administrat...
TMP	C:\Documents and Settings\Administrat...

Variable	Value
ComSpec	C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_C...	NO
GSK_TRACE_FILE	c:\temp\gsktrace.log
LDAP_DEBUG	65535
LDAP_TRACE_FILE	c:\temp\ldaptrace.log

(continued..)

- ***For UNIX:***

as the *user ID* that starts the IBM HTTP Server create an **environment variable** called: GSK_TRACE_FILE

the environment variable can be created in either of the two ways:
setenv GSK_TRACE_FILE *value* (full path and filename)
csh example:
setenv GSK_TRACE_FILE /usr/HTTPServer/logs/gsktrace_log

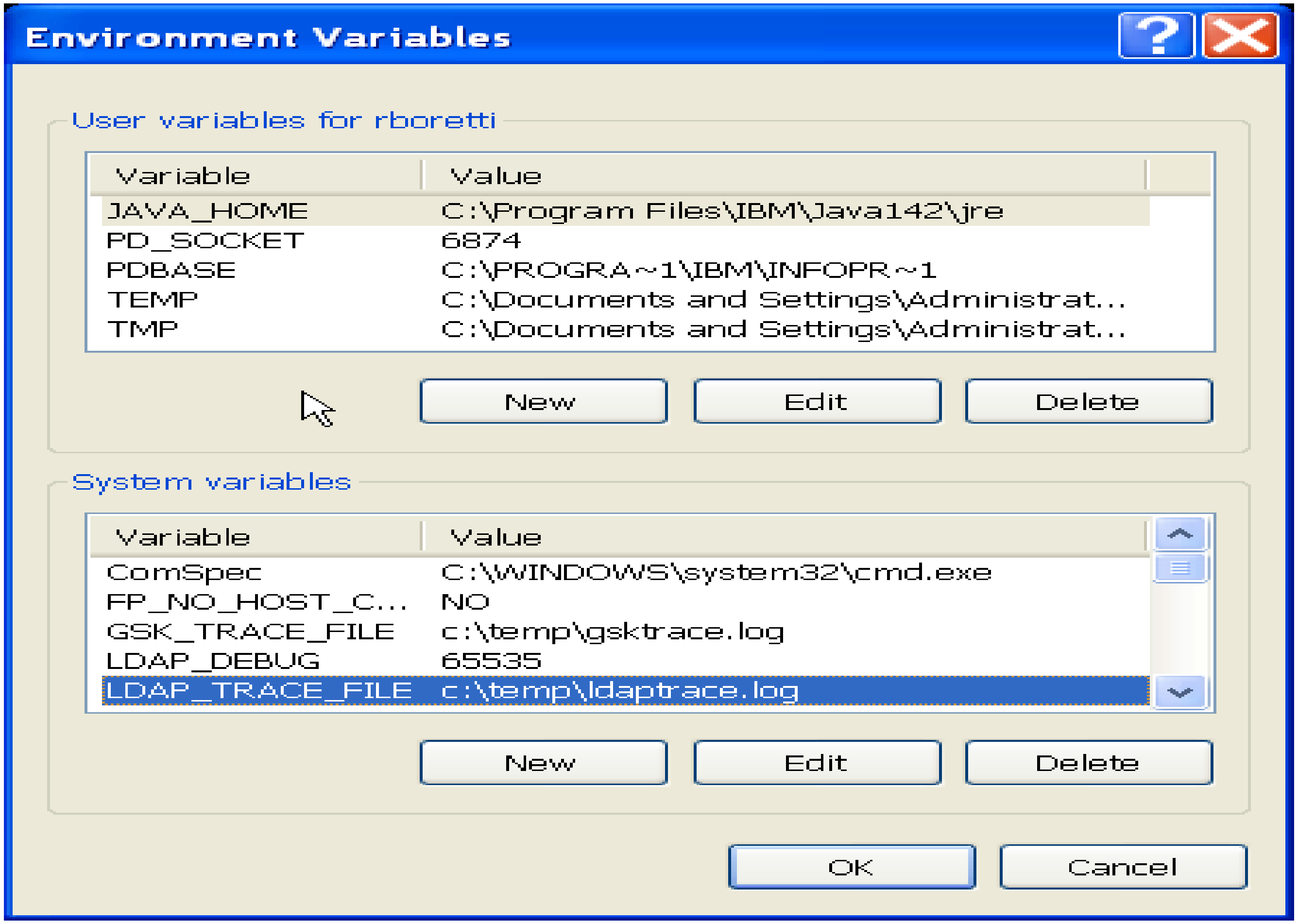
OR

export GSK_TRACE_FILE=*value* (full path and filename)
ksh example:
export GSK_TRACE_FILE=/usr/HTTPServer/logs/gsktrace_log

(continued..)

- In addition, to SSLTrace and Gskit Tracing
  - If SSL is used between the IBM HTTP Server and an **LDAP Server**
    - ***For Windows:***
      create the following *system variable*:
      LDAP_TRACE_FILE
      set the value with the name for the log file (for example: c:\temp\ldaptrace.log)
      LDAP_DEBUG with a value set to **65535**

(continued..)



User variables for rboretti

Variable	Value
JAVA_HOME	C:\Program Files\IBM\Java142\jre
PD_SOCKET	6874
PDBASE	C:\PROGRA~1\IBM\INFOPR~1
TEMP	C:\Documents and Settings\Administrat...
TMP	C:\Documents and Settings\Administrat...

System variables

Variable	Value
ComSpec	C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_C...	NO
GSK_TRACE_FILE	c:\temp\gsktrace.log
LDAP_DEBUG	65535
LDAP_TRACE_FILE	c:\temp\ldaptrace.log

(continued..)

- ***For UNIX:***

as the *user ID* that starts the IBM HTTP Server create an **environment variables** called:
LDAP_TRACE_FILE
LDAP_DEBUG

csh example:

```
setenv LDAP_TRACE_FILE /usr/HTTPServer/logs/ldaptrace.log
setenv LDAP_DEBUG=65535
```

OR

ksh example:

```
export LDAP_TRACE_FILE=/usr/HTTPServer/logs/ldaptrace.log
export LDAP_DEBUG=65535
```

(continued..)

- If SSL problem involves the **WebSphere HTTP plug-in**
  - edit **plugin-cfg.xml** and change *loglevel* to *Trace*

example:

```
<Log LogLevel="Trace” Name="D:\Web~\AppServ\logs\http_plugin.log"/>
```

(continued..)

For **IBM Key Management** Utility problems

- If you are using IBM HTTP Server version 6.0, set JAVA_HOME to <ihsinst>/_jvm.

  If you are using IBM HTTP Server version 6.1, set JAVA_HOME to <ihsinst>/java/jre

  If using an IBM HTTP Server release version earlier than 6.0, set JAVA_HOME to any 32-bit IBM JRE 1.4.2/1.5 at the latest service level

Java™ JVM™

(continued..)

- Then, run the following *iKeyman* command

```
gsk7ikm -Dkeyman.debug=true
-Dkeyman.jnitracing=ON -
Djava.security.debug=ALL
2>ikeyman.txt
```

(continued..)

- for **step-by-step** instructions on enabling the various traces mentioned in the previous slides..

MustGather: IBM HTTP Server SSL handshake and configuration problems

http://www-1.ibm.com/support/docview.wss?uid=swg21141302

MustGather: Errors using iKeyman with IBM HTTP Server

http://www-1.ibm.com/support/docview.wss?uid=swg21202820

(continued..)

MustGather: LDAP authentication problems with IBM HTTP Server

http://www-1.ibm.com/support/docview.wss?uid=swg21141304

MustGather: CMS key database (.kdb) and certificate problems

http://www-1.ibm.com/support/docview.wss?uid=swg21141303

What information can I log in the access log that can help me troubleshoot SSL?

- The IBM® HTTP Server implementation provides Secure Sockets Layer **(SSL) environment variables** that are configurable with the LogFormat directive in the httpd.conf file

- Any of the *SSL environment variables* can be logged for **each client request** in the web server's *access log*

(continued..)

- This information can be very useful when trying to determine..
  - what **cipher** was used for a particular request
  - whether a request was **SSL** or **non-SSL**
  - if *client authentication is enabled*, what **client certificate** was passed
  - what **server certificate** was used for a specific client request

(continued..)

- Example:

```
LogFormat "%h %l %u %t \"%r\" %>s %b %{HTTPS}e
   %{SSL_CIPHER}e %{SSL_CLIENT_DN}e" SSL
CustomLog logs/access.log SSL
```

```
   192.168.0.10 - - [29/Jul/2004:02:16:51 -0400] "GET
   /view_doc_bttnOFF_a.gif HTTP/1.1"304 ON
   SSL_RSA_WITH_RC4_128_SHA CN=jane Doe,O=ibm,C=US

   192.168.0.10 - - [29/Jul/2004:02:16:51 -0400] "GET
   /visit_web_bttnOFF_a.gif HTTP/1.1"304 ON
   SSL_RSA_WITH_RC4_128_SHA CN=jane Doe,O=ibm,C=US
```

Reference key
%{HTTPS}e = **ON** (OFF is displayed if HTTP)
%{SSL_CIPHER}e = **SSL_RSA_WITH_RC4_128_SHA**
%{SSL_CLIENT_DN}e = **CN=jane Doe,O=ibm,C=US**

(continued..)

- For more information and a ***complete list*** of all available *SSL environment variables* that can be logged in the access log

Logging SSL request information in the access log for IBM HTTP Server
http://www-1.ibm.com/support/docview.wss?uid=swg21176455

What does a particular SSL message in the web server's error log mean?

- When trying to determine what a particular *message* means, it is helpful to break them down into categories as follows..
  - **configuration messages -** indicates a problem with the SSL *configuration* in the web server's httpd.conf
  - **handshake messages -** relates to issues in SSL that occur during the *handshake* between a client and the web server
  - **I/O error messages -** Most often relates to issues during the *reading and writing* of data to and from the client
  - **SSL initialization messages -** Most often relates to issues when trying to load gskit or SSL during *web server startup* or at the very beginning of initialization of protocol

(continued..)

- For a ***complete list*** of all SSL related messages and their meaning and resolution

configuration messages
http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/ihs/ihs/rihs_troubconfigmsg.html

handshake messages
http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/ihs/ihs/rihs_troubhandmsg.html

I/O error messages
http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/ihs/ihs/rihs_troubiomsg.html

SSL initialization messages
http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/ihs/ihs/rihs_troubinitmsg.html

What does a particular SSL message in the HTTP plug-in log mean?

- The **two most common** SSL related messages seen in the http_plugin.log are..
  - Failed in r_gsk_secure_soc_init: **GSK_ERROR_BAD_CERT**(gsk rc = 414)

    http://www-1.ibm.com/support/docview.wss?uid=swg21215867

  - str_security (gsk error 408): **GSK_ERROR_BAD_KEYFILE_PASSWORD**

    http://www-1.ibm.com/support/docview.wss?uid=swg21177702

How can I confirm what certificate is being used?

- There are **two simple ways**
  - *log it* in the *access.log* for each request using the SSL environment variable.. %{SSL_SERVER_CN}e
  - from a *browser*

    Firefox – tools →page info →security →view

    Netscape® – view →page info →security →view

    Internet Explorer – page → security report

(continued..)

- To see what certificate is being passed from **WebSphere** to the **HTTP plug-in** requires *bypassing* the plugin and hitting the WebSphere Application Server port directly..

  example: https://hostname:9443/wps/portal

  - then from a *browser*

    Firefox – tools →page info →security →view

    Netscape – view →page info →security →view

    Internet Explorer – page → security report

Let’s Not Forget..

- Additional information related to debugging and troubleshooting SSL that was not covered today

  - SSL *performance* related issues

    http://publib.boulder.ibm.com/httpserv/ihsdiag/ihs_performance.html

  - IBM HTTP Server *crashes* or *hangs*

    http://www-1.ibm.com/support/docview.wss?uid=swg24008409

Additional WebSphere Product Resources

- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at: http://www.ibm.com/developerworks/websphere/community/

- Learn about other upcoming webcasts, conferences and events: http://www.ibm.com/software/websphere/events_1.html

- Join the Global WebSphere User Group Community: http://www.websphere.org

- Access key product show-me demos and tutorials by visiting IBM Education Assistant: http://www.ibm.com/software/info/education/assistant

- View a Flash replay with step-by-step instructions for using the Electronic Service Request (ESR) tool for submitting problems electronically: http://www.ibm.com/software/websphere/support/d2w.html

- Sign up to receive weekly technical My support emails: http://www.ibm.com/software/support/einfo.html

Questions and Answers