Intermittent Shibboleth Decompression error experienced by CCLE & SSC

Problem

On Sunday, 10/11/2009, CCLE and SSC reported an issue that some Shibboleth logins were failing. Authentication itself was going thru, however they were not getting the data. Attribute query was failing with this error:

```
```

The error was intermittent. No other SP reported this problem. Again on Wednesday, 10/14/2009 CCLE reported the same problem. About one in 10 logins were failing with this error.

Cause

We were able to reproduce this error at AIS. This is the sequence of events that leads to this error:

1. Restart services at the IdP
2. Restart shibd daemon and web server at the SP
3. Access Shibboleth enabled resource at the SP. Everything works fine at this point
4. Restart shibd at the SP. This triggers the intermittent decompression error. Problem remains even after rebooting the server (SP).
5. Our tests show that restarting Apache at the IdP solves the problem. However if you restart shibd at the SP problem resurfaces.

This was caused by a bug in OpenSSL library which is used for SSL handshake during Attribute Query between SP & IdP. For in-depth details please read

1. [https://spaces.internet2.edu/display/SHIB2/NativeSPTroubleshootingCommonErrors](https://spaces.internet2.edu/display/SHIB2/NativeSPTroubleshootingCommonErrors), section `error:1408F06B:SSL routines:SSL3_GET_RECORD:bad decompression`

No other SP experienced the issue probably because they didn’t restart shibd since the last IdP restart.

Resolution

One work around was to disable zlib compression for SSL connections using OPENSSL_NO_DEFAULT_ZLIB environment variable.

We set the environment variable `OPENSSL_NO_DEFAULT_ZLIB=1`. Starting apache using the init script does in fact pick up the variable from `/etc/sysconfig/httpd` but for reasons we don’t yet understand Apache still starts with zlib enabled. It is probably a bug somewhere in Apache. We are following up with the vendor Red Hat.

Finally we restarted Apache manually with zlib compression disabled. CCLE and other SPs are working fine since.

Manual restart is not a practical solution, so we are still seeking a permanent solution with Red Hat.