Infrastructure - Story #7810

Need to avoid buffer overflow condition during HTTP client TLS renegotiation

2016-05-16 23:33 - Chris Jones

Status:	New	**Start date:**	2016-05-16
Priority:	Normal	**Due date:**	
Assignee:	Rob Nahf	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Story Points:			

Description

In #2693, #6539, and other tickets we've documented issues with Safari failing to connect to CN and MN services when the server side is configured with 'SSLVerifyClient optional' and Safari has certificates installed in the Keychain that happen to not be trusted by the CN or MN. The workaround is to conditionally set the SSLVerifyClient directive.

However, a side affect of this is that HTTP clients look to be forced to buffer the request on the server during the TLS renegotiation phase. The default buffer size is 128K, and therefore most all POSTs to MNs and CNs that involve data files exceed this limit, and the connection fails due to a buffer overflow condition. An example on the Arctic Data Center deployment shows:

```
./arcticdata.io.error.log.1:[Fri May 13 13:24:10.681521 2016] [ssl:error] [pid 9096] [client 98.228.75.248:54733] AH02018: request body exceeds maximum size (131072) for SSL buffer, referer: https://arcticdata.io/catalog/
```

The main workaround, as mentioned in this "Stack Overflow thread":http://stackoverflow.com/a/15394058/4200841, is to have clients leverage the HTTP 1.1 'Expect' header feature. By setting this header value to '100-continue', it cues the server that a large payload is coming (> 128K!) and to do the renegotiation without buffering the request.

This story is a placeholder to add tasks for each DataONE client product we manage to include this header: d1_libclient_java, d1_libclient_python, matlab-dataone (covered by the Java fix, but needs incorporation), rdataone, and MetacatUI.

Note that a temporary fix on the server side is to increase the buffer size on the MNs and CNs using the 'SSLRenegBufferSize' directive, but the memory consequences need to be considered, as well as the possibility of DOS exposure.

History

#1 - 2016-05-17 14:29 - Chris Jones

- Description updated

#2 - 2016-05-17 14:31 - Chris Jones

I've added a ticket in the MetacatUI tracker for Lauren: https://projects.ecoinformatics.org/ecoinfo/issues/7029

#3 - 2018-01-17 19:09 - Dave Vieglais

- Assignee changed from Dave Vieglais to Rob Nahf

#4 - 2018-01-17 19:09 - Dave Vieglais

- Sprint set to Infrastructure backlog