Infrastructure - Bug #3255

Safari 6.0 fails to connect to Metacat MN with SSLVerifyClient

2012-09-17 19:16 - Mark Servilla

Status:	Rejected		**Start date:**	
Priority:	Normal		**Due date:**	
Assignee:			**% Done:**	0%
Category:			**Estimated time:**	0.00 hour
Target version:				
Milestone:	None		**Story Points:**	
Product Version:				

Description

Safari 6.0 web browser on OS X 10.8 and 10.7 fails to connect to a Metacat Member Node when using the Apache web server setting "SSLVerifyClient Optional".

This issue originated from an LTER Information Manager (Sven Bohm - KBS) when he attempted to connect to the URL " https://metacat.lternet.edu/das", which resulted in the following Safari error message (see LTER RT Ticket #2053 - http://rt3.lternet.edu/rt/Ticket/Display.html?id=2053):

> Safari can't open the page "https://metacat.lternet.edu/das" because Safari can't establish a secure connection to the server "metacat.lternet.edu".

This error was confirmed by Mark Servilla using Safari on both Mac OS X 10.7 and 10.8; this error also occurs on " https://knb.ecoinformatics.org" as of 2012-09-17T13:00.

This issue is apparently the result of the Safari 6.x web browser not supporting web servers that require or even make optional "SSLVerifyClient" during peer renegotiation and has been an issue since Safari 5.x (see: http://openradar.appspot.com/8696868, http://lists.apple.com/archives/fed-talk/2011/Jul/msg00069.html, http://tools.ietf.org/html/rfc5746) - this conclusion is not verified.

To mitigate this issue on tropical.lternet.edu (metacat.lternet.edu), the Apache2 web server had the following directive inserted, which isolates the need for client certificate verification to only DataONE related communication while in the "knb" context:

SSLVerifyClient Optional
SSLVerifyDepth 10

Note: Safari requests that require communication with D1 services on this Metacat will still result in a connection failure.

Local testing indicates that Safari now successfully connects to https://metacat.lternet.edu/das; Ben Leinfelder (NCEAS) confirms that peer communication between this Metacat instance and D1 still succeeds after making the Apache2 configuration change.

Sven Bohm confirmed that he was now able to successfully access "https://metacat.lternet.edu/das".

Related issues:

Related to Infrastructure - Bug #2693: Error -1205 "Client Certificate Reject...	**Closed**

History

#1 - 2012-09-28 16:06 - Dave Vieglais

- Tracker changed from MNDeployment to Bug

#2 - 2013-01-30 19:56 - Dave Vieglais

- Project changed from Member Nodes to Infrastructure

- Start date deleted (2012-09-17)

- translation missing: en.field_remaining_hours set to 0.0

- Milestone set to None

#3 - 2014-10-02 18:02 - Skye Roseboom

- Status changed from New to Rejected