Infrastructure - Bug #2693

Error -1205 "Client Certificate Rejected" by Safari

2012-05-04 13:02 - Dave Vieglais

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Dave Vieglais	**% Done:**	100%
Category:	Authentication, Authorization	**Estimated time:**	0.00 hour
Target version:	CCI-2.3.1		
Milestone:	None	**Story Points:**	
Product Version:	*		

Description

When accessing https://cn-stage.dataone.org using Safari and the user has a client side certificate installed in their keychain, but not one trusted by DataONE, the Server correctly rejects the certificate. Safari *should* continue the secure connection as unauthenticated (like other browsers do), but instead reports an error condition to the user, preventing their access to the site.

This is a bug in Safari, but workarounds should be investigated so that users may continue to access the ONEMercury interface with that browser. Possible options include:

- disable client side certificates for the /onemercury URL
- make /onemercury accessible over regular HTTP
- Have the user retrieve and install a CILogon cert in their keychain (a bad option since then they are bound to using that cert which will be short lived, or long lived with potentially out of date information).

Related issues:

Related to Infrastructure - Bug #3255: Safari 6.0 fails to connect to Metacat...	**Rejected**		
Related to Infrastructure - Bug #6539: completely unable to access cn.dataone...	**Closed**		
Related to MN Dashboard - Bug #6506: Member Node Dashboard not loading in Saf...	**Closed**	**2014-10-06**	**2015-01-12**

History

#1 - 2012-05-04 17:24 - Ben Leinfelder

Using Safari Version 5.1.3 (7534.53.10) I can just hit "Cancel" when it asks me which client certificate I want to use when connecting and then just lets me through to the onemercury UI as expected. I have a Self-signed certificate as well as an old CILogon certificate in my keychain.
When I remove the CILogon certificate, I get the behavior Dave described.
Odd!

#2 - 2012-05-30 12:42 - Dave Vieglais

- Target version deleted (Sprint-2012.19-Block.3.2)

- Position set to 1

#3 - 2013-08-14 18:28 - Dave Vieglais

- translation missing: en.field_remaining_hours set to 0.0

- Start date deleted (2012-05-04)

#4 - 2013-10-02 04:03 - Dave Vieglais

*- Product Version set to **

Comment from Jim Basney:

The Apache mod_ssl configuration directive to control what CAs are trusted
for client certificates is SSLCACertificateFile or SSLCACertificatePath. I
think if you set that to only the CAs you use for client certificates, it
should tell browsers to ignore other client certificates and possibly

solve the Safari issue.

#5 - 2014-03-14 03:42 - Chris Jones

I've run into the same problem on Mac OS X 10.9.2 (Mavericks) on Safari 7.0.2 while connecting to https://cn.dataone.org/onemercury, and having a single certificate installed in my Keychain (my Apple ID certificate for the App Store [com.apple.idms.appleid.prd...]).

Instead of using the 'Acceptable client certificate' list provided by the server, Safari looks to be sending the Apple ID certificate anyway, and the server rejects it (correctly). Safari's behavior should be to continue to the site unauthenticated as other browsers do.

#6 - 2016-04-12 01:27 - Matthew Jones

We have hit this same Safari error on https://arcticdata.io, and found a workaround. In the workaround, we simply configure Apache to check the user agent, and if it is Safari, then to set @SSLVerifyClient none@. The consequences of this are that, for Safari, the only way to log into DataONE is with the new AuthTokens -- X.509 certificates from CILogon will be ignored. But, as nobody except developers uses CILogon certs in browser user agents, this works well for most end users, and avoids the Safari failures to connect. Other user agents should be unaffected, and CN-MN and MN-MN communication should be fine as well. Here's the apache config inside of our SSL virtual host directive used to set this up:

SSLVerifyClient none

SSLVerifyClient optional

#7 - 2016-04-25 22:54 - Chris Jones

With the Arctic Data Center deployment, we've found a side-effect of adding the conditional SSLVerifyClient code Matt mentioned above.

Basically, after the change, POSTing data to the repository with a request larger than around 128K was causing a buffer overflow during the Apache SSL renegotiation phase with the client. the error was:

```
[Tue Apr 19 14:11:18.334162 2016] [ssl:error] [pid 22897:tid 140098161288960] [client 128.111.54.100:37784] AH02018: request body exceeds maximum size (131072) for SSL buffer
[Tue Apr 19 14:11:18.334203 2016] [ssl:error] [pid 22897:tid 140098161288960] [client 128.111.54.100:37784] AH02257: could not buffer message body to allow SSL renegotiation to proceed
```

After reading http://stackoverflow.com/questions/14281628/ssl-renegotiation-with-client-certificate-causes-server-buffer-overflow we decided to change the client code to add a 'Expect: 100-continue' header to each upload request to let Apache know to not to download the whole request body during the renegotiation. This seems to be working, but it's something to consider for DataONE when making this SSL config change.

#8 - 2016-05-31 20:55 - Robert Waltz

- Related to Task #7821: Verify Expect: 100-Continue header on POST or PUT requests added

#9 - 2016-06-01 23:16 - Rob Nahf

- % Done changed from 0 to 30

- Status changed from New to In Progress

I believe the single-certificate situation Ben reported a few years ago has been resolved in the latest version of Safari (9.1), as I can chose not to use the certificate, and also easily remove the certificate preference if I accidentally map it to the domain. Nevertheless, when I don't want to use a client certificate, Safari pops up the certificate selection dialog for every page loaded on the dataone site, so it's still annoying.

How I tested:

On a fresh user account running OSX 11.4 (El Capitan) and Safari 9.1, I tested connection to cn.dataone.org and cn-dev.test.dataone.org. Both pop up the certificate dialog, where there is only one certificate listed, and both continue to connect after 2-3 'cancel' or escape clicks, taking me to the dataone search page.

On cn-dev.test.dataone.org, I re-entered the url, and again got the dialog - which I interpret as it did not remember my selection from before. I chose the only certificate, and since it wasn't trusted, failed to connect, (after trying to modify my keychain, which I denied). Subsequent attempts to navigate to cn-dev.test.dataone.org failed as before, but without the certificate selection dialog.

I then opened the Keychain Access utility, found and removed the cn-dev.test.dataone.org "identity preference" and tried to connect again. It now gave me the certificate selection dialog, and hitting cancel 2 times, it allowed me to connect without a certificate.

cn-dev apache2 config:

SSLVerifyClient require
SSLVerifyDepth 10

```
#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on
SSLOptions +StrictRequire +StdEnvVars +ExportCertData
SSLVerifyClient optional
SSLVerifyDepth 10
```

#10 - 2016-06-01 23:36 - Rob Nahf

would configuring DataONE servers to trust Apple CAs solve the problem? (Assuming if you are using Safari, you will at least have one Apple-signed certificate?

https://www.apple.com/certificateauthority/

#11 - 2016-06-03 19:48 - Robert Waltz

- Related to deleted (Task #7821: Verify Expect: 100-Continue header on POST or PUT requests)

#12 - 2016-10-27 15:53 - Chris Jones

So, while the fixes described in #note-6 and #note-7 above helped, it also introduced an unwanted side effect for POSTing to the server. With that configuration, the entire body of the POST is forced to be buffered on the server during the SSL renegotiation phase. The default @SSLRenegBufferSize@ is 128K, so for uploads of files of any size above 128K (most!) will cause the renegotiation to fail since it can't buffer the file. We increased that size to 100MB, but obviously it doesn't scale - GB range files will fail, or if you keep increasing the buffer size, you'll just run out of RAM, particularly in concurrent connection scenarios.

We've since changed our configuration on the MNs. The trick is to default to @SSLVerifyClient none@, and then only ask for optional certificates when the user agent doesn't match @webkit@. On the MN, we used:

```
SSLVerifyClient none


SSLVerifyClient optional
```

This works great, doesn't require buffering the body, and allows cert-based auth for CN synchronization and MN-MN replication.

However, token-based auth is failing in Safari still because the CNs are still set to @SSLVerifyClient optional@ when the browser calls @/portal/oath@ on the CN (that then redirects to orcid.org).

I'd recommend we change the CN configurations to:

```
SSLVerifyClient none


SSLVerifyClient optional
```

In this setup, all web requests default to not requesting a certificate, but calls to the DataONE API endpoints under @/cn@ will be asked for an optional certificate when they don't match @webkit@, case insensitive. This allows curl, java, R, and python clients to use certificates when desired, along with CN sync and MN repl.

#13 - 2016-11-10 18:06 - Jing Tao

- Target version set to CCI-2.3.1

- Milestone changed from CCI-1.0.0 to None

#14 - 2016-12-02 00:18 - Dave Vieglais

- % Done changed from 30 to 100

- Status changed from In Progress to Closed

Appears to be resolved.

Huzzah! thanks to apache 2.4

#15 - 2017-05-09 21:32 - Chris Jones

Due to issues with other clients, we've updated the configuration to not ask for client certs for any browser-based clients:

SSLVerifyClient none

SSLVerifyClient optional

SSLVerifyDepth 10