Infrastructure - Bug #8051

CORS-based CN calls fail using Internet Explorer on Windows

2017-03-22 20:02 - Chris Jones

Status:	In Progress	**Start date:**	2017-03-22
Priority:	Normal	**Due date:**	
Assignee:	Chris Jones	**% Done:**	30%
Category:	dataone-cn-os-core	**Estimated time:**	0.00 hour
Target version:			
Milestone:	None	**Story Points:**	
Product Version:			

Description

As noted in #2693, #6539, and #3255, Safari does not handle TLS handshakes correctly when asked for a client X509 certificate. Similarly, IE 11 (and 10) on Windows 7 (and maybe others) does not handle TLS handshakes correctly.

The MetacatUI application used on certain Member Nodes (KNB, ARCTIC, ...) makes calls to the CN Identity API to get account information for users and their associated groups. This is done via an XHR, using the CORS pre-flight mechanism of calling @OPTIONS@ on the REST endpoint. During this call, the CN is returning an @HTTP 403@ Not Authorized response to IE11 on Windows, but succeeds on Firefox and Chrome on Windows.

It seems (but we're not sure) that IE is responding to the request for a client certificate and whatever is sent is being rejected by the CN web server. However, it's not super straight forward. When Apache is configured with:

SSLVerifyClient optional
SSLVerifyDepth 10

IE11 succeeds on the @OPTIONS@ request. However, when the CN is configured to conditionally set @SSLVerifyClient@ within a @@ block:

SSLVerifyClient none

SSLVerifyClient optional

SSLVerifyDepth 10

the request fails (which is currently the production configuration).

However, after testing in STAGE, IE11 works fine when not asked for a client certificate (@SSLVerifyClient none@). It seems that the interaction with Apache changes based on the conditional logic in a specific @@ block, and IE11 responds incorrectly in some way.

To alleviate issues with browser-based client certificate requests, I suggest that we adopt the following configuration:

SSLVerifyClient none

SSLVerifyClient optional

SSLVerifyDepth 10

This configuration excludes most desktop/handheld browser clients from being asked for an X509 certificate. However, it still allows for Java, Python, curl, R, etc. clients to connect using client-side certificates. Since we've migrated to JWT token-based browser authentication, this seems reasonable to me.

This is currently a blocker in production, so we should consider a manual change to the production CNs before this gets rolled into a CCI release, if agreed upon. Thoughts welcome.

History

#1 - 2017-03-23 14:05 - Chris Jones

Dave pointed out http://stackoverflow.com/questions/18422980/security-error-using-cors-in-ie10-with-node-and-express . The accepted answer configures the server to not request a certificate, which is my suggestion above. This SO article also mentions IE Security settings, but changing those didn't have an effect (and isn't what we want to rely on either).

I've also found http://stackoverflow.com/questions/15442122/cors-with-ie-xmlhttprequest-and-ssl-https , which indicates that IE aborts when there is no @onprogress@ callback defined in the XHR. However, after testing this, I found no change either.

To isolate the issue, I wrote up the following HTML page that can be placed on any server that is not the CN in order to force the CORS request:

<!DOCTYPE html>

XHR CORS Test

```
    <script type="text/javascript">
    var XHRTest = {
        accounts_url: "https://cn.dataone.org/cn/v2/accounts",

        handle_error: function(response) {
            console.log("Error: ");
            console.log(response);
        },

        handle_load: function(response) {
            console.log("Loaded: ");
            console.log(response);
        },

        sendXHR: function() {
            var xhr = new XMLHttpRequest();
            xhr.onerror = XHRTest.handle_error;
            xhr.onprogress = function(msg) {console.log("Progress called.")};
            xhr.onload = XHRTest.handle_load;
            xhr.open("GET", XHRTest.accounts_url, true);
            xhr.send();
        }
    };
    </script>

</head>
<body onload = "XHRTest.sendXHR()">
    <span>Open the developer console to see the XHR results object.  Look at ProgressEvent.srcElement.response
</span>
</body>
```

This code aborts in IE11 on Windows 7 with

XMLHttpRequest: Network Error 0x4c7, The operation was canceled by the user

and the error callback is called. For Chrome 57 on Mac and Edge on Windows 10 it works fine, and we get the @/accounts@ XML.

I'm going to try changing the @SSLOptions@ directive by adding @OptRenegotiate@ to see if it changes the behavior.

#2 - 2017-03-23 14:46 - Chris Jones

Setting @SSLOptions +OptRenegotiate@ had no effect.

#3 - 2017-03-23 15:08 - Chris Jones

Based on the following entries in the Apache @error.log@ on cn-stage-ucsb-1.test.dataone.org, we can confirm that the SSL renegotiation is failing, and is a client-side issue:

[Thu Mar 23 15:04:30.207440 2017] [ssl:debug] [pid 21982:tid 140522672846592] ssl_engine_kernel.c(1911): [client 199.102.125.230:39905] AH02043: SSL virtual host for servername cn-stage.test.dataone.org found
[Thu Mar 23 15:04:30.254078 2017] [ssl:info] [pid 21982:tid 140522723202816] [client 199.102.125.230:34870] AH01964: Connection to child 130 established (server cn-stage.test.dataone.org:443)
[Thu Mar 23 15:04:30.254802 2017] [ssl:debug] [pid 21982:tid 140522723202816] ssl_engine_kernel.c(1911): [client 199.102.125.230:34870] AH02043: SSL virtual host for servername cn-stage.test.dataone.org found
[Thu Mar 23 15:04:30.296749 2017] [ssl:debug] [pid 21982:tid 140522672846592] ssl_engine_kernel.c(1844): [client 199.102.125.230:39905] AH02041: Protocol: TLSv1.2, Cipher: ECDHE-RSA-AES256-SHA384 (256/256 bits)
[Thu Mar 23 15:04:30.298445 2017] [ssl:debug] [pid 21982:tid 140522672846592] ssl_engine_kernel.c(222): [client 199.102.125.230:39905] AH02034: Initial (No.1) HTTPS request received for child 136 (server cn-stage.test.dataone.org:443), referer: https://dev.christopherjones.co/xhr-cors-test.html
[Thu Mar 23 15:04:30.298608 2017] [ssl:debug] [pid 21982:tid 140522672846592] ssl_engine_kernel.c(570): [client 199.102.125.230:39905] AH02255: Changed client verification type will force renegotiation, referer: https://dev.christopherjones.co/xhr-cors-test.html
[Thu Mar 23 15:04:30.298632 2017] [ssl:info] [pid 21982:tid 140522672846592] [client 199.102.125.230:39905] AH02221: Requesting connection re-negotiation, referer: https://dev.christopherjones.co/xhr-cors-test.html
[Thu Mar 23 15:04:30.298656 2017] [ssl:debug] [pid 21982:tid 140522672846592] ssl_engine_kernel.c(770): [client 199.102.125.230:39905] AH02260: Performing full renegotiation: complete handshake protocol (client does support secure renegotiation), referer: https://dev.christopherjones.co/xhr-cors-test.html
[Thu Mar 23 15:04:30.298717 2017] [ssl:info] [pid 21982:tid 140522672846592] [client 199.102.125.230:39905] AH02226: Awaiting re-negotiation handshake, referer: https://dev.christopherjones.co/xhr-cors-test.html
[Thu Mar 23 15:04:30.370405 2017] [ssl:debug] [pid 21982:tid 140522672846592] ssl_engine_kernel.c(1911): [client 199.102.125.230:39905] AH02043: SSL virtual host for servername cn-stage.test.dataone.org found
[Thu Mar 23 15:04:30.370936 2017] [ssl:debug] [pid 21982:tid 140522723202816] ssl_engine_kernel.c(1844): [client 199.102.125.230:34870] AH02041: Protocol: TLSv1.2, Cipher: ECDHE-RSA-AES256-SHA384 (256/256 bits)
[Thu Mar 23 15:04:30.492266 2017] [ssl:error] [pid 21982:tid 140522672846592] [client 199.102.125.230:39905] AH02261: Re-negotiation handshake failed: Not accepted by client!?, referer: https://dev.christopherjones.co/xhr-cors-test.html
[Thu Mar 23 15:04:30.492426 2017] [ssl:debug] [pid 21982:tid 140522672846592] ssl_engine_io.c(1212): (70014)End of file found: [client 199.102.125.230:39905] AH02007: SSL handshake interrupted by system [Hint: Stop button pressed in browser?!]
[Thu Mar 23 15:04:30.492448 2017] [ssl:info] [pid 21982:tid 140522672846592] [client 199.102.125.230:39905] AH01998: Connection closed to child 136 with abortive shutdown (server cn-stage.test.dataone.org:443)

#4 - 2017-03-23 21:21 - Jing Tao

- Assignee changed from Jing Tao to Chris Jones

#5 - 2017-03-28 16:35 - Dave Vieglais

- % Done changed from 0 to 30

- Milestone set to None

- Project changed from CN REST to Infrastructure

- Category changed from d1_cn_rest to dataone-cn-os-core

- Status changed from New to In Progress

To be included with the next release that includes dataone-os-core