Infrastructure - Story #8823

Recent Apache and OpenSSL combinations break connectivity on Ubuntu 18.04

2019-06-19 02:03 - Dave Vieglais

Status:	New	**Start date:**	2019-06-19
Priority:	High	**Due date:**	
Assignee:	Dave Vieglais	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Story Points:			

Description

The latest Ubuntu 18.04 release of Apache is 2.4.29 and OpenSSL is 1.1.1.

This combination creates a significant delay in TLS renegotiation that results from the Apache config option on the CNs:

```
SSLVerifyClient none
<Location "/cn">
    <If " ! ( %{HTTP_USER_AGENT} =~ /(windows|chrome|mozilla|safari|webkit)/i )">
        SSLVerifyClient optional
    </If>
</Location>
```

Which is intended to disable client certificate authentication for web browsers, but allow it for others. This approach worked fine on older Apache / OpenSSL but the new combination creates a several second wait when the server discovers the client is not a web browser and tells it to reconnect with the option of including a client certificate.

The latest released version of Apache is 2.4.39 and this is available through a PPA intended for Debian developers. This has been installed so far on dev-2, sandbox, stage, and stage-2 with the process:

```
sudo add-apt-repository ppa:ondrej/apache2
sudo apt update
sudo apt dist-upgrade
sudo systemctl restart apache2
```

This installs Apache 2.4.39 and OpenSSL 1.1.1c which appears to resolve the apparent bug in the 2.4.29 / 1.1.1 combination.

One issue with the update is that by default, Apache now offers TLSv1.3, which is great except that it appears to cause problems with at least Python clients failing to connect and getting a 403 error. For example:

```
$ python3
>>> import requests
>>> r = requests.get("https://cn-sandbox-ucsb-1.test.dataone.org/cn/v2/monitor/ping")
>>> r.status_code
403
```

That TLSv1.3 is the problem was verified with cn-stage-unm-2 by configuring Apache with:

```
  SSLProtocol all -TLSv1.3 -SSLv2 -SSLv3
```

to disable TLSv1.3. After this change the Python client was able to connect as expected.

A workaround has not yet been researched.

It is not clear if this issue applies to other clients such as R and Java, so until we learn one way or the other, TLSv1.3 will be disabled on the CNs.

--This issue will likely apply to Member Nodes as well once TLSv1.3 is generally available or if MNs choose to install Apache 2.4.39.-- CORRECTION: this issue only applies when attempting to renegotiate TLS after headers have been transferred, so will not typically apply to a MN.

Subtasks:

Task # 8824: Install Apache 2.4.39 and disable TLSv1.3 on CNs	**In Progress**

History

#1 - 2019-06-19 02:04 - Dave Vieglais

- Description updated

#2 - 2019-06-19 02:07 - Dave Vieglais

- Description updated

#3 - 2019-06-19 02:18 - Dave Vieglais

The issue with TLSv1.3 is Reason: Cannot perform Post-Handshake Authentication.

Hence, there is no way our current CN configuration will work with TLSv1.3. The alternatives are to:

1. drop client certificate authentication, or
2. provide a separate base URL for clients that use client certificate authentication.

#4 - 2019-06-19 02:43 - Dave Vieglais

- Description updated