

Infrastructure - Bug #7408

CILogon does not appear to be retrieving subjectInfo

2015-10-06 02:25 - Dave Vieglais

Status:	Closed	Start date:	2015-10-06
Priority:	Normal	Due date:	
Assignee:	Ben Leinfelder	% Done:	100%
Category:	Authentication, Authorization	Estimated time:	0.00 hour
Target version:		Story Points:	
Milestone:	None		
Product Version:	*		

Description

When retrieving a client certificate from CILogon, it is expected that CILogon makes a call to a CN in the respective environment to retrieve subjectInfo for the subject. This does not appear to be happening.

Environment: production

SSH to cn.dataone.org, watch /var/log/apache2/other_vhosts_access.log

Open browser to <https://cilogon.org/?skin=DataONE>

Successfully authenticate, and retrieve certificate (/tmp/x509up_u501)

command:

```
openssl x509 -noout -text -in /tmp/x509up_u501
```

shows no subject info, lack of subjectInfo verified with other tools.

Log grep of other_vhosts_access.log shows no request to retrieve subjectInfo

Need to diagnose where the issue is and rectify.

History

#1 - 2015-10-06 13:22 - Dave Vieglais

- Status changed from New to Closed

- % Done changed from 0 to 100

Turns out to be a problem on the CILogon service site, missing a perl library. Email thread below.

Was able to confirm that the service works as expected for production environment.

I found the problem. The URLs were being encoded correctly. However, there was a missing Perl module "Crypt::SSLeay".

I installed it as

```
# yum install perl-Crypt-SSLeay
```

Now things are working for my test script. Please try your logon again to verify that the fix works for you.

I apologize for the problem. Thank you for bring the issue to our attention.

--

Terry Fleury

tfleury@illinois.edu

On 10/6/2015 7:01 AM, Dave Vieglais wrote:

Jim,
thanks for the quick response.

Seems to be an issue with URL encoding?

The request:

```
curl "https://cn.dataone.org/cn/v1/accounts/CN=David%20Vieglais%20A2105,O=University%20of%20Kansas,C=US,DC=cilogon,DC=org"
```

works, whereas:

```
curl "https://cn.dataone.org/cn/v1/accounts/CN=David%20Vieglais A2105,O=University of Kansas,C=US,DC=cilogon,DC=org"
```

returns the 404 error.

I'll check to see if perhaps URL handling changed on our end. Would you mind checking to verify the request from CILogon is being encoded?

I am very surprised to hear that this may of been an issue for a year now.

thanks,
Dave V.

On 6 Oct 2015, at 6:58, Basney, Jim wrote:

Hi Dave,

Thanks for the congrats. All is well here. Sorry for the trouble with the CILogon certificate generation, and sorry I didn't see your message until this morning.

You're using the correct URL + skin parameter. They are:

DataONE - cn.dataone.org
DataONEDev - cn-dev.test.dataone.org
DataONEStage - cn-stage.test.dataone.org
DataONESandbox - cn-sandbox.test.dataone.org

Then we do a GET to `https://$cnsrver/cn/v1/accounts/$DN`.

However, when I try it from the command-line via curl, I'm getting an error:

```
$ curl "https://cn.dataone.org/cn/v1/accounts/CN=David Vieglais A2105,O=University of Kansas,C=US,DC=cilogon,DC=org"
<?xml version="1.0" encoding="UTF-8"?>
```

```
[LDAP: error code 32 - No Such Object]
```

Is there a problem with my curl command-line? As far as I can see, nothing has changed for the DataONE skins on the CILogon side recently, but I agree CILogon isn't getting the subjectInfo structure included in the issued certificates. Doing a quick search through our issued certificates, the last time I see the 1.3.6.1.4.1.34998.2.1 extension appearing is Oct 24 2014.

Regards,
Jim