Security API documentation

# Introduction:

The motivation behind developing this API was to provide a very simple way for performing authentication using caBIG core infrastructure. The api uses Dorian as the Identity Provider and Grid Grouper for providing group membership information.

# API doc:

The interface that end-user will use to perform authentication consists of two methods (provided by the SecurityClient interface):

**public String login(String username, String password, long timeoutMilliSec) throws SecurityAPIException;**

Parameters:

username: username to login

password: password to login

timeoutMilliSec : timeout specified in milliseconds. The request will timeout based on this parameter.

Returns:

If login was successful, returns a string in the following format

**"PASS \n"**

**"groups: <comma-separated-list> \n"**

**"session-id: <caBigSessionId> \n"**

groups is a comma separated list of groups the current user is affiliated with.

session-id is a unique session-id that gets generated per user login. The next time this user-id can be used to authenticate instead of user credentials while the session is still active. The session expires after 12 hrs.

If unsuccessful returns the following

**"FAIL \n"**

**"code:  <integer>"**

**"reason: <Sting>"**

Throws:

SecurityAPIException when some exception is thrown communicating with Dorian.

**public String login(String sessionId, long timeoutMilliSec) throws SecurityAPIException;**

Parameters:

sessionId: session-id of the current active session

timeoutMilliSec : timeout specified in milliseconds. The request will timeout based on this parameter.

Returns:

If login was successful, returns a string in the following format

**"PASS \n"**

**"groups: <comma-separated-list> \n"**

**"session-id: <caBigSessionId> \n"**

groups is a comma separated list of groups the current user is affiliated with.

session-id is the same as the input parameter

If unsuccessful returns the following

**"FAIL \n"**

**"code:  <integer>"**

**"reason: <Sting>"**

Throws:

SecurityAPIException when some exception is thrown communicating with Dorian.

# Configuration Parameters:

The following code snippet shows how to configure the SecurityClientFactory instance . The SecurityClientFactory is used to obtain instance of the SecurityClient with specified settings.

Parameters:

Properties props = **new** Properties();

props.setProperty("CABIG.identityProviderUrl",

https://dorian.training.cagrid.org:8443/wsrf/services/cagrid/Dorian");

props.setProperty("CABIG.authServiceUrl",

"https://dorian.training.cagrid.org:8443/wsrf/services/cagrid/Dorian");

props.setProperty("CABIG.gridGrouperUrl",

"https://grouper.training.cagrid.org:8443/wsrf/services/cagrid/GridGrouper");

SecurityClientFactory factory = **new** SecurityClientFactory(props);

client = factory.newInstance(SecurityClientType.*CABIG*);

identityProviderUrl : URL of the target grid identity provider. The snippet uses the test Dorian grid’s url.

authServiceUrl: URL of the target grid auth service. In the snippet, Dorian is used as both identity provider and also as the auth service.

gridGrouperUrl: URL of the gridGrouper web service.

# Email Discussion Thread:

On 4/15/11 7:48 PM, "Alan M Snyder" <[amsnyder@stanford.edu](mailto:amsnyder@stanford.edu)> wrote:

No that timeout is for the response. It would be best if the client can

control how long the API call blocks. For example of a TCP timeout is 90

seconds, you don't really want to wait 90 seconds. Perhaps just 2 or 3

seconds is long enough.

----- Original Message -----

From: "Yusuf M. Saghar" <[nadirsaghar@emory.edu](mailto:nadirsaghar@emory.edu)>

To: "Tony Pan" <[tony.pan@emory.edu](mailto:tony.pan@emory.edu)>, "Alan M Snyder"

<[amsnyder@stanford.edu](mailto:amsnyder@stanford.edu)>

Cc: "Peter 'Yan (NIH/NCI) [C]'" <[yanpe@mail.nih.gov](mailto:yanpe@mail.nih.gov)>, "Pat Mongkolwat"

<[p-mongkolwat@northwestern.edu](mailto:p-mongkolwat@northwestern.edu)>, "Danny K" <[dannyko@stanford.edu](mailto:dannyko@stanford.edu)>,

"Ashish Sharma" <[ashish.sharma@emory.edu](mailto:ashish.sharma@emory.edu)>

Sent: Friday, April 15, 2011 12:41:43 PM

Subject: Re: API to log into CaBig Grid.

The 'timeout' that we are referring to here , does it mean a "session

timeout" ( time for which the user's session is active ) or is it a tcp

connection timeout ( time before the request times out) ?

String loginCaBig(String usernmae, String password, long timeoutMilliSec

);

String loginCaBig(String sessionId, long timeoutMilliSec );

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nadir Saghar

System Software Engineer

Center for Comprehensive Informatics, Emory University

36 Eagle Row, #567, Atlanta, GA 30322

Phone: 404-712-0196; Fax: 404-727-4992

nadirsaghar@ < [mailto:s.johnson@emory.edu>emory.edu](mailto:s.johnson@emory.edu%3Eemory.edu)

On 4/14/11 4:01 PM, "Pan, Tony" < [tony.pan@emory.edu](mailto:tony.pan@emory.edu) > wrote:

Re. the session id:

So the sessionId are acting as unique identifier between the "service"

and the builder, instead of a true security token?

Nadir:

The sessionid would act as an "unsigned, unencrypted" token to our API

(coming in from the client app, through the application service, to our

class). As such, we will not be able to truly verify the source of the

information so we need to be careful what we store and pass back. In the

implementation, DO NOT store the SAML and x509 tokens in memory or on

disk. Just extract the needed information (identity string, life time,

etc), and store only those. My concern is that if our class holds the

secure tokens, and if later on the token is pass back to client or to

another caGrid service, there would be no way of ascertain who made the

request to retrieve the token from our class. It's best to be safe and

not store any saml or x509 right now, so that if the need comes up later,

we would be required to have a formal discussion about that.

Tony

-----Original Message-----

From: Alan M Snyder [ <mailto:amsnyder@stanford.edu> ]

Sent: Thursday, April 14, 2011 3:28 PM

To: Pan, Tony

Cc: Peter 'Yan (NIH/NCI) [C]'; Pat Mongkolwat; Danny K; Saghar, Yusuf M.;

Sharma, Ashish

Subject: Re: API to log into CaBig Grid.

The most complicated part is probably the timeout handling - do you

absolutely need that on a per-call basis?

That isn't essential, so if it slow down development don't worry about

that feature. In some cased the TCP timeout might be 30+ seconds, but

likely if you don't get a response within a second or two you know

something is wrong.

Re. session Id - do you really need to have multiple sessions ...

After seeing that the "service" was going to separate from the AIM

Template Builder yesterday, it became apparent the a sessionId would be

useful to have when trying to upload/download something from the service.

It means that a person would only need to inter a user-name password once

(say when logging into the AIM Template Builder) and then when they

upload to the "Service" the sessionId is passed and the service can just

check that instead of requiring a second user/password authentication.

I just want to make a disclaimer: ...

understood.

----- Original Message -----

From: "Tony Pan" < [tony.pan@emory.edu](mailto:tony.pan@emory.edu) >

To: "Alan M Snyder" < [amsnyder@stanford.edu](mailto:amsnyder@stanford.edu) >, "Ashish Sharma" <

[ashish.sharma@emory.edu](mailto:ashish.sharma@emory.edu) >

Cc: "Peter 'Yan (NIH/NCI) [C]'" < [yanpe@mail.nih.gov](mailto:yanpe@mail.nih.gov) >, "Pat Mongkolwat"

< [p-mongkolwat@northwestern.edu](mailto:p-mongkolwat@northwestern.edu) >, "Danny K" < [dannyko@stanford.edu](mailto:dannyko@stanford.edu) >,

"Yusuf M. Saghar" < [nadirsaghar@emory.edu](mailto:nadirsaghar@emory.edu) >

Sent: Thursday, April 14, 2011 12:15:01 PM

Subject: RE: API to log into CaBig Grid.

We are working on this, hopefully sometime next week. The most

complicated part is probably the timeout handling - do you absolutely

need that on a per-call basis? We are probably going to go with the jar

approach so we can internally handle any credential that caGrid hands

back.

Re. session Id - do you really need to have multiple sessions for the

same user that do not share user authentication state information? i.e,

do you expect group or login information to change from session to

session? I would propose that we get rid of the second function. The

first function can internally check to see if the user's log-in is still

valid (12 hour lifetime). If so, just return the currently cached

information (equivalent to your session).

I just want to make a disclaimer: please consider the API to be work in

progress and subject to change if there is need from your side or from

our side. We were not planning on releasing an API or implementation

until later. This is a quick thing we are doing so you can continue with

your work.

Thanks

Tony

-----Original Message-----

From: Alan M Snyder [ <mailto:amsnyder@stanford.edu> ]

Sent: Wednesday, April 13, 2011 5:53 PM

To: Pan, Tony; Sharma, Ashish

Cc: Peter 'Yan (NIH/NCI) [C]'; Pat Mongkolwat; Danny K

Subject: Re: API to log into CaBig Grid.

Tony, Ashish,

I'd like to modify the request I sent to you earlier today, based on a

meeting with Peter and Pat about the AIM Template Builder and the AIM

Template Service. (These now appear to be two separate processes.)

I'd like on jar file that implements the following two methods.

String loginCaBig(String usernmae, String password, long

timeoutMilliSec);

String loginCaBig(String sessionId, long timeoutMilliSec);

For both methods the response is the same. It is a string in the format.

If it passes:

"PASS \n"

"groups: <comma-separated-list> \n"

"session-id: <caBigSessionId> \n"

--

If it fails:

"FAIL \n"

"code: <integer>"

"reason: <Sting>"

The reason for the change is the sesionId would be useful when

uploading/retrieving an AIM Template from the "service".

Alan

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This e-mail message (including any attachments) is for the sole use of

the intended recipient(s) and may contain confidential and privileged

information. If the reader of this message is not the intended recipient,

you are hereby notified that any dissemination, distribution or copying

of this message (including any attachments) is strictly prohibited.

If you have received this message in error, please contact the sender by

reply e-mail message and destroy all copies of the original message

(including attachments).

This e-mail message (including any attachments) is for the sole use of

the intended recipient(s) and may contain confidential and privileged

information.  If the reader of this message is not the intended

recipient, you are hereby notified that any dissemination, distribution

or copying of this message (including any attachments) is strictly

prohibited.

If you have received this message in error, please contact

the sender by reply e-mail message and destroy all copies of the

original message (including attachments).